Abstract

This guide contains comprehensive information for network administrators, engineers, and operators who manage the IMC platform.
Legal and notice information

© Copyright 2010-2012 Hewlett-Packard Development Company, L.P.

No part of this documentation may be reproduced or transmitted in any form or by any means without prior written consent of Hewlett-Packard Development Company, L.P.

The information contained herein is subject to change without notice.

HEWLETT-PACKARD COMPANY MAKES NO WARRANTY OF ANY KIND WITH REGARD TO THIS MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Hewlett-Packard shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Acknowledgments

Adobe® is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

Oracle and Java are registered trademarks of Oracle and/or its affiliates.
Contents

1 Introduction to IMC

   IMC Overview................................................................................................................................. 1
   IMC base platform features .................................................................................................................. 2
      Role based administrative controls................................................................................................. 2
      Resource management ........................................................................................................................ 3
      Configuration and change management .......................................................................................... 4
      Network asset management .............................................................................................................. 5
      Real time fault management .............................................................................................................. 5
      Performance monitoring and management ......................................................................................... 6
      Global ACL management .................................................................................................................... 7
      Security monitoring ............................................................................................................................ 8
      Global VLAN management .................................................................................................................. 8
      Virtual Network Manager ................................................................................................................... 9
      Reporting ............................................................................................................................................ 9
      Intuitive user interface ....................................................................................................................... 10

   IMC service modules ............................................................................................................................ 10
      Wireless Service Manager .................................................................................................................. 10
      Voice Service Manager ...................................................................................................................... 11
      User Access Manager ........................................................................................................................ 11
      Endpoint Admission Defense ............................................................................................................. 12
      User Behavior Auditor ....................................................................................................................... 13
      QoS Manager ..................................................................................................................................... 13
      Network Traffic Analyzer ................................................................................................................... 14
      MPLS VPN Manager ........................................................................................................................... 14
      Service Health Manager ..................................................................................................................... 15
      How IMC works .................................................................................................................................. 15
      SOA framework .................................................................................................................................. 18

2 Planning considerations for a successful implementation ........................................................................... 20

   Knowing your organization’s network resource management requirements ........................................ 20
   Identifying network infrastructure stakeholders .................................................................................... 20
   Identifying stakeholder needs .............................................................................................................. 21
   Common data requirements .................................................................................................................. 21

   Knowing your network infrastructure .................................................................................................. 23
   Knowing your network topology .......................................................................................................... 23
   Knowing your device vendors, series, and models ................................................................................ 24
   Knowing access requirements and standards of your organization ..................................................... 24
   Identifying security policies and restrictions for monitoring ................................................................. 25
   Identifying the integration requirements and opportunities .................................................................. 25
   Translating requirements into actions .................................................................................................. 25

3 Exploring the IMC interface .......................................................................................................................... 29

   Logging into IMC .................................................................................................................................. 29
   Exploring the IMC home page ............................................................................................................... 29
      Basic operations on the IMC home page ............................................................................................. 30
      Alarm, performance and resource widgets ......................................................................................... 33
      Customizing spaces and system-defined widgets ............................................................................. 43
      Customizing RSS widgets .................................................................................................................. 45
      Device status via status bar ................................................................................................................... 45
      Alarm sound settings .......................................................................................................................... 46
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navigating IMC functions</td>
<td>48</td>
</tr>
<tr>
<td>Quick Start</td>
<td>59</td>
</tr>
<tr>
<td>Floating menus of the navigation tree</td>
<td>59</td>
</tr>
<tr>
<td>Navigating IMC using breadcrumb trails</td>
<td>59</td>
</tr>
<tr>
<td>Online help system</td>
<td>61</td>
</tr>
<tr>
<td>System-wide help</td>
<td>61</td>
</tr>
<tr>
<td>Context sensitive help</td>
<td>62</td>
</tr>
<tr>
<td>Global search</td>
<td>63</td>
</tr>
<tr>
<td>Performing a basic device search</td>
<td>63</td>
</tr>
<tr>
<td>Performing a basic user search</td>
<td>64</td>
</tr>
<tr>
<td>Performing an advanced search for a device</td>
<td>64</td>
</tr>
<tr>
<td>Performing an advanced search for an interface</td>
<td>65</td>
</tr>
<tr>
<td>Performing an advanced search for a user</td>
<td>65</td>
</tr>
<tr>
<td>Personalizing the IMC web interface</td>
<td>66</td>
</tr>
<tr>
<td>Accessing a favorite</td>
<td>66</td>
</tr>
<tr>
<td>Adding a favorite</td>
<td>66</td>
</tr>
<tr>
<td>Modifying a favorite</td>
<td>67</td>
</tr>
<tr>
<td>Sorting favorites</td>
<td>67</td>
</tr>
<tr>
<td>Deleting a favorite</td>
<td>67</td>
</tr>
<tr>
<td>Wizard Center</td>
<td>68</td>
</tr>
<tr>
<td>Quick Start</td>
<td>68</td>
</tr>
<tr>
<td>Support third-party device</td>
<td>69</td>
</tr>
<tr>
<td>Task Management</td>
<td>70</td>
</tr>
<tr>
<td>Accessing Task Management</td>
<td>70</td>
</tr>
<tr>
<td>Message history</td>
<td>71</td>
</tr>
<tr>
<td>Message options</td>
<td>71</td>
</tr>
<tr>
<td>Logging out of IMC</td>
<td>72</td>
</tr>
<tr>
<td>4 Configuring IMC for use</td>
<td>73</td>
</tr>
<tr>
<td>Securing IMC and access to managed resources</td>
<td>73</td>
</tr>
<tr>
<td>Resource Management: managing network resources with global settings</td>
<td>74</td>
</tr>
<tr>
<td>Device access templates</td>
<td>74</td>
</tr>
<tr>
<td>Configuring vendor and device information</td>
<td>92</td>
</tr>
<tr>
<td>Managing filters to filter interfaces</td>
<td>101</td>
</tr>
<tr>
<td>Operator management: managing secure access to IMC</td>
<td>103</td>
</tr>
<tr>
<td>Managing operator groups</td>
<td>104</td>
</tr>
<tr>
<td>Securing IMC access via authentication services</td>
<td>108</td>
</tr>
<tr>
<td>Securing IMC through operator login control templates</td>
<td>111</td>
</tr>
<tr>
<td>Establishing IMC password strategies</td>
<td>113</td>
</tr>
<tr>
<td>Managing IMC operators</td>
<td>114</td>
</tr>
<tr>
<td>Modifying IMC passwords</td>
<td>124</td>
</tr>
<tr>
<td>Managing online IMC operator access</td>
<td>124</td>
</tr>
<tr>
<td>Group Management: managing resources using groups in IMC</td>
<td>126</td>
</tr>
<tr>
<td>Device groups</td>
<td>126</td>
</tr>
<tr>
<td>User groups</td>
<td>132</td>
</tr>
<tr>
<td>Configuring IMC for alarm notifications</td>
<td>135</td>
</tr>
<tr>
<td>Mail server settings</td>
<td>135</td>
</tr>
<tr>
<td>SMSC settings</td>
<td>136</td>
</tr>
<tr>
<td>Integrating IMC alarms into other management systems</td>
<td>137</td>
</tr>
<tr>
<td>IMC hierarchical alarm configuration</td>
<td>137</td>
</tr>
<tr>
<td>MIB management</td>
<td>138</td>
</tr>
<tr>
<td>Adding a compiled MIB to IMC</td>
<td>138</td>
</tr>
<tr>
<td>Compiling a MIB in IMC</td>
<td>139</td>
</tr>
<tr>
<td>Removing a compiled MIB from IMC</td>
<td>140</td>
</tr>
<tr>
<td>Configuration center options</td>
<td>141</td>
</tr>
</tbody>
</table>
5 Resource management .......................................................... 153

Adding devices in IMC .................................................. 154

Adding devices manually to IMC ........................................ 154

Auto discovering devices .................................................. 158

Adding devices by importing device information .................. 172

Viewing devices with Device, IP, and Topology Views ............. 176

Viewing devices via the Device View .................................. 177

Viewing devices via the IP View ........................................ 179

Viewing devices via the Network Topology ......................... 181

Viewing devices with custom views ................................... 201

Viewing device interfaces with port groups ......................... 206

Managing port groups .................................................... 206

Searching for devices in IMC ........................................... 210

Searching for a device using the basic search feature ............. 211

Searching for a device using the advanced search feature ....... 211

Managing one device via device details .............................. 212

Accessing the device details page ..................................... 212

Managing multiple devices using batch operations ................ 276

Using batch mode to configure SNMP settings ..................... 276

Using batch mode to configure Telnet settings ..................... 278

Using batch mode to configure SSH settings ....................... 279

Using batch mode to configure polling intervals ................. 280

Using batch mode to modify login types ............................ 281

Using batch mode to modify ping settings ......................... 282

Using batch mode to modify interface up/down alarm filter .... 282

Checking device configurations in batch mode .................... 283

Modifying device configurations in batch mode ................... 284

Managing multiple devices from the device list .................... 299

Navigating to the device list .......................................... 300

Device list management options .................................... 301

Navigating to the device list .......................................... 308

Device list management options .................................... 310

Terminal access ......................................................... 317

Allocating IP addresses ................................................. 318

Unauthorized access .................................................... 323

History access log ....................................................... 329

Real-time location ....................................................... 332

Access configuration .................................................... 333

IP to MAC address binding ........................................... 340

Unauthorized access processing policy .............................. 344

Network Asset Manager ................................................ 345

Viewing network assets ............................................... 345

Asset OID ....................................................................... 350

Managing asset information in Network Asset Manager ........ 353
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>6 Extending and customizing functions to support third-party devices</td>
<td>375</td>
</tr>
<tr>
<td>Extending an existing function to support third-party devices</td>
<td>375</td>
</tr>
<tr>
<td>Creating a vendor folder</td>
<td>375</td>
</tr>
<tr>
<td>Creating a drive index file and a drive folder</td>
<td>376</td>
</tr>
<tr>
<td>Creating drive definition file</td>
<td>377</td>
</tr>
<tr>
<td>Defining the common service (CLICommon)</td>
<td>379</td>
</tr>
<tr>
<td>Defining services and actions for a component</td>
<td>380</td>
</tr>
<tr>
<td>Defining specific services</td>
<td>381</td>
</tr>
<tr>
<td>Defining the TCL script and Perl script</td>
<td>385</td>
</tr>
<tr>
<td>Extending a customized function</td>
<td>386</td>
</tr>
<tr>
<td>Defining background custom script</td>
<td>387</td>
</tr>
<tr>
<td>7 Configuration and change management</td>
<td>403</td>
</tr>
<tr>
<td>Configuration templates</td>
<td>403</td>
</tr>
<tr>
<td>Software library</td>
<td>403</td>
</tr>
<tr>
<td>Configuration compare</td>
<td>404</td>
</tr>
<tr>
<td>Configuration audit and reports</td>
<td>404</td>
</tr>
<tr>
<td>Software update</td>
<td>404</td>
</tr>
<tr>
<td>Auto backup plan</td>
<td>404</td>
</tr>
<tr>
<td>Configuration check</td>
<td>404</td>
</tr>
<tr>
<td>Using the Configuration Center</td>
<td>405</td>
</tr>
<tr>
<td>Accessing the Configuration Center</td>
<td>405</td>
</tr>
<tr>
<td>Querying for devices in the Configuration Center</td>
<td>406</td>
</tr>
<tr>
<td>Device configuration options in the Configuration Center</td>
<td>407</td>
</tr>
<tr>
<td>Managing device configurations with templates</td>
<td>420</td>
</tr>
<tr>
<td>Accessing configuration templates</td>
<td>420</td>
</tr>
<tr>
<td>Querying configuration templates</td>
<td>421</td>
</tr>
<tr>
<td>Organizing configuration templates</td>
<td>422</td>
</tr>
<tr>
<td>Creating a configuration template</td>
<td>423</td>
</tr>
<tr>
<td>Modifying a configuration template</td>
<td>429</td>
</tr>
<tr>
<td>Renaming a configuration template</td>
<td>431</td>
</tr>
<tr>
<td>Copying a configuration template</td>
<td>431</td>
</tr>
<tr>
<td>Exporting a configuration template</td>
<td>433</td>
</tr>
<tr>
<td>Deploying a configuration template</td>
<td>434</td>
</tr>
<tr>
<td>Deleting a configuration template</td>
<td>434</td>
</tr>
<tr>
<td>Managing the software library</td>
<td>434</td>
</tr>
<tr>
<td>Viewing the software library</td>
<td>434</td>
</tr>
<tr>
<td>Viewing the details of a software library entry</td>
<td>435</td>
</tr>
<tr>
<td>Searching for a software library entry</td>
<td>436</td>
</tr>
<tr>
<td>Importing software into the software library from a file</td>
<td>436</td>
</tr>
<tr>
<td>Importing software into the software library from a device</td>
<td>437</td>
</tr>
<tr>
<td>Adding OSM software into the software library</td>
<td>437</td>
</tr>
<tr>
<td>Renaming a software library entry</td>
<td>438</td>
</tr>
<tr>
<td>Modifying a software library entry</td>
<td>439</td>
</tr>
<tr>
<td>Exporting a software library entry</td>
<td>440</td>
</tr>
<tr>
<td>Deleting a software library entry</td>
<td>440</td>
</tr>
<tr>
<td>Establishing baselines by using a software library entry</td>
<td>440</td>
</tr>
<tr>
<td>Comparing device configurations</td>
<td>441</td>
</tr>
<tr>
<td>Configuration center</td>
<td>441</td>
</tr>
<tr>
<td>General configuration compare</td>
<td>442</td>
</tr>
</tbody>
</table>
Using Syslog to alarm rules ................................................................. 562
Browsing alarms ........................................................................ 568
Alarm details ............................................................................ 569
Querying alarms in IMC ............................................................... 571
Browsing real-time alarms ............................................................. 572
Browsing root alarms .................................................................. 575
Browsing all alarms ................................................................... 580
Faulty devices ........................................................................... 585
Alarm statistics .......................................................................... 585
TopN ......................................................................................... 586
Configuring alarm notifications ......................................................... 587
Managing email alarm notifications .................................................. 587
Managing SMS alarm notifications .................................................. 594
Managing alarm forwarding: Integrating with other management systems ........................................................................ 599
Managing hierarchical alarm settings .................................................. 605
Access device and core device alarm settings ........................................ 605
9 Performance management .............................................................. 607
Managing performance with global index settings ..................................... 607
Accessing global index settings .......................................................... 608
Searching global index settings .......................................................... 608
Managing global index settings .......................................................... 609
Managing individual device monitoring settings ...................................... 614
Accessing the monitor list .................................................................. 614
Switching monitor list .................................................................... 615
Searching for monitors ................................................................... 615
Managing device monitors ................................................................. 617
Viewing performance reports .............................................................. 622
Accessing performance view list .......................................................... 622
Querying performance view list .............................................................. 623
Organizing performance views with folders ................................................ 624
Managing performance views .............................................................. 625
Managing IMC’s performance monitor settings for topology maps .......................................................... 633
Accessing data shown in topo ................................................................. 633
Managing data shown in topo ................................................................. 634
Managing real-time performance monitor ................................................ 635
Viewing real-time monitor window ........................................................ 636
Managing Monitors ........................................................................ 636
Managing monitor graphs ................................................................. 640
Managing performance option .............................................................. 643
Setting display option .................................................................... 643
Setting monitor option .................................................................... 643
10 Access control list management ...................................................... 645
Simplifying ACL rule creation using the assistant ....................................... 646
Managing services using the ACL assistant .................................................. 647
Managing net address groups using the ACL assistant ................................... 650
Managing time ranges using the ACL assistant .................................................. 653
Configuring subnet mask type for ACL management ....................................... 657
Managing ACL templates in IMC .......................................................... 658
Viewing ACL templates ................................................................... 659
Creating ACL templates .................................................................. 661
Modifying ACL templates .................................................................. 671
Copying an ACL template .................................................................. 680
Exporting an ACL template .................................................................. 681
Deleting ACL templates ................................................................... 681
13 Reporting in IMC

My real time reports
Resource statistics report
Alarm analysis reports
Performance analysis summary reports
Customizing my real time report page
Resetting my report
Real time reports
Real time report templates
Managing real time reports
Managing real time report data sources
Real time report options
Scheduling real time reports
Quick custom reports
Quick custom report templates
Managing quick custom reports

14 Support and other resources

Contacting HP
Subscription service
Related information
Documents
Websites
Conventions
About HP IMC documents

Index
1 Introduction to IMC

IMC Overview

Network managers, engineers, and operators face complex challenges in their mission to deliver a reliable and available network infrastructure. They must manage an array of technologies that, together, constitute the network infrastructure including wireless LAN, MPLS, voice, and more. They must ensure the successful delivery of business services that run on it. They must manage network users as resources to ensure network availability and reliable access for all users. Also, they must manage these resources—networks, users, and services—in the context of the need and demand for established practices of operational excellence. These practice areas include how:

- The IT staff manages and audits device configurations and configuration changes
- Faults in the network are detected, reported, and resolved
- The performance of the infrastructure and the services that run on them are measured, monitored, and maintained
- Operators identify and address security threats, user identity, authentication, and behavior issues.

IMC is a comprehensive management platform that simplifies how IT staff can successfully meet these challenges. IMC was built from the ground up to support the FCAPS model for comprehensive management of the network infrastructure. In addition, IMC was designed to support the ITIL operational center of excellence IT practices model. IMC’s single-pane management paradigm enables end-to-end business management of IT services to address the stringent demands of today’s mission-critical enterprise IT operations.

IMC provides scalability by supporting distributed and hierarchical system architectures, through additional operating system and database support to meet the requirements of complex networks. IMC uses a SOA model to provide full resource, service, and user management. Its modular design enables the integration of traditionally separate management tools. IMC enables enterprises to expand their infrastructure management in scale and to seamlessly accommodate new technologies at the same time.

IMC base platform features

IMC consists of a base platform and service modules that offer additional functionalities. The base platform provides administrators and operators with the basic and advanced functionality needed to manage IMC and the devices managed by IMC. The IMC base platform provides the following functions:

- Administrative controls for managing IMC and access to it. This includes granting or restricting operator access to IMC features through operator and operator group management. The base platform also includes features for the system-wide management of device data collection and information shared by all IMC modules including the creation and maintenance of device, user, and service groups, and device vendor, series, and device model information. It also includes SNMP MIB management and other system-wide settings and functions. See "Role based administrative controls" (page 2).
- A broad feature set for network device management, from the ability to manage SNMP, Telnet, and SSH configurations on a device to configuring Spanning Tree and PoE energy management for managed switches and much more. See "Resource management" (page 3).
• Management of the configuration and system software files on devices managed by IMC. This includes storing, backing up, baselining, comparing, and deploying configuration and software files. See "Configuration and change management" (page 4).

• Real time management of events and the translation of events into faults and alarms in IMC. This includes creating, managing, and maintaining alarm lists, trap and Syslog filters and definitions, and configurations for notifications of alarms. See "Real time fault management" (page 5).

• Monitoring, reporting, and alarming on the performance of the network and the devices that comprise it. This includes managing global and device specific monitors and thresholds as well as creating views and reports for displaying performance information. See "Performance monitoring and management" (page 6).

• Access control list (ACL) management. This includes creating and maintaining ACL templates, resources, and rule sets and deploying ACL rule sets to devices managed by IMC. It also includes monitoring and leveraging ACLs that exist on devices for deployment to other network devices. See "Global ACL management" (page 7).

• Monitoring and managing security attacks and the alarms they generate. See "Security monitoring" (page 8).

• Global management of VLANs on all devices that support VLANs, managed by IMC. See "Global VLAN management" (page 8).

These are the functional areas of IMC’s base platform. In addition, the IMC framework and suite of services also includes service modules for extending the scope and reach of IMC’s ability to manage the network infrastructure.

Role based administrative controls

For network engineers, operators or managers to be successful, they must have the tools and access to the resources they need. These tools should support the IT staff in accomplishing the task of IT service delivery within the IT guidelines and practices for operational excellence. IMC enables organizations to meet these requirements because it provides administrators with both the tools and the ability to grant access to only those features and resources operators need. IMC provides controls and audit trails to support IT management best practices.

In IMC, management rights and access to all resources managed by IMC are granted or restricted through the use of three IMC features: operator groups, device groups, and custom views of the devices. Through the configuration of the operator account these three features converge to define the specific set of access and management rights and restrictions assigned to each operator. First, administrators define operator by selecting which IMC features members of the group can access. The IMC features that an administrator can grant or restrict access through operator groups include Resource Management, Alarm Management, Intelligent Configuration Center, Report Management, Performance Management, Network Asset Management, Security Control Center, Virtual Network Management, ACL Management, VLAN Management, Syslog Management, QoS Management, Data Analysis Management, and the Data Analyzer. Administrators can grant or rescind operator access to these functional areas of IMC as well as to specific features within these areas.

Next, administrators create device groups, which enable administrators to group devices by device type (usually a grouping of similar device types). Once device groups are created, administrators can assign operators to a device group, thus granting them access and rights to manage the devices in that group. In other words, operators do not have access and cannot even view devices that are not included in the groups to which they have been granted access.

Lastly, operators can create custom views, which also allow administrators to grant or restrict access and management rights to a group of devices in the custom view.
After creating the operator groups, device groups, and device views, the administrator assigns or restricts rights through the configuration of the operator account.

In addition to these flexible role-based administrative controls, IMC provides administrators with the following administrative controls over IMC features and the devices managed through IMC:

- Supports secure operator access to IMC via LDAP or RADIUS authentication.
- Provides operators with the ability to view the online activity of IMC operators and tools for logging online operators off and blocking their access temporarily or permanently.
- Employs the concept of access control to enable administrators to permit or deny operator access to IMC based on individual IP addresses as well as IP address ranges.
- Supports IT compliance practices by providing audit trails that detail changes IMC operators have made to devices in the infrastructure.

Resource management

IMC provides comprehensive element management for HP, H3C, and 3Com devices from the convenience of a single web portal. From the Resource tab, operators have access to a feature set for managing and monitoring many aspects of a device. IMC offers these management capabilities for a wide range of devices including routers, switches, wireless, voice, desktops, and servers. From this portal, operators can add, configure, monitor or manage one device at a time or multiple devices. In addition, operators can create batch jobs for managing more than one device.

IMC provides operators with several methods for adding devices. Operators can add devices manually. Operators can also use one of IMC’s four auto discovery methods: Routing-Based, ARP-Based, IPSec VPN-Based, or network segment based auto discovery to add devices to IMC. Operators can also add devices by importing a comma delimited list of devices and their attributes. Finally, operators can use IMC’s batch operation feature for adding devices.

IMC also provides operators with four different views for monitoring and managing devices:

- **Device View** groups devices by device type.
- **IP View** groups devices by IP address.
- **Network Topology View** offers operators a physical view of devices by generating a topology map of the network. Operators can create custom maps down to individual racks in the data center. Topology maps down to data center maps in IMC are active. A left mouse click on a topology map provides device monitoring information. A right mouse click on a topology map provides operators with device configuration and management features.
- **Custom View** provides operators with user-defined views to support the needs of their organization. IMC incorporates access control features into the custom view enabling administrators to manage access to devices through the use of these views. All views provide operators with summary color-coded views of current alarm status for devices in each view.

All views provide operators with access to IMC’s device monitoring and management features. From top-level summary views, operators can drill down to the **Device List**. From devices lists, operators can navigate to the **Device Details** page for each device.

The **Device Details** page provides operators with both summary and detailed information and real time data that operators need to ascertain the health and status of a device. The **Device Details** page provides operators with summary information including device label and system name, IP Address and Mask, location and contact information, hardware, product and serial number information. In addition, the **Device Details** page offers operators real time performance data, real time service monitoring data, and configuration management details for the selected device.
From the **Device Details** page, operators can take action to troubleshoot issues with the selected device. Also, operators can Telnet or SSH to the device, ping or traceroute to the device or launch a Web Manager or Device Panel view.

From the **Device Details** page, operators can also configure the selected device. Operators can modify SNMP, Telnet, or SSH settings, polling, ping, or Web manager parameters or configure ACLs for the selected device. Depending on the device type, operators can also view and configure PoE, VLAN interfaces, address binding, port security, RMON, Spanning Tree, and protocols including RIP, BGP, and OSPF.

## Configuration and change management

IMC’s **Configuration Center** combines the tasks of network device change and configuration management. With this feature, operators have the tools necessary to effectively manage device configurations and audit changes while also adhering to practices that support operational excellence.

Like IMC’s **Resource Management** feature, the **Configuration Center** has a portal for accessing most of IMC’s change and configuration management features. From this portal, operators have access to the configuration management details and history for devices managed by IMC. Operators can view the latest startup and running configurations for managed devices. Operators can also modify, restore, compare, deploy, backup, restore, and establish a baseline for configuration files. From this same page, operators can view configuration and software histories, prepare a device for software upgrades by removing unneeded files, and deploy software to devices.

Configuration templates provide operators with support for standardizing device configurations. With these templates, operators can create, store, baseline, and deploy configuration templates to one or more devices. Operators can create templates using a portion or an entire configuration file that has been backed up to IMC. Operators can also import a portion or an entire configuration file into a template, and can create templates from scratch. In IMC, configuration templates are either file based or segment based. A file based configuration template contains the contents of an entire configuration file. A segment based configuration template contains just a portion of a configuration file. Once a template has been created, it becomes available in the **Deployment Guide** for deployment to one or more compatible devices.

IMC also provides operators with a convenient facility for storing system software and other files in the **Software Library**. Operators can upload system or other files from devices managed by IMC or from the operator’s local computer. After uploading software to the **Software Library**, operators can establish a software baseline for devices using entries in the software library. Operators can then run software baselines to identify devices whose software differs from the baseline. System software in the **Software Library** becomes available in the **Deployment Guide** for deployment to one or more compatible devices.

The **Deployment Guide** provides operators with a process for selecting the configuration files or software to be deployed and the devices to deploy them to. As part of this process, IMC validates whether or not a configuration file or system software file can be successfully deployed. IMC also checks device resources to ensure that there are sufficient resources on every device to support a successful configuration file or software deployment. If not, operators can use the **Clean Device Space** feature to make room for new deployments. This ensures successful deployments and minimizes network outages due to configuration or system software deployment failures. Once a deployment task has been submitted to IMC, operators can view and manage the progress and results of a task using the **Deployment Task List**.

The **Auto Backup Plan** provides operators with the ability to schedule automated backups of device configurations. With this feature, operators can back up the startup or running configuration files for all manageable devices. IMC also provides operators with reporting on backup histories and from this page operators can quickly deploy a backup configuration file when necessary.

Most system and network administrators appreciate the value of a tool that compares the contents of two files. Using the **Compare with other Device Configurations** feature, operators can view two configuration files side-by-side and quickly identify what has changed as IMC highlights all differences. Additionally, IMC
notifies an operator of a changed device configuration. Operators can choose to view the entire file or only the differences, in addition to viewing each difference.

IMC also provides operators with the ability to track or audit changes to device configurations. IMC provides you with four auditing features. The Configuration Backup Report provides a view of the backup history of both the startup and running configuration files for devices managed by IMC. Operators can also initiate a configuration file restore for one or more devices from this report.

Using the Configuration Baseline Report feature, operators can view IMC’s comparisons of the startup and running configuration files against the configured baseline file. If changes between the files exist, IMC notes these changes and provides a link for the operator to manually compare the contents of the two files. From the Configuration Baseline Report page, operators can also launch the Deployment Guide to restore the baseline configuration to the device.

The Software Update Report provides operators with software update histories for all devices managed in IMC. From this page, operators can also launch the Deployment Guide to restore selected software to the source device.

With the Software Baseline Report, operators can compare the current system software against the configured baseline file. If differences between the baseline version and the current system software exist, IMC notes these differences. From the Software Baseline Report page, operators can launch the Deployment Guide to restore the baseline software to the device.

The Configuration Check feature supports organizations in adhering to compliance and standards. This feature enables operators to write rules and then create groups of rules that check the configuration of devices. First, the operator creates check rules that can include the contents of an entire configuration file or configuration command or just a portion. Then, operators can combine check rules into groups for ease of deployment. Once rules and groups are created, operators then create a configuration Check Task that combines rules or groups of rules with the list of selected devices and compares the device configuration against the content configured in the rules. Configuration check tasks results are displayed in the configuration check Task Report.

Network asset management

With Network Asset Manager, administrators and operators can track assets as well as changes to assets. This feature provides operators with a list of asset and drilldown capabilities into individual device details or device audit details. Operators can also query IMC for specific audit records and manage the device auditing process.

Real time fault management

IMC’s integrated network management system of fault, performance, auditing, security, and configuration reduces the effort required to manage complex network infrastructures. This becomes apparent to network managers with the integration of fault management. With IMC, network managers have one database of network devices in IMC that drives various tasks of network management. IMC’s database is leveraged in all IMC functions, including fault management. No longer do network managers have to maintain multiple databases for each functional area of performance, fault, asset, configuration, and security.

Like most IMC features, the alarm or event management system in IMC uses the existing device database and couples it with sophisticated SNMP trap processing and Syslog parsing algorithms to intelligently generate alarms for notifying operators and support organizations when a network failure or an event of interest occurs. IMC uses rules to define what an event of interest is and which events generate alarms. IMC includes pre-defined system rules and also provides operators with the ability to create user-defined rules for generating events and alarms.
IMC also includes root symptom analysis and built-in downstream event suppression by mapping out the network infrastructure and defining relationships between devices. IMC defines these relationships automatically through its comprehensive discovery algorithms. Using this information, IMC intelligently distinguishes between alarms that are most likely pointing to the root cause and those that are merely a symptom of a problem elsewhere in the infrastructure. Operators can specify alarm presentation based on these distinctions. IMC also provides operators with the ability to modify IMC’s mapping of the core and access devices used for root cause or symptom analysis and event suppression.

As with most other features, IMC provides operators with a single pane for viewing alarms in IMC as well as several alarm viewing options. From each of the alarm views, operators can drill down to view the detailed information for a particular alarm and take actions to correct the problem. Operators can also drill down to the Device Details page for accessing the monitoring information and configuration features for the device reporting issues.

IMC also offers operators the ability to notify members of the support organization. IMC supports email and SMS or text notifications. In addition, operators can forward alarms generated in IMC to other IMC instances or to other management systems including Help Desk system and manager of managers systems.

Performance monitoring and management

True to the FCAPS model, IMC also provides you with the ability to monitor the performance of devices managed by IMC. The Performance Management features of IMC provide operators with the ability to customize the collection, alarming and presentation of performance data. In addition, operators can leverage system or user-defined global or individual monitors to collect performance information, generate historical reports, and generate alarms when performance monitors meet threshold conditions. IMC enables the real time and historical performance management for managed devices.

IMC provides over two hundred global system defined monitors for measuring the availability, reachability, and performance of network devices. In addition to monitoring for standard device types such as routers and switches, IMC also supports the performance monitoring of technologies including IPSec VPNs, WLAN, QoS, VSM, and RMON. In addition, IMC provides operators with the ability to compile MIBs into IMC and create custom global monitors, which can then be applied to the monitor sets for one or more devices.

Sixteen of the over two hundred system defined monitors are configured with polling intervals, threshold settings, and alarm level settings to enable immediate, proactive performance monitoring of devices managed in IMC. Of these sixteen, IMC by default is configured to automatically add four primary performance monitors to devices when they are added to IMC. By default, IMC monitors devices for availability, response time, CPU usage, and memory usage.

IMC provides operators with flexibility for customizing global monitors including threshold settings. Operators can also add global monitors to the monitor sets for individual devices. This enables operators to tailor the performance monitoring for every device if needed. Operators can also customize the threshold settings for individual device monitors.

Once performance monitors have been created, operators can add performance views that include one or more monitors. Operators can add performance view shortcuts to the left navigation system, enabling one-click access to performance data for mission-critical devices. As with most of IMC’s features, performance data and the configuration of performance monitoring can be accessed from multiple places and most easily from the Device Details page.

IMC provides the real time monitor feature, which allows you to monitor the performance indexes of the key devices in your network, so that you can detect and solve problems in time.
Global ACL management

ACL Manager provides operators with a comprehensive feature set for managing ACLs for devices managed by IMC. With ACL Manager, operators can view and configure existing ACLs on a device managed by IMC, and import ACLs from devices into ACL Manager as a template or as an ACL resource. Once ACL templates and resources are created, they can be deployed to devices managed by IMC. Using ACL’s convenient **ACL Deployment** wizard, operators can easily and successfully deploy ACLs and ACL uses to devices managed by IMC. With ACL Manager’s Deployment task management features, operators can monitor and manage the deployment of ACLs and ACL resources. ACL Manager supports four types of ACLs: **Basic, Advanced, Link, and User-Defined.** With these four ACL types, operators can create rules based on 1) Source IP address or address range and mask; 2) Layer 3 and Layer 4 information including IP source and destination addresses, Layer 4 protocol information; 3) Layer 2 information including MAC source and destination addresses; and 4) user defined hexadecimal patterns and masks.

ACL templates in ACL Manager serve as a container for the configuration options required to create an ACL. Once an ACL template has been created, it can be imported as an ACL resource. An ACL resource in ACL Manager is an ACL that contains one or more rule sets. ACL resources, once created, can then be deployed to devices managed by IMC that support ACLs.

The ACL **Assistant** facilitates ACL template rule creation by modularizing some of the configuration components of an ACL rule, including services, network addresses, and time ranges. With services, operators can define one or more TCP or UDP ports as a named service. With net address groups, operators can specify an IP address or range of IP addresses and their subnet mask. With time ranges, operators specify fixed or recurring date and time ranges. Once these are created, the services, net address groups, and time range groups become available for use when configuring rules for templates.

ACL Manager also offers administrators and operators a feature set for simplifying the task of managing ACLs and their rule sets. The **ACL Resource List** provides operators with a single portal for viewing and managing all of the ACLs that can be deployed to network devices. From the **ACL Resource List**, operators can view, add, rename, and delete ACLs.

From the **ACL Resource List**, operators navigate to the **Rule Set List** for managing every aspect of a rule set for a given ACL. From this page, operators can view information for every rule in a set as well as take action on all of the rules in the list. Actions include adding, modifying, copying, deploying, or deleting existing rule sets. From the **Rule Set List**, operators can also import the contents of a template into a new rule set of an existing ACL.

ACL Manager also provides operators with two key features for managing the effect on network performance that an ACL can have. First, operators can redefine or sort manually the order of appearance of rules in a rule set, which can be crucial to its effectiveness when the rule set’s match order is based on the order of rule appearance. In addition, ACL Manager provides operators with an **Optimize** feature for evaluating the effect of rules on network performance as well as making and implementing recommendations for reducing the effect of ACLs on network performance.

ACL Manager also simplifies and streamlines the process for managing ACLs on devices. With ACL Manager, operators have a single portal for viewing and managing the ACL configurations on all devices that support ACLs. ACL Manager also provides operators with a single portal for managing ACL configurations for the selected device. From this portal, operators can view, synchronize, and refresh the ACL configuration data for the device as well as modify the ACL configuration polling interval. Options are also provided for managing ACL device configurations, including adding and deleting ACL definitions, exporting ACL text files, and applying ACLs as packet filters or VLAN filters to one or more interfaces on the device.

ACL Manager facilitates the deployment of ACLs and rule sets using the **ACL Deployment** wizard. This wizard provides operators with a step-by-step process for successfully deploying ACLs and ACL uses for packet and VLAN filtering as well as removing ACLs and ACL uses. During the deployment task configuration process,
IMC evaluates the selected devices and ACLs to determine whether or not the task can be executed successfully. IMC identifies when devices do not match the configuration selections and display warning messages and evaluation results to guide the successful deployment of ACL resources. The ACL Deployment wizard provides a facility for viewing and managing all deployment tasks via the ACL Deployment Task List.

Security monitoring

IMC offers administrators and operators a proactive and integrated security monitoring and management system with SCC. SCC provides operators with real time threat monitoring, detection, and analysis. In addition, SCC includes the ability to define security control policies that enable operators to take manual or automated actions when a security attack occurs.

IMC detects and provides actions for security and threats that include Flow Exception, Flow Monitor Abnormal, Flow Monitor Serious, IP Spoofing, WinNuke, SYN Flood, ICMP Flood, UDP Flood, IP Sweep, TCP Port Scan, UDP Port Scan, IPS Worm, IPS Scan, Traceret, Large ICMP, Smurf, ICMP Redirect, ICMP Unreachable, Fraggle, Source Route, Route Record, Land, Teardrop, TCP Flag, Ping of Death, Frag Flood, IP Fragment, Scan, ARP Overspeed, DHCP Server Detect, and Duplicate ARP Address.

IMC monitors many of these security threats in real time by receiving and processing two data sources: Syslog events and SNMP traps sent by devices. The Syslog messages that IMC alarms on include Duplicate Addresses, ARPOverspeed, DHCP Server Detect, and IMC’s attack event. IMC also processes SNMP traps sent by managed devices, The SNMP traps that SCC currently supports for security attack alarm include Duplicate Address, ARPOverspeed, DHCP-Server Detect, Flow Monitor Abnormal for IMC’s UAM component, Flow Monitor Serious for UAM’s component, and SecCenter. Once IMC has detected and escalated a security event to an alarm, it is displayed in one of the two tabular views, the Attack Alarm List and the Real Time Attack Alarm List for security attack alarms. SCC also provides operators with a visual display of attacks through the attack path topology map.

Operators can respond to attack alarms by initiating actions, such as shutting down an interface, sending an email, sending a message to the online user, kicking the online user off, and adding the online user to the blacklist.

SCC also provides integration with IMC’s EAD service module that enables SCC to receive security events from IPS and other security aware devices in the network and turn those events into actions, such as isolating or blocking endpoints to protect network assets.

Through the use of security control policies, operators can proactively manage their response to security threats and attacks. Service control policies allow operators to define what actions are taken in response to attack alarms. A security control policy combines the identification and alarming of a security attack with an action that can be taken in response to the security attack. The actions configured for security control policies can be executed manually or they can be configured to run automatically upon detection of the security attack.

Like many IMC modules, SCC also provides operators with summarized reporting of security attacks in the last hour. Summary reports include the Top 10 Attack Alarms Report, Top 10 Attack Sources Report, Top 10 Attack Destinations Report, and Execution Results Report.

SCC can be integrated with the SMS. You can open the SMS management page in SCC to view information about security devices managed by the SMS. Through the SMS, SCC integrates the monitoring functions for security devices in the entire network.

Global VLAN management

With IMC, operators have the ability to manage VLANs globally or on a per device basis. IMC’s Global VLAN option gives operators the ability to create standardized VLANs across all devices in the infrastructure.
that support VLANs. Operators can create VLANs and add, configure, or remove them from all devices that support this feature.

IMC also employs the batch operation concept to VLAN management by enabling operators to create and configure VLANs on one or more devices, including configuring access, trunk, or hybrid ports using the batch feature for VLAN management.

For individual device VLAN management, operators can select devices for configuring VLANS. From the same interface, operators can also configure virtual interfaces, access ports, trunk ports, or hybrid ports for each VLAN.

With IMC’s VLAN Topo option, operators can launch a network topology view that highlights devices for the selected VLAN and grays out devices that are not part of the VLAN. Operators can actively monitor and manage devices in the selected VLAN from the topology map.

**Virtual Network Manager**

VNM provides the ability to manage virtual network devices such as servers, virtual machines, and virtual switches. You can view virtual network resource configuration in Virtual Network View. By creating a vSwitch or port group, you can plan and manage your network.

In addition, VNM provides the virtual machine migration function. You can migrate a virtual machine from a server with limited resources to a server with enough resources to ensure the efficiency of the virtual machine. VNM automatically collects data on the vManager—a server that manages virtual servers. In the Migration Recommendation List, you can select manual or automatic migration. After the migration is complete, you can view the migration report.

With the Topology function, you can see the virtual network architecture to facilitate planning a virtual network.

**Reporting**

IMC offers administrator and operator performance and resource reporting options in the Report tab. From this tab, operators can find template driven reports for network assets, configuration and configuration changes, network device and link status and events, alarms, and network device health. In addition, operators can find reports on network user and service activity and device and link detail reports.

There are two types of report categories in IMC:

- **Real Time Report** offers operators reports on resource statistics, configuration and change, fault or alarm and performance reporting on network devices and interfaces, users and services.

- **Quick Custom Report** provides two types of informational reports – device and link. Device detail reports include information on device status, label, IP address, MAC address, device type, model, vendor, location, contact, sysOID, hardware version, software version, serial number and product number for managed devices. Quick custom reports based on link details include information on devices connected to either end of a link. This information includes device name, port, IP address, and port speed.

IMC provides every operator with the ability to customize the reporting interface to meet individual reporting needs. Using the Add My Real Time Report and the Add My Quick Report links, operators can customize the Report main page to include only those reports that are most useful. After adding a report to the Report main page, operators can access the report by clicking on the report name link and entering report parameters, including date and time, to access the information they need quickly.
Intuitive user interface

IMC includes many features that enable administrators and operators to effectively manage the network infrastructure. The tabular navigation system located at the top of every IMC page provides one click access to most of IMC’s features. Most of IMC’s main features include lists that provide operators with access to the managed resources. Most lists provide active links for drilling down into the details for individual components, such as the Device Details page. From these individual device or component pages, operators can access the IMC features that enable them to manage, monitor, configure, and audit network resources. IMC also provides operators with many paths to the same destination. For convenience, IMC provides operators with quick start guides and With the My Favorites feature, operators can create links to the IMC features they use most often. Once created, My Favorites links become available on every IMC page through the My Shortcut→My Favorites link located in the upper left corner of the left navigation system.

IMC provides two forms of online help:
- Universal online help system provides operators with detailed information on IMC features with examples and instructions.
- User interface provides operators with context sensitive help that includes instructions and guidance specific to a particular page or feature. User interface also provides a basic and advanced search facility available on almost every window in IMC. Using this feature, operators can quickly access the device details for any device based on the search criteria they entered. Most lists in IMC also provide operators with the ability to search or filter the list based on the criteria entered.

IMC service modules

IMC’s modular and scalable SOA architecture supports extension of IMC’s scope of coverage beyond the functionality of the base platform.

Additional and optional service modules are available to extend coverage. These additional areas of coverage include managing wireless and voice devices, QoS, MPLS VPNs, user access and behavior, traffic analysis, and endpoint security. IMC provides these additional areas of management from a single, integrated platform and web portal.

Wireless Service Manager

IMC provides network administrators and engineers with a unified management system for both wired and wireless networks. With IMC’s Wireless Service Manager module, operators can perform wireless LAN WLAN device configuration, topology, performance monitoring, RF coverage and planning, WLAN intrusion detection and defense, and generate WLAN service reports from the same platform they use to manage wired networks. In addition, IMC provides operators with historical reports for monitoring how wireless network usage, performance, and roaming patterns have changed over months or years.

WSM provides the following functionality:
- Unified management of wired and wireless devices includes network devices such as ACs, APs, Fit APs and mobile terminals.
- Wireless and wired network scans to identify and locate unauthorized rogue APs on a network, including those that are not in range of authorized APs or sensors. Once detected, rogue APs or unauthorized users are denied access to the network.
- Detects wireless attacks and sends alerts about network vulnerabilities to administrators.
- Provides specialized views and reports for multiple classes of users—from Level ½ helpdesk staff to network engineers, security auditors, IT managers and other user-defined groups.
• Provides template support for wireless device configuration that facilitates centralized configuration and control over wireless devices.

• UAM’s wireless service logical topology mapping provides visually display of wireless network deployment and the current state of devices and links on the network.

• Provides information about a mobile terminal on the network, including its MAC address, signal strength, transmit rate set, RSSI, SSID, channels used, and associated AC and AP. It also provides the roaming records of each mobile terminal.

• Provides topologies that show real-time RF information about the wireless network.

• Provides rogue device detection that identifies wireless intrusions as well as the intrusion AP. WSM also enables you to query information about the intrusion AP and add the intrusion AP to a blacklist.

• Provides wireless statistics reports that you can query and customize.

From a single pane, operators can manage the wired and the wireless infrastructure using IMC’s base platform and the Wireless Service Manager.

Voice Service Manager

IMC coupled with the VSM module offers operators an integrated management solution that provides a comprehensive set of tools for managing converged voice and data networks easily and efficiently. IMC’s VSM offers a single pane for voice resource and service management for 3Com and H3C voice infrastructures, including VCX® Connect platforms, Media Gateway, and IP phones. IMC VSM also provides comprehensive management and notification of any issues that may impact service quality. VSM monitors the network using built-in rules, diagnoses problems, tracks changes to IP phone status, and tracks inventory of communications devices and IP phones. It also provides tools to facilitate rapid troubleshooting and fault isolation; service-level, real-time alerting, and reporting are built in.

VSM provides the following functionality:

• The ability to configure, monitor, and optimize the performance of media servers, gateways, and endpoints.

• Monitoring of VoIP traffic.

• Real-time, graphical service-level views of the entire VoIP infrastructure.

• Tracking the real-time operational status of every VCX system and IP phone.

• Notification of issues that may impact service quality.

• Tracking of changes to IP phone status.

• Tracking and inventory of communications devices and IP phones.

• Tools to facilitate rapid troubleshooting and fault isolation.

• Real-time tracking, evaluation, and reporting on user experience and metrics such as delay, loss, and jitter. Measures service quality and calculates reports associated with active calls on the system.

• Call quality metrics gathered from IP phones that enable administrators to assess call quality and address issues proactively.

• IMC’s VSM module provides complete monitoring and management of the voice infrastructure, including VCX, NBX, and related IP telephony devices, ensuring a single pane of management and service quality for voice infrastructure-related devices.

User Access Manager

The UAM module provides IMC users with authentication and authorization services for endpoints accessing the network edge. As a component of the IMC management platform, UAM supports access policies across
devices such as Ethernet switches, routers, broadband access servers, and VPN access gateways to centrally manage access for wired, wireless, and remote users. UAM, together with the base IMC platform and other IMC modules, provides network operators with integrated management of users, resources, and services.

UAM provides the following functionality:

- RADIUS server that supports centralized AAA management of endpoints that connect and use network services.
- Policy management provides access control with tiered privilege levels. IMC UAM enables multiple 802.1X authentication methods such as PAP, CHAP, EAP, and MS-CHAPv2, and leverages existing user directories as a RADIUS proxy directly to LDAP-compliant user stores such as the Microsoft Active Directory, Novelle Directory, OpenLDAP, or as a local user store.
- Realms can be created within UAM to authenticate user names and passwords against distributed UAM databases. This provides authentication redundancy, increasing security and enabling the authentication of roaming users. IMC UAM provides flexible authorization policies to dictate access by defining access policies for individual users, devices, and groups. Additionally, policies provide the ability to control access by location and time of day.
- Reporting capabilities through its centralized, Web-based management console, enabling network administrators to quickly scan the activity and status of all devices currently or historically connected to the network. Reports may be used for real-time analysis, historical analysis, compliance auditing, and troubleshooting.
- A comprehensive directory of all network attached devices and endpoints—including printers, IP telephony equipment, uninterruptible power supplies, HVAC systems, PXE boot hosts and badge readers—to provide additional control and authentication for "non-networking" devices.
- A single, central database of devices, users, and available services — important for networks that include more than one remote communications server and access device.
- Topology view of access services provides immediate visualization of the access infrastructure and online users. This provides a tool for monitoring and managing access systems and users.

User Access Manager is integrated with other IMC services and features, providing operators with one pane for managing critical network resources.

**Endpoint Admission Defense**

The EAD module supports operators in reducing network vulnerabilities by integrating security policy management and endpoint posture assessment for identifying and evaluating, alerting on, and isolating risks at the network edge. NAC solutions have typically involved the integration of several functions that were usually deployed, configured, managed, and audited as independent systems. The HP IMC management platform provides all of these functions in a single platform, eliminating the complexity of managing multiple systems. With EAD, IMC integrates security threat evaluation, identification, location, security event awareness, and the execution of protective measures into a centrally managed and monitored platform. IMC reduces implementation costs and complexity while increasing overall network security.

EAD provides the following functionality:

- Reduces the risk of malicious code or actions by detecting endpoint patches, viruses, ARP attacks, abnormal traffic, the installation and execution of sensitive software, as well as the status of system services.
- Works in conjunction with the user access manager to define and apply appropriate security posture policies to every user or device on the network. With EAD, administrators can build policies for operating systems and operating system patches, registry settings, applications, processes, and services into their EAD policies.
• The EAD security policy component allows administrators to control endpoint admission based on identity and the posture of the endpoint. Network operators can regulate network access based on identity, posture to prevent unauthorized access to network assets and resources. If an endpoint is not compliant with required software packages and updates, network assets can be protected by blocking or isolating endpoints’ access or by non-intrusive actions such as notification and monitoring of the endpoint.

• Works in conjunction with the iNode desktop client to gather endpoint posture information to determine if an endpoint is compliant with established security policies.

• With the iNode desktop client, key data theft protection features can also be enabled, such as controlling access to USB and CD drives, to protect sensitive data.

• To ensure continued security, EAD provides continual monitoring of endpoint traffic, installed software, running processes and registry changes.

• IMC leverages the existing instrumentation of network devices supporting NetStream and sFlow data to provide greater visibility and control over network usage. Interaction with the integrated User Access Manager component enables traffic flows to be linked with users rather than IP addresses alone for comprehensive auditing of network usage. EAD also provides operators with an EAD Service report that allows administrators and operators to view and analyze statistics related to security services.

EAD provides operators with a single console for identifying, evaluating, locating, monitoring, reporting on, and protecting the network from the many threats that can be introduced at the network edge.

User Behavior Auditor

The UBA module is a log auditing tool that enables operators to view user and network access information. UBA is designed to process large, complex log files and present the information in a simplified tabular format. UBA provides auditing of NAT, Web, and FTP site visits and more.

UBA provides the following functionality:

• UBA supports processing of log files from NAT, NetStream, Flow, and the DIG probe. With UBA log analysis, operators have visibility into user behavior that supports problem identification and resolution as well as network resource planning.

• UBA can perform general behavior audits as well as NAT audits, Web visiting audits, FTP audits, and mail audits.

• User defined auditing templates

The combination of UAM and UBA offers operators tools for managing user access and authentication to critical network resources as well as visibility into the behavior of users on the network.

QoS Manager

The QoSM is the core component of IMC’s QoS solution. QoSM provides operators with a common set of QoS device and configuration management features for easily managing QoS for different device types. IMC’s QoSM straightforward implementation of QoS management enables operators to focus on most critical aspects of QoS management - service planning. The QoS manager provides the following functions:

• Auto discovery feature for discovering the real time QoS configurations for devices in the network.

• Traffic classification is the basis for providing differentiated services. QoSM enables operators to organize traffic into different classes based on the configured match criteria, such as source or destination address, IP protocol type, port number, and more.

• For managing traffic control and network resources effectively, QoSM enables operators to configure CAR, GTS, priority marking, queue scheduling, and congestion avoidance.
• Enables operators to perform traffic control through the use of QoS policies. QoS policies in IMC allow operators to associate a class with traffic behavior. QoSM supports multiple class-to-traffic behavior associations in a policy.

• Like the Configuration Center in IMC’s base platform, QoSM also utilizes a deployment manager for applying QoS policies to targeted devices. Operators can define different deployment schemes based on the network design, enabling operators to manage and maintain QoS services throughout the network. The QoSM deployment manager enables operators to manage the application and removal of QoS policies for devices that support QoS. With the QoSM auditing feature, operators can check the consistency between the current configurations on the devices and the policy applications in the scheme.

• Leverages ACL information on devices to provide operators with a method for creating and managed ACLs.

• List of QoS-capable devices that enables operators to quickly and effectively manage their QoS implementations

• SLA Manager allows you to manage and monitor network performance through the management of service types, service levels, and SLA instances.

The three types of reports are instance report, SLA Service Agreement report, and user-defined group SLA report.

Network Traffic Analyzer
The NTA provides operators with real time traffic analysis. NTA is a graphical network monitoring tool that leverages industry standard sources of network traffic data to generate real-time displays of TopN users and applications. Routers and switches that support NetFlow provide NTA with the data that feeds NTA reports. NTA analysis and reports support operators in understanding how network bandwidth and resources are being used as well as with information on which hosts and uses are consuming network resources. NTA also supports operators in identifying network bottlenecks, with support in taking corrective measures. The information provided by NTA supports mission critical network management activities such as network planning, monitoring, optimization, and troubleshooting.

NTA provides the following features and benefits:

• Uses embedded instrumentation available in switches and routers including sFlow, NetFlow, and Netstream. This lowers the cost of network monitoring by eliminating the need for expensive probes.

• Supports both the strategic and tactical aspects of network management. NTA delivers detailed information on network bandwidth usage pattern, enabling operators and engineers to make well-informed policy and planning decisions. NTA also provides detailed information on specific applications, users, and ports, enabling operators to quickly determine the source of spikes and bursts to proactively monitor, control, and manage network usage.

• Provides network managers with network-wide surveillance of complex multilayer switched and routed environments, ensuring the rapid identification and resolution of threats to the network. This information allows administrators to identify suspicious behavior, respond to security threats, ensure quality of service, and enforce security policies.

MPLS VPN Manager
The MVM module brings operators VPN monitoring and management features for MPLS networks to the IMC suite of network management applications.

MVM provides the following features:
• Allows operators to auto discover, map MPLS VPN topologies, monitor, audit, measure performance, and manage VPN deployment for MPLS networks.
• Support for heterogeneous networks that include MPLS VPN devices from Cisco, H3C, and Huawei VPN devices.
• Includes a MVM TE sub-component that provides monitoring of TE devices, addition and publishing of tunnels, and protection of service quality.
• MVM TE enables operators to monitor the entire MPLS VPN network, distribute suitable network resource and ensure service quality.

Service Health Manager

With the increase of network applications, various services impose higher requirements on the reliability and stability of the network. It is difficult for the network administrator to provide a reliable network for services and make sure that various applications can satisfy the customer requirements.

Service Health Manager provides the following functions:
• Visual service quality management
• Integration of the alarm, performance, NTA, and NQA data
• Use of the KQI and SLA to monitor and measure the service health and visually manage the service health
• Visual display of SLA statistics and rating results in diagrams and tables, so that you can understand the overall service level and promptly find out potential problems

How IMC works

Network managers have been challenged by the number of systems that were required to manage and monitor the network infrastructure. Separate, specialized systems were and continue to be used for managing network faults, configuration, performance, auditing, assets, security, and performance. Network managers were required to maintain separate databases of devices and device information. Integration and interoperability between these systems were often and continue to be complex and expensive. The end result was often monolithic systems with large feature sets that were not always aligned with the services or needs of IT organizations or Network Operations Centers with multiple consoles, all reporting different, uncorrelated information about the health and performance of the network infrastructure.

The SOA model for application development has changed what is possible for management of the network infrastructure. SOA is an adaptable set of design principles oriented around business services that inform how an application is developed and integrates with other applications. An application developed with an SOA architecture provides its users with a set of loosely integrated services with well defined interfaces and a method for users of those services to become aware of, communicate with, and use the services made available by the SOA application.

In SOA, a "service" is a unit of work that is bounded, well defined, and well understood. Each service is independent, with a set of defined interfaces that other applications can call upon to execute in a standard way without requiring any knowledge of how the service is performed. A service can be a business process or a step in a business process. Services can be combined, used, and reused to create applications that meet business needs. SOA also defines how services or service providers and service consumers communicate. A service provider is a module or service in the application that provides a service, function, or unit of work. A service consumer is a service that makes use of the service offered by a service module and can be another service in the application. In SOA, service providers publish the services they offer and the requirements to participate in those services. The format of service requests and responses are well defined for both service
providers and service consumers. Service requests and responses are published on the shared message or communication bus and service providers and consumers both subscribe to messages sent on the bus.

From a software development perspective, SOA applications benefit by the separation of the business logic from the layers that manage and communicate with computer and other resources such as web and database interfaces. Web interfaces in SOA applications are provided for the most part by common libraries defined at the basic and service presentation layer. This means that developers can rely on existing and established libraries for quickly delivering a consistent, coherent user interface. In addition, developers can leverage existing modules or protocols at the data abstraction layer for communicating with databases and devices they read data from or write data to.

IMC is a suite of loosely integrated services based on a SOA framework that delivers unified resource management for devices in the network infrastructure based on the FCAPS model. IMC service modules encompass the FCAPS model for delivering fault, configuration, asset and auditing, performance, and security management in a single framework. In addition, IMC provides service modules that extend to other value added service areas including MPLS VPN management, wireless service management, traffic analysis, voice service management, guest access management, authentication and authorization, and EPON provisioning. In addition, IMC provides business service solutions including SLA management, desktop asset management, network access control solutions, and user behavior monitoring and management.

Three layers in IMC conform to the three layers of a SOA framework. The first layer is the Data Abstraction and Data Access Layer, allowing for the separation of the business logic from database communications. The Data Abstraction layer provides access data for resources managed by IMC as well as access to databases that store information about the managed resources. IMC leverages industry standard technologies such as JDBC and JNDI for handling IMC database communications. Using JDBC as the interface to the database enables IMC to communicate with virtually any database that also supports JDBC. IMC also relies on industry standard protocols including SNMP, Syslog, Telnet, and SSH for communicating with and collecting information on devices managed by IMC.

The IMC platform also has a Service Presentation Layer and Basic Presentation Layer that also separates the business logic from the processes that present IMC’s services and data to the IMC administrators and operators. IMC leverages common and external SPL to deliver a unified user interface for the base IMC platform and IMC modules based on XML and Web Services. Using a unified Web SDK allows IMC to use Java libraries to publish and subscribe on the message bus for the presentation of information in a web format. IMC also leverages report platforms and topology platforms at the presentation layer to deliver IMC topology mapping and reporting services.

The heart of IMC is the Service Logic Layer and Common Service Units of its SOA framework, also known as the middleware. The standard and external Service Logic Libraries (SLL) at the Service Logic Layer contain the business logic internal to IMC that drives the data analytics and processing analytics for all services delivered by IMC. The CSU in IMC—Resource, Fault, Security, Performance, Configuration, Log, and Data Analyzer—are the processes external to the business logic that manage access and communication between the business logic at the Service Logical Layer and the processes at the Presentation and Data Abstraction and Access Layers. In other words, the Common Service Units are what make the business logic contained available to all other processes in IMC as it handles publishing and subscription within IMC for all services. Figure 1 (page 17) shows a graphical representation of the IMC framework and the components that constitute it.
The example scenario is initiating an auto discovery. Navigate to the **Device Details** page for a device just discovered and shutdown an interface on the device. Assume the **Home** page as the starting point for this exercise. This is a high level overview of the process and does not contain specific, packet for packet, request/response pairs.

From IMC’s home page, click the **Resource** tab located at the top of the **Home** page. The common SPL publishes the request for the **Resource** page to the communication bus. The Resource CSU picks up the request and invokes the DAL for the data that is used to render the dynamic data (device status) that is displayed on the **Resource** home page. The DAL publishes a call to the database for current information on the status of devices in IMC and the database picks up the request. The results of the database query for current information are stored in the Data Cache. The Resource CSU picks up the results of the database query and publishes the **Home** page response with the dynamic data to the communication bus. The common SPL picks up the **Home** page response and renders it on the operator’s local computer.

Next, click the **Auto Discovery** link to begin the process of automatically discovering and adding devices to IMC. The common SPL publishes the request for auto discovery on the communication bus, which is picked up by the Service Logic Layer. The Service Logic Layer identifies and forwards the request to the appropriate CSU, in this case the Resource CSU. The Resource CSU publishes the **Auto Discovery** response on the communication bus, which the common SPL picks up. The common SPL renders the auto discovery configuration page on the operator’s computer.

Next, enter configuration parameters for the auto discovery and click the **Auto Discovery** button to begin the discovery process. The common SPL publishes the configuration information we entered for the auto discovery on the communication bus, which is picked up by the Resource CSU. The Resource CSU initiates the discovery CSU and pushes data through the JDBC interface into tables in the IMC database using the communication bus. In addition, the Resource CSU publishes the data to the communication bus, which is picked up by the common SPL for real time web updates on the operator’s local computer. The Resource CSU manages these parallel processes of discovery, of pushing and processing of data to the database, and of updating the operator’s web interface with a current status.
Next, navigate to the **Device View** and click **All Devices** to view a list of all devices. The navigation prompts the common SPL to publish a request for the **All Devices** page, which is picked up and responded to by the Resource CSU. The Resource CSU publishes a request for data, since IMC views all have dynamic data, which is picked up by the Data Abstraction Layer. The Data Abstraction layer responds to the request by publishing a response with current information from the Data Cache or by initiating a query to the database, if necessary, to render current real time status information on the **All Devices** page. The Resource CSU publishes the response, which the common SPL picks up and displays on the operator’s local computer.

Then, navigate to the **Device Details** page for the device by clicking on the link in the **Device Label** field from the **All Devices** list. The navigation prompts the common SPL to publish the request for the data specific to the selected device for the **Device Details** page, which is picked up by the SLL. The SLL identifies which of the several CSUs should be invoked by the request and forwards the request to the appropriate CSU, in this case the Resource CSU. The Resource CSU again publishes a request for data, which is picked up by the Data Abstraction Layer. The Data Abstraction Layer responds to the request by initiating a query to the database to render the **Device Details** information for the requested device. The Data Abstraction Layer publishes the response, which is picked up by the Resource CSU and published on the communication bus, which the Service Logical Layer picks up and displays on the operator’s local computer.

From the **Device Details** page, click the **Interface List** to drill down into the list of interfaces for the selected device and from there click on the interface to shut down. The navigation prompts the common SPL to publish the request for the **Interface List** and the **Interface Details** page for the specific interface. The SLL picks up both requests. The SLL identifies which of the several CSUs should be invoked by the request and forwards the request to the appropriate CSU, in this case the Resource CSU. The Resource CSU again publishes the request for data, which is picked up by the Data Abstraction Layer. The Data Abstraction Layer responds to the request by initiating a query to the database to render the information on the **Interface List** page. The Data Abstraction layer publishes a response, which is picked up by the Resource CSU and published on the communication bus, which the common SPL picks up and displays on the operator’s local computer.

Lastly, click the ✗ **DOWN** option from the **Action** menu located on the right of the **Interface Details** page. The navigation prompts the common SPL to publish the request for the interface ✗ **DOWN** function, which is picked up by the SLL. The SLL identifies which of the several CSUs should be invoked by the request and forwards the request to the appropriate CSU, in this case the Configuration CSU. The Configuration CSU publishes the request on the communication bus, which is picked up by the Data Abstraction Layer. The Data Abstraction layer determines which of the 2500+ device abstractions is required to fulfill this DOWN request. (A device abstraction in IMC includes a combination of information about the device including vendor, device type, model, command set, and execution method.) Once the Data Abstraction Layer has identified the abstraction to use, it then publishes a request on the communication bus for the method of communication. The IMC database picks up the request and publishes the communication method (SNMP, Telnet, or SSH) configured for the device. The Data Abstraction layer picks up the response and begins communicating with the device itself using the communication method specified by the database. Using the command set and execution method specified in the abstraction, the Data Abstraction Layer issues the interface **DOWN** request to the device. The Data Abstraction Layer then publishes the status for the **DOWN** request to the communication bus, which is picked up by the Configuration CSU. The Configuration CSU publishes the status to the communication bus, which is picked up by the common SPL and rendered on the operator’s local computer.

**SOA framework**

The SOA single, integrated framework provides organizations with a foundation for network management based on the FCAPS model that is both scalable and extensible. Network infrastructures can grow in size, in demand for performance, in diversity of device types, and in demand for new functionality and IMC grows with them. First, networks grow in size. With IMC’s SOA framework, organizations can deploy multiple IMC
systems to new areas of growth. All IMC instances can communicate with each other and share information through hierarchical or parent/child relationships with each other.

Networks can also grow in their demand for higher performance from IMC as the demand for network services and network management services grows. Given IMC’s distributed processing at the CSU or middleware layer and a communication bus that all IMC instances and service modules publish and subscribe to, operators can meet this demand by deploying separate instances of one or more CSUs. For example, organizations that have high demand for fault management may consider deploying the Fault CSU on a dedicated system. Or, large organizations that use IMC to manage device configurations and change may consider deploying the Configuration CSU on a dedicated system for higher performance.

IMC can also grow in diversity of device types that can be managed. IMC abstracts information about device vendors, device types, command sets, and execution methods and stores this at the Data Abstraction Layer that is shared by all CSU modules. This means that IMC can easily and seamlessly add new devices as they emerge and continue to add abstractions for existing devices with each new release of IMC.

Given IMC’s SOA framework, HP continues to develop new CSU modules at the middleware layer that are aligned with IT functional needs as those needs change and grow. Extending IMC to meet new functional needs is as simple as developing a new Common Service Unit that participates in the publish/subscribe communication bus and shared Data Access Layer and IMC database resources.

In short, IMC’s framework offers administrators and operators room to grow as their networks grow and their demand for integrated network management grows.
2 Planning considerations for a successful implementation

Executing a successful deployment of IMC requires gathering information about what infrastructure stakeholders need as well as what information they have about the network infrastructure, devices that comprise it, and services that run on it. Understanding what your stakeholders’ needs and requirements are help you understand how IMC must be configured to meet those needs. Stakeholders and IT staff also have very valuable information on the network, its idiosyncrasies and performance that also support you in configuring IMC successfully.

In addition to interviewing stakeholders to understand what their requirements are, you need to investigate various areas of the network infrastructure. You need to know your network in order to ensure a successful implementation of IMC.

Once you have interviewed your stakeholders and investigated the many and varied layers of a network infrastructure, you are ready to begin translating requirements into actionable configuration tasks to create a successful deployment of IMC.

Knowing your organization’s network resource management requirements

Collaborating with your stakeholders to identify their needs and to determine if and how their needs are met by IMC is critical to the successful deployment of IMC. Therefore, identifying and interviewing your stakeholders to understand their requirements for IMC and to gather from them the information you need to configure IMC effectively is a great place to begin planning your IMC deployment.

Identifying network infrastructure stakeholders

To ensure a successful IMC deployment, you must identify your organization users and their needs. The most likely stakeholders of IMC are those who manage, engineer, and support the network infrastructure. This includes network managers, engineers, administrators, and the NOC staff. The network engineering and operations teams benefit significantly by the services IMC offers and they are the greatest source of information and experience for guiding a successful deployment of IMC.

Network security teams also have a need or interest in gaining visibility into the network infrastructure. Teams that engineer and support data center environments also benefit by IMC. Teams that develop and support databases and applications also have some interest or need for visibility into the network infrastructure. Systems management staff responsible for managing system software upgrades and patches have an interest in the visibility that IMC provides.

Teams that support the tracking and resolution of failures and problems, including Help Desks, have an interest in IMC. For organizations that have formal or informal processes for monitoring, managing, and reporting on service quality and compliance with service level agreements are also IMC stakeholders. Organizations that deal with governance, risk and compliance issues and initiatives, those who deal with auditing IT controls are also stakeholders for IMC. Managers, engineers and teams charged with meeting the performance requirements of the network and those who plan for the future capacity demands for IT services are also key stakeholders of IMC.
Each group of stakeholders has a unique perspective and store of knowledge and experience of the network infrastructure that help guide a successful IMC deployment. The most obvious example is the network engineering team who can provide network diagrams, and device model and series information for network devices. They also should participate in the decisions regarding which traps or Syslog events from network devices should be escalated to alarms and which traps should be filtered. They should also provide input into alarm thresholds and frequency of alerting. For organizations that do in-house application development, QA teams can be a resource for information on application environments as well as what services, systems, and devices should be monitored and what the device and application dependencies are. Also, they can help guide alarm threshold definitions.

Identifying stakeholder needs

The requirements for most stakeholders can be reduced to two basic needs: visibility and access. Visibility is the ability to see into the network infrastructure; to see into the devices, resources, links, and systems that constitute it; and the ability to see how well the network is performing and meeting the organization’s needs. Delivering visibility to stakeholders is accomplished by collecting data from network resources, analyzing it, and presenting it in various formats. In addition, some if not all stakeholders need access to IMC to configure or manage devices and to obtain data.

Common data requirements

Use the following questions as a starting point for developing your own process and set of questions for gathering requirements from those people in your organization who use or benefit by IMC.

1. What Data is needed?
   - What are the devices, resources, or systems that constitute the services that the stakeholders are responsible for?
     The list of devices, resources, systems that a stakeholder offers provide you with two key pieces of information: 1) the list of resources to monitor; and 2) the vendor, series, and model information you need to research to determine what metrics or data is available and therefore what data you can collect from every device.
   - What are the key metrics or performance indicators that the stakeholders use to measure the effectiveness of the services they are responsible for delivering?
     The list of key metrics or performance indicators that a stakeholder offers provide you with several key pieces of information: 1) how the stakeholder measures success; 2) what the stakeholder needs in terms of data to measure success; and 3) if the information that the stakeholder needs can or cannot be met by the data collected by IMC from the devices, services, or systems that constitute the service the stakeholder delivers.
   - What are the quantifiable targets or goals that the stakeholders have set for delivering on their service commitments?
     The list of goals that a stakeholder defines enables you to align with the stakeholder’s needs and use IMC to meet the organization’s needs and goals. In addition, this information helps define threshold settings for alarms and monitoring requirements.
   - What baseline data do the stakeholders have for measuring their targets and goals against?
     Having baseline data enables you to measure the effect that IMC has had on supporting the realization of the organization’s goals and aligning IT with business objectives.

2. For What Timeframe?
Is the data for alarming purposes? Is the data needed in near real time? If so, what are the service level commitments for performance, outage duration, or service availability? How long can the organization wait before being notified of a problem or outage?

These questions identify some of the monitoring requirements for fault or event management. Fault management identifies current failures or problems that need immediate attention. The collection and processing of data and event notification for fault monitoring need to align with the service level commitments that stakeholders make. For example, a service level commitment of 99.999% network reachability translates into about five minutes of network outage per year. Therefore, the polling interval used for monitoring for reachability must be significantly less than five minutes in order to support the achievement of this service level commitment.

Is historical reporting required? If so, in what areas is historical reporting needed? On resource performance? On faults or events in the network? On device configurations and changes to configurations? On network assets and changes to network assets? On security events? On access to IMC and changes to IMC?

These questions identify in what areas historical reporting is needed. Historical reporting can encompass everything from network and performance management to asset, configuration, change, incident, problem, and service level management. In fact, most groups require some form of historical reporting and the key is to provide stakeholders with reports targeted to meet their needs.

What level of data granularity is needed? How much summarization is needed? For how long does data need to be retained?

The first question can be translated to how frequently data must be polled from the devices, a key requirement as it defines how you configure polling in IMC. How many data samples does the stakeholder need to reliably measure for their key performance indicators? Once you have this information, you can evaluate the load that polling places on 1) the resources being monitored; 2) the network resource and bandwidth consumption that monitoring introduces; and 3) the processing and storage load that places on IMC. Ultimately, this involves finding a balance between stakeholder needs and network and IMC resource consumption.

Data retention and summarization requirements vary for different stakeholders. The on-call network operations team usually requires data retention with less summarization, typically one day to one week of data retention. Less summarization or more granularity is needed for network operations teams as they are most closely focused on pinpointing when, how, and why problems occurred. The data retention and summarization requirements of performance analysts whose time horizon may be up to one month or more fall in a mid-range. Capacity planner time horizons are much longer and may span five years and with much greater data summarization.

Data retention is another matter for asset, problem, incident, change and configuration management as both detail and summary reports are required. In such cases, data export options may be considered.

3. In What Format?

If the data is needed for alarming purposes, what method is used? Email or SMS text notifications? Console display of events and alarms? Integration with other management systems? Integration with Help Desk ticketing systems?

The format and method for the delivery of data varies considerably for stakeholders. Operations teams needing data as quickly as possible rely on methods such as Email or SMS text messaging, console presentation or integration with other management systems for the quick delivery of data. Oftentimes, operations teams and NOCs use one or more of these methods and formats for data.

If the data is needed for historical reporting, what kinds of reports are needed? Tabular, graphical?
Historical reporting requirements typically focus more on how the data is presented. Understanding how your stakeholders want the data presented (bar charts, pie charts, scatter graphs, and tables) helps you meet their needs.

- Is export to raw data files required?

Many times stakeholders want raw data as they have their own systems for analyzing and presenting the data in ways most useful for them. Additionally, stakeholders may have data retention or polling requirements that extend beyond the scope or ability of IMC. Understanding the data requirements of your stakeholders enables you to know whether or not exporting data from IMC is the best option available for your stakeholders.

**Stakeholder access and configuration requirements**

In addition to the data that provides stakeholders with visibility into network resources and services, stakeholders also need access to IMC. Access may be needed for viewing purposes only, for configuring and managing devices, users, and services in IMC, or for the configuration and management of IMC itself. Understanding what levels of access are needed to IMC and the devices, users, and resources it manages helps you configure IMC to support stakeholder needs.

**Knowing your network infrastructure**

To deploy IMC successfully, you need to have a clear understanding of the network infrastructure that IMC monitors and manages.

**Knowing your network topology**

While IMC does auto discoveries, it relies on the accurate identification of seed IP addresses to begin the discovery process. Identifying those IP addresses that best serve as seed IP addresses to discover the whole of your network ensures a successful IMC deployment. Also, IMC can auto discover logical relationships in the network infrastructure and this influences how IMC identifies root and symptom alarms in its event deduplication and root cause analysis algorithms. If needed, you can make adjustments to the devices IMC defines as the core and access devices that determine how root and symptom alarms are identified. The network documentation that you need includes topology maps, IP addressing schemes, and information identifying areas of your network that require special attention. The topology maps you need should ideally include both physical and logical diagrams of the network. A logical map helps you understand the relationships between devices and verify the accuracy of the topology maps generated by IMC. Physical diagrams, including data center maps and details of individual wiring racks, support you in creating accurate data center topology maps in IMC.

Next you need current and accurate documentation on the IP address schemes used. IP address documentation should also include any areas in your infrastructure that have overlapping address spaces. In addition, this documentation should include any locations or devices on the network that use non-routable IP addresses.

The network documentation should also identify areas or zones in your network that have special access requirements. For example, many companies prefer to separate internal corporate user traffic from external customer traffic and use layers of firewalls to separate these zones. In addition, many corporations create zones within zones to create secure application environments for the web, application, and database tiers. Tiers and zones may have specific access requirements. Understanding the management system requirements is necessary to configure IMC to manage devices in those tiers and zones.
Knowing your device vendors, series, and models

IMC uses device vendor, series, and model information in the Configuration Center to determine whether or not configuration and software files can be successfully deployed to devices in the network. Knowing what you have and configuring this information when IMC cannot auto discover supports you in managing the complex task of device configuration and software and patch management.

Make a list of all of the vendors that provide the devices and resources that are the building blocks of your network. In addition, gather the device series and model information for every unique device type in your environment. Take the output of an asset inventory for your network and combine it with the device vendor, model, and series information you have gathered so that you have clear and comprehensive details for all devices in your network. Comparing asset inventories to IMC’s database of devices provides a gap analysis of what you have versus what IMC knows about your network.

Identifying device vendor, series, and model information enables you to more easily identify and research vendor specific enterprise MIBs that contain objects, including traps, for customized and optimized monitoring of devices. Once you have identified the MIB objects you want to poll for, you can create user-defined global index monitors that you can apply to all devices of the same vendor series and model type. Once you have identified the traps you want to process, you can create user-defined trap definitions and apply them to all devices of the same type.

Having concise, usable, and consistently applied device naming standards simplifies IMC administration and use. IMC uses the MIB-2 object sysName, the administratively assigned name for a managed device, as the Device Label or name in IMC unless an IMC administrator or operator configures a custom Device Label.

Knowing access requirements and standards of your organization

The two aspects to access to consider in the planning stages of an IMC deployment are:

- Access requirements for your organization and restrictions for IMC to manage devices
- Requirements for providing operators with access to IMC

IMC uses several methods to manage devices. First, IMC uses SNMP (v1, v2c, or v3) to poll devices for management and monitoring data and also to receive SNMP traps from devices for proactive notification of events on managed devices. Second, IMC uses ping or ICMP requests for status polling and reachability statistics for devices managed by it. IMC also uses Telnet or SSH to manage devices.

You need to understand your organization’s policy on the use of SNMP, ICMP, Telnet, and SSH in the various zones and application tiers in your network in order to use IMC to manage devices in them. In addition, IMC uses TCP and UDP ports to communicate with other IMC servers and modules and understanding your organization’s policy on permitting this traffic facilitates a successful implementation.

You need to work with the teams that manage access control lists and firewall rules to ensure that SNMP, ICMP, Telnet, and SSH traffic are permitted for all networks, zones, and application tiers that have resources you want to manage. In addition, you need to ensure that the TCP and UDP ports that IMC uses to communicate with other servers and modules are also permitted. Alternatively, your organization may have a management VLAN or subnet dedicated to management systems for which this traffic is permitted for devices in the VLAN or subnet. If your organization has such a VLAN or subnet, be sure to locate the IMC servers in this VLAN or subnet.

To manage a device using SNMP, Telnet, and SSH, you need to configure the device to support these protocols. For SNMP, this requires enabling SNMP on every managed device, using the version of SNMP your organization mandates. It also requires configuring the device to forward SNMP traps to IMC if you
have designated IMC as the device to process and display SNMP traps. You need to configure IMC with the
SNMP configuration information that allows it to both SNMP poll devices as well as to receive SNMP traps
from managed devices. Use the SNMP templates feature to configure IMC for all devices that are monitored
and managed using SNMP. You can configure IMC to receive traps from devices when the devices are
auto-discovered or added to IMC.

With Telnet and SSH, you need to configure every device to enable Telnet and/or SSH sessions to it. See the
vendor documentation for instructions. You also need to configure IMC with the Telnet or SSH configuration
information in order for IMC to establish a session with a managed device. You can use Telnet and SSH
templates to simplify the process of adding device specific Telnet and SSH configuration information to IMC.
Some features in IMC require a Telnet or SSH application on the operator’s local computer. IMC can use the
native Telnet and SSH clients that most operating systems provide. Check with your organization’s
requirements regarding the use of Telnet or SSH for secure access to managed devices.

Identifying security policies and restrictions for monitoring

To successfully deploy IMC, you must identify the various zones and application tiers in your network and
what the access policies are for each of them. Is ICMP, SNMP, Telnet, and SSH traffic permitted to and from
each one of these zones that contains one or more devices you want to manage and the VLANs or subnets
that IMC resides on? Or, what is required to permit ICMP, SNMP, Telnet, and SSH traffic to these zones and
tiers?

You need to configure the version of SNMP that is mandated by your organization on each device to be
managed using SNMP. This SNMP configuration on the device must match the SNMP configuration for the
device in IMC.

You need to identify your organization’s requirements for the use of Telnet or SSH for managed devices and
configure each device and IMC accordingly.

Identifying your organization’s password requirements for SNMP community strings, Telnet, and SSH
passwords as well as IMC operator accounts enables you to configure IMC to meet those requirements.

Identifying the integration requirements and
opportunities

IMC may not be the only management system in your infrastructure. Consider the following questions to
determine how to accomplish integration:

• Is IMC the destination for events and alarms generated by IMC as well as by other management
  systems?
• Is IMC the repository and console for SNMP traps and Syslog events?
• Does your organization have a manager of IMCs or other system that processes events from many
  management systems?
• Does your organization have a help desk to which events and alarms should be forwarded?

Translating requirements into actions

The first step in a successful deployment is gathering requirements. The next step is translating requirements
into actions, which vary by organization.

The following lists provide some ideas for configuring IMC:
Compiling information

- Compile a list of vendors that include vendor contact information.
- Compile a list of vendor series information for all unique device series.
- Compile a list of vendor model information for all unique device models.
- Identify what metrics collected by IMC can be translated into key metrics or performance indicators to meet stakeholder requirements. Do any of the metrics require enterprise MIBs that need to be compiled into IMC? New user-defined global monitors created?
- Obtain MIBs to compile into IMC to support additional fault and performance monitoring.
- Compile MIBs into IMC.
- Compile a list of devices that includes the following information for each device:
  - Vendor
  - Series Name
  - Model Name
  - SNMP Settings
  - Telnet Parameters
  - SSH Parameters
  - Default or Custom status polling requirements
  - Default or Custom configuration polling requirements
  - Default or Custom performance monitoring requirements
  - List of services running on the device that require monitoring
  - Management IP Address
  - Identify people that require access for viewing or managing the device.
  - Identify recipients of email or text notifications for alarms for this device.
  - Identify device groups to which this device should belong.
  - Identify custom views to which this device should belong.

Network infrastructure

- Work with your organization’s network, security, and change control teams to implement network management VLANs and to permit traffic between IMC and all devices managed by IMC for all zones and tiers in application environments.
- Make or request changes to device naming conventions to simplify and standardize naming between IMC and the physical devices.

Event and performance management

- Verify that IMC’s system-defined trap and Syslog definitions capture all events and escalate events to alarms for devices as defined by the requirements you have gathered.
- Verify that IMC’s system defined trap and Syslog filters eliminate unwanted events as needed.
- Configure user-defined trap and Syslog definitions and configure to escalate to alarms as needed to meet requirements.
- Configure user-defined trap and Syslog filters to eliminate unwanted events.
- Create user-defined global monitors to meet stakeholder requirements for monitoring performance and reporting.
• Customize as needed the default set of monitor indices before adding devices to IMC so that once devices are added the default set of monitors are applied.
• Define performance monitoring thresholds for global monitors that map to key metrics for devices as needed or that notify operators of degraded conditions.
• Configure status and configuration polling intervals for devices to map to key metrics and service level commitments.
• Configure email, SMS, and alarm forwarding to other management systems based on requirements.
• Identify custom reporting requirements for faults, performance, configuration, change, security, and asset management.
• Configure Data Export based on data export and retention requirements.

Groups and views
• Define operator groups based on stakeholder requirements for access to IMC feature and devices, users, and services managed by IMC.
• Create device, user, and service groups based on stakeholder requirements for device access and management requirements.
• Create custom views based on stakeholder requirements for access to devices.
• Add vendor, device series, device category, and device model information.

Device access
• Create an SNMP template for every unique SNMP configuration.
• Create a Telnet template for every unique Telnet configuration.
• Create an SSH template for every unique SSH configuration.
• Create an SOAP template for Virtual Network Manager to manage virtual network devices.
• Create a WMI template for Virtual Network Manager to manage virtual network devices.
• Create a PowerShell template for Virtual Network Manager to manage virtual network devices.

System configuration
• Configure the transfer mode option for configuration center for transferring software and configuration files.

Adding devices
• Compile a list of seed IP addresses that allows you to streamline the discovery process.
• Develop a strategy for adding devices to the network using one or more of IMC’s auto discovery methods.
• Auto discover devices using one or more methods as needed and include in the configuration the ability to automatically register IMC to receive SNMP traps from supported devices for all devices configured to send SNMP traps to IMC.
• Add devices manually that cannot or were not auto discovered and include in the configuration the ability to automatically register IMC to receive SNMP traps from supported devices for all devices configured to send SNMP traps to IMC.
• Add devices to device groups and custom views based on information gathered.
• Add device vendor, series, category, and model information to devices manually added or to devices for which this information could not be discovered automatically.
• Using physical maps, create data center maps for dynamic data center mapping.
• Use the IP address scheme documentation to document the allocation of IP addresses in IMC.
• Map IP to Mac addresses and MAC addresses to interfaces as needed.
• Configure Asset Manager to collect asset information based on stakeholder requirements.
• Configure configuration backups and configuration checks as dictated by requirements.
• Configure performance views to meet historical reporting requirements for chart type and metrics.
• Configure My Real Time Reports as needed to meet reporting requirements.
• Apply configuration and software baselines to all devices.
• Disable status polling for devices that cannot be pinged.

Access to IMC

• Create operator accounts based on requirements gathered for operator access to devices and IMC services and features.
• Configure a password strategy in IMC that aligns IMC passwords with organizational policies on passwords.
• Configure IMC to use an existing LDAP system for password authentication if your organization uses LDAP.
• Restrict operator access to IMC as needed by configuring login control templates.
3 Exploring the IMC interface

IMC provides unified visibility for all IMC features, services and components via a single web portal. This web portal offers a common launch point for all installed IMC base and add-on modules.

IMC administrators use this web portal for configuring all IMC settings and functions. Network infrastructure engineers, administrators, and managers will use the web portal for performing tasks from viewing and managing network user activity to configuring devices and viewing their current status and performance.

Standard IMC supports access to IMC resources from mobile clients. It allows you to view faulty device and interface information, query specific device information, view alarm information, perform device reachability test (ping), view custom views and device views, and log in to IMC through the browser on a mobile client. IMC supports the Android and iPhone clients.

In this chapter, we will explore the IMC web interface. We will also explore IMC’s context sensitive online help. The online help system provides help for each window as well as system-wide help.

IMC also provides administrators with the ability to customize IMC to meet their individual needs. We will explore how to customize the IMC interface to meet individual administrator needs.

Logging into IMC

To log into IMC:

1. Enter the URL for the IMC server in your browser, including the port number for IMC.
   - http://servername:portnumber/imc
   - https://servername:portnumber/imc
   Where server name is the name of the IMC server and port number is the TCP port assigned to IMC during installation.
   Alternatively, you can use the IP address of the server in lieu of the server name.

2. Enter the user ID assigned to you in the Operator field.

3. Enter your password in the Password field.

4. Click Login or press Enter.

Exploring the IMC home page

The IMC home page displays information in a hierarchical way. It comprises two layers, space and widget. If you log in to the IMC for the first time, you can see the default space, which comprises six widgets displaying the alarm, resource, and performance summary information of the IMC, as shown in Figure 2 (page 30).

IMC’s modules also offer a variety of widgets in order to meet your viewing and monitoring needs. You can customize a space and add system-defined alarm, resource, performance, and other modules’ widgets to your space. In addition, you can customize RSS widgets, which provide you with the ability to subscribe to the RSS feeds.
For the default space displayed on your first login to the IMC home page, no data is available for any widgets. After you add devices to IMC, the system generates statistics immediately and displays them in the default space.

Basic operations on the IMC home page

On the IMC home page, you can perform basic operations on the spaces and widgets.

Freezing/Unfreezing a space tab

1. Move the pointer over the icon on the top left corner of the default space, and the icon changes to .

2. To freeze the space tab, click . Then the icon changes to , and a tab bar and function links appear on the top of the space, as shown in Figure 3.

   The name of the default space is Welcome.

3. To unfreeze the space tab, click .

   Then the tab bar and function links of the space are hidden. The space tab and relevant links are shown in Figure 3 (page 31).
Adding a space

1. Click of the space tab, and a new space tab named “New Space” appears.
2. Type the name for the new space, and click any blank part of the page to complete naming the space.

Renaming a space

- To rename a space, click next to the space name on the space tab, and select Rename from the list, or
- Double click the space, type a new name for the space, and click any blank part of the page to complete renaming the space.

Switching between spaces

To switch between spaces, click the relevant space tabs.

Saving a space

To save current space, click on the top right corner of the space.

If no modification is made for the current space, is displayed in gray. You do not need to save the space.

Deleting a space

1. Click next to the space name on the space tab.
2. Select Delete from the list.
3. Confirm your operation.

You cannot delete the default space Welcome.

Adding new widgets to a space

1. Launch the dialog box for adding widgets by clicking on the top right corner of the space.

If no widget is contained in the space, is displayed in the middle of the space. You can launch the dialog box for adding widgets by clicking the button.

By default, the dialog box provides 13 types of resource, alarm, and performance statistics widgets defined by the system.
2. Select the layout for widgets:
   On the top middle of the widget adding dialog box, select a layout.
   - means two widgets are displayed per row. The left widget occupies 2/3 and the right occupies 1/3 of the row.
   - means two widgets are displayed per row. The left widget occupies 1/3 and the right occupies 2/3 of the row.
   - means two widgets are displayed per row, each occupying 1/2 of the row.
   - means three widgets are displayed per row, each occupying 1/3 of the row.

3. Locate a widget by using one of the following methods:
   - Query a widget
     On the top right corner of the dialog box, type the keyword of a widget name and click Query. All widgets matching the query criteria are displayed in the dialog box. The query supports fuzzy matching and is case-sensitive.
   - Sort widgets
     a. On the top left corner of the dialog box, select the All, Resource, Alarm and Performance tab to display all widgets, resource-related widgets, alarm-related widget, and performance-related widgets.
     b. On the bottom right corner of the page, click Previous or Next to display widgets on the previous or next pages.

   Use either method to display the desired widgets in the dialog box.

4. Click for a widget to add it to the space.
   Then changes to Succeeded, indicating the widget is added successfully.
   You can add up to 10 widgets to a space.

5. Click OK to complete the operations and return to the space.

**Changing the widget layout of a space**

1. Click Edit on the top right corner of the space to launch the widget dialog box.
   On the top middle of the widget dialog box, select a layout.
   - means two widgets are displayed per row. The left widget occupies 2/3 and the right occupies 1/3 of the row.
   - means two widgets are displayed per row. The left widget occupies 1/3 and the right occupies 2/3 of the row.
   - means two widgets are displayed per row, each occupying 1/2 of the row.
   - means three widgets are displayed per row, each occupying 1/3 of the row.

2. Click OK to complete the operations and return to the space.

**Expanding/Collapsing all widgets of a space**

- Click Expand All on the top right corner to expand all widgets of the current space, or
- Click Collapse All on the top right corner to collapse all widgets of the current space.

**Expanding/Collapsing a widget of the space**

- Click Restore on the top left corner of a widget to expand it, or
• Click Minimize on the top left corner of a widget to collapse it.

**Dragging and dropping a widget**

1. Move the pointer over the name bar of a widget.
2. When the cursor becomes a black cross, drag and drop the name bar to place the widget to the desired position.

**Maximizing a widget**

1. To maximize a specific widget, click Maximize on the top right corner of the widget.
2. To return the widget to its original widow size, click Restore on the top left corner of the widget.

**Displaying a widget in a new window**

To display a widget in a new window, click New Window on the top right corner of the widget.

**Refreshing a widget manually**

To refresh a widget, click Refresh on the top right corner of the widget.

**Setting the refresh interval**

1. Click the Setting icon on the top right corner of the widget to launch the Setting dialog box. If other parameters are required for the widget, two options, Setting and Refresh Interval, are provided.
2. Click Refresh interval to enter the refresh interval setting window.
   - If no other parameters are required for the widget, the Setting dialog box appears. The available options include No Refresh, 1, 5, 10, and 30, in minutes.
3. Select a refresh interval, and click OK.

**Deleting a widget from the space**

To delete a widget, click Delete on the top right corner, and then confirm your operation.

**Alarm, performance and resource widgets**

By default, IMC provides 13 types of resource, alarm and performance statistics widgets defined by the system.

**Alarm TopN**

By default, the Alarm TopN widget, shown in Figure 4 (page 34) displays top 5 devices generating the most alarms (the y-axis indicates the device type, and the x-axis indicates the alarm quantity). The content includes the device information (Device Label (IP) by default), alarm type, and the quantities of alarm.
The color of the alarm for each device reflects in real time. Color-coding of the severity or alarm level conforms to industry standards and is displayed in the list below:

- **Critical**
- **Major**
- ** Minor**
- **Warning**

Click the **Setting** icon on the top right corner of the widget and select **Setting** to launch the **Setting** dialog box.

- **Alarm Level**— Specifies for the alarm view which the alarm to be displayed. The available options include **Critical, Major and Higher, Minor and Higher, Warning and Higher**.
- **Alarm Statistics**— Specifies the quantities of device to be displayed for the **Alarm view**. The available options include **5, 10**.

**CPU utilization (%) – TopN**

By default, the CPU utilization table, shown in Figure 5 (page 35), displays the top 5 high-utilization CPUs within the last hour. The content includes the time range, device/slot that the CPU belongs, and the CPU utilization.
Click the Setting icon on the top right corner of the widget and select Setting to launch the Setting dialog box:

- **Time Range**—Specifies the time range for statistics collection. The available options include Last Hour, Today, Yesterday, This Week, Last Week, This Month, Last Month, This Year, and Last Year.
- **Top**—Specifies the number of monitoring instances for the widget. The available options include 5, 10, 20, and 30.

By default, CPU Utilization (%) - TopN widget is displayed on the Welcome space of the IMC home page.

**Memory utilization (%) – TopN**

By default, the memory utilization table, shown in Figure 6 (page 35), displays the top 5 high-utilization memories within the last hour. The content includes the time range, device/slot that the memory belongs, and the memory utilization.
Click the Setting icon on the top right corner of the widget and select Setting to launch the Setting dialog box:

- **Time Range**—Specifies the time range for statistics collection. The available options include Last Hour, Today, Yesterday, This Week, Last Week, This Month, Last Month, This Year, and Last Year.
- **Top**—Specifies the number of monitoring instances for the widget. The available options include 5, 10, 20, and 30.

By default, **Memory Utilization (%) – TopN** widget is displayed on the Welcome space of the IMC home page.

**Device response time (ms) – TopN**

By default, the device response time table, *Figure 7 (page 36)*, displays the top 5 devices with the longest response time within the last hour. The content includes the time range, device name and IP, and the response time.

*Figure 7 Device Response Time*

<table>
<thead>
<tr>
<th>Device Response Time (ms) - TopN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitor Index</td>
</tr>
<tr>
<td>Time Range</td>
</tr>
<tr>
<td>Top</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Device</th>
<th>Instance</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco(172.1.0.21)</td>
<td>[0]</td>
<td>15.633</td>
</tr>
<tr>
<td>S3100(172.2.0.2)</td>
<td>[0]</td>
<td>0.000</td>
</tr>
<tr>
<td>MSTP4_xiaopang(172.1.0.11)</td>
<td>[0]</td>
<td>6.400</td>
</tr>
<tr>
<td>70_Access_j(172.0.0.2)</td>
<td>[0]</td>
<td>5.333</td>
</tr>
<tr>
<td>08X04-SQL08-222(192.108.5.222)</td>
<td>[0]</td>
<td>3.200</td>
</tr>
</tbody>
</table>

Click the Setting icon on the top right corner of the widget and select Setting to launch the Setting dialog box:

- **Time Range**—Specifies the time range for statistics collection. The available options include Last Hour, Today, Yesterday, This Week, Last Week, This Month, Last Month, This Year, and Last Year.
- **Top**—Specifies the number of devices for the widget. The available options include 5, 10, 20, and 30.

By default, **Device Response Time (ms) – TopN** widget is displayed on the Welcome space of the IMC home page.

**Device unreachability (%) – TopN**

By default, the device unreachability table, *Figure 8 (page 37)*, displays the top 5 devices with the highest unreachability rate within the last hour. The content includes the time range, device name and IP, and the unreachability rate.
Click the **Setting** icon on the top right corner of the widget and select **Setting** to launch the **Setting** dialog box:

- **Time Range** — Specifies the time range for statistics collection. The available options include Last Hour, Today, Yesterday, This Week, Last Week, This Month, Last Month, This Year, and Last Year.
- **Top** — Specifies the number of devices for the widget. The available options include 5, 10, 20, and 30.

By default, **Device Unreachability (%) – TopN** widget is displayed on the **Welcome** space of the IMC home page.

**Bandwidth utilization (In) (%) – TopN**

By default, the **Bandwidth Utilization (In) table**, Figure 9 (page 37), displays the top 5 devices with the highest inbound traffic bandwidth utilization within the last hour. The content includes the time range, device name, IP, and the Interface In-Bandwidth Usage.

**Figure 8 Device unreachability**

<table>
<thead>
<tr>
<th>Monitor Index</th>
<th>Device Unreachability Proportion (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time Range</td>
<td>Last Hour</td>
</tr>
</tbody>
</table>

| Top | 5 |

<table>
<thead>
<tr>
<th>Device</th>
<th>Instance</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>ar46-mp1(172.2.0.11)</td>
<td>[0.0]</td>
<td>0.000%</td>
</tr>
<tr>
<td>76_Access-si(172.6.0.2)</td>
<td>[0.0]</td>
<td>0.000%</td>
</tr>
<tr>
<td>6(172.6.0.180)</td>
<td>[0.0]</td>
<td>0.000%</td>
</tr>
<tr>
<td>172.2.0.30(172.2.0.30)</td>
<td>[0.0]</td>
<td>0.000%</td>
</tr>
<tr>
<td>126-ict(172.6.0.126)</td>
<td>[0.0]</td>
<td>0.000%</td>
</tr>
</tbody>
</table>

**Figure 9 Bandwidth utilization (In)**

<table>
<thead>
<tr>
<th>Monitor Index</th>
<th>Interface In-Bandwidth Usage (%) - Top 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time Range</td>
<td>Last Hour</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Device</th>
<th>Instance</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSTP4_xiapang(172.1.0.14)</td>
<td>[interface.Ethernet1/0/17]</td>
<td>0.293%</td>
</tr>
<tr>
<td>Nortel Switch (172.1.0.105)</td>
<td>[interface.Nortel Ethernet Routing Switch 5510-24T Module - Port 1]</td>
<td>0.005%</td>
</tr>
<tr>
<td>H3C(172.1.0.56)</td>
<td>[interface.GigabitEthernet1/0/1]</td>
<td>0.004%</td>
</tr>
<tr>
<td>MSTP1_xiapang(172.1.0.11)</td>
<td>[interface.GigabitEthernet2/0/24]</td>
<td>0.004%</td>
</tr>
<tr>
<td>MSTP3_xiapang(172.1.0.13)</td>
<td>[interface.Ethernet1/0/20]</td>
<td>0.003%</td>
</tr>
</tbody>
</table>
Click the Setting icon on the top right corner of the widget and select Setting to launch the Setting dialog box.

- **Time Range**—Specifies the time range for statistics collection. The available options include Last Hour, Today, Yesterday, This Week, Last Week, This Month, Last Month, This Year, and Last Year.
- **Top**— Specifies the number of devices for the widget. The available options include 5, 10, 20, and 30.

### Bandwidth utilization (Out) (%) – TopN

By default, the Bandwidth Utilization (Out) table, Figure 10 (page 38), displays the top 5 devices with the highest outbound traffic bandwidth utilization within the last hour. The content includes the time range, device name, IP, and the Interface Out-Bandwidth Usage.

**Figure 10 Bandwidth utilization (Out)**

<table>
<thead>
<tr>
<th>Monitor Index</th>
<th>Interface Out-Bandwidth Usage (%) - Top 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time Range</td>
<td>Last Hour</td>
</tr>
<tr>
<td>Device</td>
<td>Instance</td>
</tr>
<tr>
<td>MSTP4_xiapang4 (172.1.0.14)</td>
<td>[interface.Ethernet1/0/17] 0.034%</td>
</tr>
<tr>
<td>H3C(172.3.0.2)</td>
<td>[interface.GigabitEthernet1/0/12] 0.011%</td>
</tr>
<tr>
<td>H3C(172.3.0.2)</td>
<td>[interface.GigabitEthernet1/0/15] 0.010%</td>
</tr>
<tr>
<td>MSTP4_xiapang4 (172.1.0.14)</td>
<td>[interface.Ethernet1/0/24] 0.004%</td>
</tr>
<tr>
<td>Nortel Switch (172.1.0.105)</td>
<td>[interface.Nortel Ethernet Routing Switch 5510-24T Module - Port 1] 0.004%</td>
</tr>
</tbody>
</table>

Click the Setting icon on the top right corner of the widget and select Setting to launch the Setting dialog box.

- **Time Range**—Specifies the time range for statistics collection. The available options include Last Hour, Today, Yesterday, This Week, Last Week, This Month, Last Month, This Year, and Last Year.
- **Top**— Specifies the number of devices for the widget. The available options include 5, 10, 20, and 30.

### Customize TopN

By default, the Customize TopN widget, shown in Figure 11 (page 39), displays the CPU utilization (%) TopN view, which displays the top 5 highest-utilization CPUs within the last hour. The content includes the time range, device information (Device Label (IP) by default), Instance, and Data.
Figure 11 Customize TopN

Click the Setting icon on the top right corner of the widget and select Setting to launch the Setting dialog box.

- **Monitor Index** — Specifies the performance you want to monitor. The available options include CPU Usage (%), Memory Usage (%), Response Time of Device (ms), Device Unreachability Proportion (%), IP Datagram Receiving Rate (datagrams/s), IP Datagram Forwarding Rate (datagrams/s), Discarded Proportion of input Datagrams, Discarded Proportion of output IP Datagrams, Interface Receiving Rate (bits/s), Interface Transmitting Rate (bits/s), Interface In-Bandwidth Usage (%), Interface out-Bandwidth Usage (%), Interface Receiving Broadcasting Rate (package/s), Interface Transmitting Broadcasting Rate (package/s), Proportion of Receiving Packets Discarded (%), and Proportion of Sending Packets Discarded (%).

- **Time Range** — Specifies the time range for statistics collection. The available options include Last Hour, Today, Yesterday, This Week, Last Week, This Month, Last Month, This Year, and Last Year.

- **Top** — Specifies the number of devices for the widget. The available options include 5, 10, 20, and 30.

Network

The Network widget, shown in Figure 12 (page 39), displays the number of devices in different IP segments and custom views in the IMC.

Figure 12 Network

The color of the icon for each IP segment or custom view reflects in real time the most severe alarm or severity level of any device within the IP segment or custom view. Color-coding of the severity or alarm level conforms to industry standards and is displayed in the list below:

- Critical
These IP views provide drilldown to lists of all devices with their IP segments. To access these views, click the link of the IP segment.

These custom views provide drilldown to lists of all devices with their respective groups. To access these views, click the name of the custom view.

Click the Setting icon on the top right corner of the widget and select the Setting option to launch the Setting dialog box.

- **Columns**—Specifies the quantities of IP segments and custom views to be displayed per row for the widget. The available options include 2, 4, 6, 8, and 10.
- **Network**—Specifies the content to be displayed for the widget. Select Both to display both IP view and custom view; select IP View to display only IP view; select Custom View to display only custom view.

By default, Network widget is displayed on the Welcome space of the IMC home page.

For more information about the IP view and custom view, see "5 Resource management" (page 153).

**Device View**

As shown in Figure 13 (page 40), Device View involves two charts. The chart at the top displays the quantities of various devices in the current system (the y-axis indicates the device type, and the x-axis indicates the device quantity). The pie chart at the bottom displays the quantity and percentage of devices by their alarm status.

**Figure 13 Device View**
The color of the icon for each custom view reflects in real time the most severe alarm or severity level of any device within the custom view. Color-coding of the severity or alarm level conforms to industry standards and is displayed in the list below:

- Critical
- Major
- Minor
- Warning
- Normal
- Informational
- Unmanaged

By default, Device View widget is displayed on the Welcome space of the IMC home page.

**IP Topology**

The IP Topology widget, shown in Figure 14 (page 41), displays the IP view.

**Figure 14 IP Topology**

Click the Setting icon on the top right corner of the widget and select Setting to launch the Setting dialog box.

- **Subnet**—Specifies the subnet for which the topology is to be displayed. The available options include the existing subnets of the system.

You can use the following tools to view the custom view:

- Displays the network in its original proportion.
- Enables you to zoom in on the topology view.
- Enables you to zoom out on the topology view.
- Enables you to fit the contents of the topology view into the window.
Enables you to magnify the contents on the topology view. To exit magnify mode, click the icon again.

Provides a separate bird’s eye view window of the topology map.

Expands the topology view to full screen. To exit full screen mode, right-Click the topology view and select Exit Full Screen from the shortcut menu.

For more information about custom view, see "5 Resource management" (page 153).

Custom Topology

The Custom Topology widget, shown in Figure 15 (page 42), displays all custom views.

Figure 15 Custom Topology

Click the Setting icon on the top right corner of the widget and select the Setting to launch the Setting dialog box.

View—Specifies the custom view for which the topology is to be displayed. The available options include the existing custom views of the system.

You can use the following tools to view the custom view:

- Displays the network in its original proportion.
- Enables you to zoom in on the topology view.
- Enables you to zoom out on the topology view.
- Enables you to fit the contents of the topology view into the window.
- Enables you to magnify the contents on the topology view. To exit magnify mode, click on the icon again.
- Provides a separate bird’s eye view window of the topology map.
• • Expands the topology view to full screen. To exit full screen mode, right-click the topology view and select **Exit Full Screen** from the shortcut menu.

For more information about custom view, see "5 Resource management" (page 153).

**Port Group**

The **Port Group** widget, shown in Figure 16 (page 43), displays the port group list. You can click a port group name to view detailed port information.

**Figure 16 Port Group**

Click the **Setting** icon on the top right corner of the widget and select the **Setting** to launch the **Setting** dialog box.

- **Columns**—Specifies the quantities of IP segments and custom views to be displayed per row for the widget. The available options include 2, 4, 6, 8, and 10.

For more information about Port Group, see "5 Resource management" (page 153).

**Customizing spaces and system-defined widgets**

In addition to the default Welcome space defined by the system, you can customize a space and add widgets to your space as needed.

To customize a space and add widgets to your space:

1. Log in to the IMC, move the pointer over the **Space** icon on the top left corner of the space, and the **Space** icon changes to  
2. Click  to freeze the space tab. A tab bar appears on the top of the space.
3. Click  of the space tab, and a new space tab named “New Space” appears.
4. Type the name for the new space, and click any blank part of the page to complete naming the space.
5. Launch the dialog box for adding widgets by clicking  on the upper right corner of the space. By default, the dialog box provides system-defined alarm, resource, and performance widgets located under the **Widgets** tab.
6. Select the layout for widgets.

On the top middle of the widget adding dialog box, select a layout.

- ![Layout 1](image) means two widgets are displayed per row. The left widget occupies 2/3 and the right occupies 1/3 of the row.
- ![Layout 2](image) means two widgets are displayed per row. The left widget occupies 1/3 and the right occupies 2/3 of the row.
- ![Layout 3](image) means two widgets are displayed per row, each occupying 1/2 of the row.
- ![Layout 4](image) means three widgets are displayed per row, each occupying 1/3 of the row.
7. Locate a system-defined widget by using one of the following methods.
   o Query a widget
     Select the Widget tab in the dialog box. On the top right corner of the dialog box, type the keyword of a widget name and click Query. All widgets matching the query criteria are displayed in the dialog box. The query supports fuzzy matching and is case-sensitive.
   o Sort widgets
     Select the Widget tab in the dialog box. On the top left corner of the dialog box, select the All, Alarm, Performance, and Resource sub-tabs to display all widgets, alarm-related widgets, performance-related widgets, and resource-related widgets. On the bottom right corner of the page, click Previous or Next to display widgets on the previous or next pages.

Use either method to display the desired widgets in the dialog box.

8. Click the button of a widget to add it to the space. Then changes to Succeeded, indicating the widget is added successfully. You can add up to 10 widgets to a space.

7. Click OK to complete the operations and return to the space.

8. Click Setting on the top right corner of a widget and select Setting to launch the Setting dialog box:
   o Time Range—Specifies the time range for statistics collection. The available options include Last Hour, Today, Yesterday, This Week, Last Week, This Month, Last Month, This Year, and Last Year.
   o Top—Specifies the number of devices for the widget. The available options include 5, 10, 20, and 30.
   o Columns—Specifies the quantities of IP segments and custom views to be displayed per row for the widget. The available options include 2, 4, 6, 8, and 10. This parameter is available only for the Network widget.
   o Network—Specifies the content to be displayed for the widget. Select Both to display both IP view and custom view; select IP View to display only IP view; select Custom View to display only custom view. This parameter is available only for the Network widget.
   o Subnet—Specifies the subnet for which the topology is to be displayed. The available options include the existing subnets of the system. This parameter is available only for the IP Topology widget.
   o View—Specifies the custom view for which the topology is to be displayed. The available options include the existing custom views of the system. This parameter is available only for the Custom Topology widget.
   o Monitor Index—Specifies the performance you want to monitor. The available options include CPU Usage (%), Memory Usage (%), Response Time of Device (ms), Device Unreachability Proportion (%), IP Datagram Receiving Rate (datagrams/s), IP Datagram Forwarding Rate (datagrams/s), Discarded Proportion of input Datagrams, Discarded Proportion of output IP Datagrams, Interface Receiving Rate (bits/s), Interface Transmitting Rate (bits/s), Interface In-Bandwidth Usage (%), Interface out-Bandwidth Usage (%), Interface Receiving Broadcasting Rate (package/s), Interface Transmitting Broadcasting Rate (package/s), Proportion of Receiving Packets Discarded (%), Proportion of Sending Packets Discarded (%). This parameter is available only for the Customize TopN widget.
   o Alarm Level—Specifies for the alarm view which the alarm to be displayed. The available options include Critical, Major and Higher, Minor, and Higher, Warning and Higher. This parameter is available only for the Alarm widget.
   o Alarm Statistics—Specifies the quantities of device to be displayed for the Alarm view. The available options include 5, 10. This parameter is available only for the Alarm widget.
9. Click **OK** to confirm your changes.

10. Click **Save** on the top right corner of the space to save your configurations.

## Customizing RSS widgets

RSS widgets offer you the ability to subscribe to the RSS feeds. To customize RSS widgets:

1. Log in to IMC, move the pointer over the 🛒 icon on the top left corner of the space, and the 🛒 icon changes to 🛒.
2. Click 🛒 to freeze the space tab. Then a tab bar appears on the top of the space.
3. Click the tab you want to add the RSS widget to.
4. Launch the dialog box for adding widgets by clicking 🏢Edit on the upper right corner of the space.
5. Click the RSS tab in the dialog box to customize the RSS widget.
6. Enter the following RSS information:
   - **RSS Site**: Enter the URL of the RSS feed you want to subscribe.
   - **RSS Title**: Enter the name of the RSS widget.
7. Click the ✅Check button to test the validity of the RSS feed URL.
8. Click the ✨Add button to add another RSS widget.

## Device status via status bar

A summary of all alarms, shown in Figure 17 (page 46) is displayed on the IMC status bar located at the bottom of the Home page, as shown below. Click the icons for each severity or alarm level for drilling down into the alarms for each level.
Figure 17 Status bar

Alarm sound settings

IMC provides operators with the ability to customize the use of sound files for notifying them when new alarms are received or when existing alarms have not been cleared or recovered. Operators can use IMC system sound files or they can upload custom sound files. These sound files are then applied to severity or alarm levels.

To enable system-defined sound files for alarm levels:

1. Navigate to the Alarm Sound Setting dialog box by clicking the sound icon located in the lower left corner of the IMC home page. The Alarm Sound Setting dialog box appears.

2. Select when you want alarm sound files to play from the Sound Occasion Setting section of the Alarm Sound Setting dialog box.

3. Do one of the following:
   - If you want IMC to play sound files only when new alarms have been received, click the radio button to the left of When receiving new alarms, or
   - If you want IMC to play sound files when unrecovered alarms exist in IMC, click the radio button to the left of When existed unrecovered alarms.

You can configure IMC to play sound files for one or more alarm levels.

4. To select the alarm levels you want to play sound files for, click the checkbox to the left of the alarm level.
You can use the system sound files that are configured by default or you can choose which sound file you want to use for each alarm level.

5. To select a sound file you want to apply to an alarm level, click the **Select** button associated with the alarm level.

   The **Select Voice File** page appears.

6. Click the radio button ○ to the left of the sound file you want to apply.
7. Click **Select** to apply your sound file selection.
8. Click **Set** to apply your changes.
9. Click **Default** to restore the default sound settings.
10. Click **Close** to close the **Alarm Sound Setting** dialog box.

IMC supports the ability to add custom sound files to alarm sound notifications.

To enable custom sound files for alarm levels:

1. Navigate to the **Alarm Sound Setting** dialog box by clicking the sound icon 🎧 located in the lower left corner of the IMC home page.

   The **Alarm Sound Setting** dialog box appears.

2. Select when you want alarm sound files to play from the **Sound Occasion Setting** section of the **Alarm Sound Setting** dialog box.

3. Do one of the following:
   - If you want IMC to play sound files only when new alarms have been received, click the radio button ○ to the left of **When receiving new alarms**, or
   - If you want IMC to play sound files when unrecovered alarms exist in IMC, click the radio button ○ to the left of **When existed unrecovered alarms**.

4. Click **Voice File Manager** link located in the upper right corner of the **Alarm Sound Setting** dialog box.

   The **Upload Voice File** page appears.

5. Click **Browse** to browse your local directories for the sound file.
6. Click **Upload** to upload the selected sound file.
7. Verify that the **Upload Voice File** page indicates that the file was uploaded successfully.
8. Click **Back** to return to the **Alarm Sound Setting** dialog box.
9. Select the alarm levels you want to apply the custom sound file to by clicking the checkbox ☑ to the left of the alarm level.
10. Click the **Select** button associated with the alarm level you want to apply the custom sound file to.

   The **Select Voice File** page appears.

11. Click the radio button ○ to the left of the custom sound file you uploaded.
12. Click **Select** to apply your sound file selection and return to the **Alarm Sound Setting** dialog box.
13. Click **Set** to apply your changes.
14. Click **Default** to restore the default sound settings.
15. Click **Close** to close the **Alarm Sound Setting** dialog box.

   Sound files must be in PCM format (WAV) and the bit rate must be less than or equal to 352 kbps. The filename must include the .wav extension.

To disable sound files for alarm levels:
1. Navigate to the **Alarm Sound Setting** dialog box by clicking the sound icon located in the lower left corner of the IMC home page.
   The **Alarm Sound Setting** dialog box appears.

2. To remove sound settings, click the checked box to the left of the alarm level you want to disable sounds for.

3. Click **Set** to apply your changes.

4. Click **Close** to close the **Alarm Sound Setting** window.

5. Restart the browser for the sound setting changes to take effect.

### Navigating IMC functions

IMC provides you the following ways to navigate functions:

- After you log in to IMC, move the pointer over a tab on top of the page, and a list appears, as shown in **Figure 18** (page 48). Select the desired function to enter the relevant page.

- After you log in to IMC, click a tab on top of the page. After the page is refreshed, select the desired function from the left navigation tree to enter the relevant page, as shown in **Figure 19** (page 49).

**Figure 18 Tabular navigation**

![Tabular navigation](image)
The tabular navigation system includes the six functional areas of IMC: Resource (or performance) management, User management, Service management, Alarm (or fault) management, Report, and IMC System wide settings and configuration. All IMC features and functions can be found under these tabs.

The navigation tree located on the left of every IMC page contains context sensitive options that change as you navigate using the tabular navigation system. For example, if you click Resource from the tabular navigation system, the navigation tree on the left displays various features and functions under resource management including View Management, Resource Management, Terminal Access, Network Assets, Virtual Network Manager and Performance Management.

**Resource tab**

The Resource tab on the tabular navigation system displays the Resource Management page, shown in Figure 20 (page 49).

**Figure 20 Resource management page**
The main **Resource** page contains real time status views including:

- **Custom View Snapshot**—Real time status view for custom views
- **View Snapshot**—Real time status view by device type
- **Faulty Device List**—Real time status view of all devices reporting errors

In addition, the lower portion of the **Resource** page provides tabs for viewing real time performance statistics for a subset of devices for the last hour.

The navigation tree on the left includes the ability to navigate to various real time status views of the network infrastructure including:

- **Network Topology**—Provides a real time status view of the network infrastructure based on topology
- **Port Group**—Displays user-defined port group information.
- **Custom View**—Provides a real time status view of devices prioritized into custom views by the administrator or operator
- **IP View**—Provides a real time status view of the network infrastructure organized by IP address
- **Device View**—Provides a real time status view of the network infrastructure organized by device type

You can also manage perform configuration tasks using the navigation tree including:

- **Resource Management**—Manages resources within IMC including adding devices, device auto discovery, batch operations, and device/topology import and export.
- **Terminal Access**—Manages IP addresses including address allocation, binding, IP address location, discovery and device access.
- **Network Assets**—Implements network asset functions including asset audits and reporting.
- **Virtual Network Manager**—Manages the virtual network including servers, virtual switches, and virtual machines.
- **Performance Management**—Configures real time reports on device performance, including configuration of real time performance status reporting on the main **Resource** page.

**Topology Maps**

Topology maps available under the **Resource** tab have special navigation features.

- **Left Mouse Click**

A left mouse click with a node or link selected on the topology map, shown in Figure 21 (page 51), displays information about the selected node or link as shown below. To select a node or link, click the node or link using the left mouse button.
Right Mouse Click

A right mouse click with a node or link selected on the topology map, shown in Figure 22 (page 52), displays a list of information and configuration options that can be applied to the selected node or link, as shown below.
A right mouse click with nothing selected displays a menu for map configuration.
Resource Tab: Device Details

The Device Details page under the Resource tab also has special features. To access the Device Details page, click any active link in IMC that contains the device name/IP address.

The following section provides a high level overview of the Device Details page. For more detailed information about this page, see "Device details page" (page 212).

- Right Pane

The right pane of the Device Details page, shown in Figure 23 (page 53), contains many information and configuration options that apply to the selected device while the navigation tree on the left offers configuration options for global settings.

Figure 23 Right pane

NOTE:

The figure above contains only a partial view of the navigation pane.

For more information on using features and functions under the Resource tab, see "5 Resource management" (page 153).

User tab

Users are resources on the network that both use and impact network infrastructure resources. To view and manage network user and their activity, click the User tab, shown in Figure 24 (page 54), located in the upper portion of the IMC interface. The views available under the User tab depend on the installation of user management modules (for example, Guest Access Manager and User Access Manager).
The main User page contains real time status views of user activity including:

- **24-Hour Online History**—Shows the number of secure, insecure, and unknown users on the network.
- **Realtime Statistical Chart for Online Users**—Shows a statistical view of the number of secure, insecure and unknown users in real time.
- **24-Hour Security History**—Shows the number of users that are in breach of security policies for patches, virus protection, unsanctioned software, and other security violations.
- **Security Chart of the Day**—Displays security threats and attacks based on IMC’s security log.
- **Top10 User Groups by Online Count**—Displays the top 10 groups with the most online users. The groups have been configured by the IMC administrator or operator.

The navigation tree on the left includes configuration options for:

- **User Management**—Gives you the ability to add, delete, modify platform users and change their group assignments, search for users, add supplemental information to user profiles, import users, and delete users in individual or batch mode.
- **Access User View**—Allows you to manage the access account associated with the platform user.
- **Guest Management**—Allows you to manage the guest accounts provided by IMC UAM.
- **Guest Access Manager**—Allows you to manage the guest accounts provided by IMC Platform.

Guest Management is similar to Guest Access Manager. They are independent of each other. Guest Access Management requires only the installation of the IMC Platform. Guest Management requires the installation of both the IMC Platform and IMC UAM.

**Service tab**

Management of network infrastructure services can be accessed by clicking the Service tab, shown in Figure 25 (page 55), in the tabular navigation system.
The Service page serves as a portal for you to access all of the service modules that together constitute the IMC system. This includes modules for the base IMC system:

- **Security Control Center**
- **Configuration Center**
- **ACL Management**
- **VLAN Management**

For more information on using the services listed above, refer to the sections of this manual that correspond with these modules.

The Service page also serves as a portal for add-on modules that support you in managing and maintaining more functions of network infrastructure management including:

- **User Access Manager**
- **EAD Security Policy Manager**
- **Desktop Asset Manager**
- **Wireless Service Management**
- **Voice Service Manager**
- **MPLS TE**
- **MPLS VPN Manager**
- **VPLS**
- **Traffic Analysis**
- **User Behavior Auditor Management**

Icons for the aforementioned service modules appear under the Service tab after a successful installation of each module has been completed.

For more information on these modules and their use, please refer to the user guides for the corresponding service module.

**Alarm tab**

The real time event or fault management features of IMC can be accessed by clicking the Alarm tab, shown in Figure 26 (page 56), of the tabular navigation system.
The **Alarm** tab is IMC’s portal into the reporting of faults on the network infrastructure. IMC lists real time alarms or faults, sorted by most recent in the main portion of the **Alarm** page.

From this page, you can drill down into individual alarm details by clicking the **Description** field of an individual alarm.

You can also quickly access the device in alarm mode by clicking the **Alarm Source** of an individual alarm. This navigates the operator to **Device Details** for the device in alarm mode.

The navigation tree has the following configuration and viewing options:

- **Real-Time Alarms**—View, delete, and recover the recent 50 unrecovered alarms with the exception of information alarms.
- **Root Alarms**—View, delete, and recover the most recent important alarms with the exception of information alarms.
- **All Alarms**—View all alarms.
- **Faulty Devices**—View devices grouped by device type that are currently reporting a fault or error.
- **Alarm Statistics**—View statistical analysis of alarm distribution in real time.
- **TopN**—View devices grouped by severity of alarm.

The navigation tree also has the following configuration and viewing options:

- **Alarm Settings**—Configure alarm settings to include email and SMS notification, alarm forwarding to IMC as well as to other management systems, and downstream alarm suppression.
- **Trap Management**—Browse, filter traps, add and modify trap definitions within IMC.
- **Syslog Management**—Browse, filter and configure Syslog events.

For more information on using features and functions under the **Alarm** tab, see "8 Event and alarm management" (page 525).

**Report tab**

Real time and historical reports in IMC can be accessed by clicking the **Report** tab, shown in Figure 27 (page 57), of the tabular navigation system.
From the **Report** tab, you can access real time and historical reports. The main pane in the **Report** tab provides a listing of all configured **Real Time** reports.

From this pane, you can also add quick reports and schedule reports as well as delete reports.

From the navigation tree on the left, you can customize reports, add report templates, and schedule reports.

For more information on using features and functions under the **Report** tab, see “13 Reporting in IMC” (page 849).

**System tab**

System-wide configuration options and system level functions can be accessed by clicking the **System** tab, shown in Figure 28 (page 58), of the tabular navigation system located in the upper portion of the IMC interface.
You can configure system wide resources and settings including:

- **Resource Management**—Configures IMC to manage devices globally by configuring templates for SNMP, Telnet, SSH, SOAP, PowerShell, and WMI access. Manage devices through vendor, series, model and category definitions and MIB management.

- **Operator Management**—Manages access to IMC via operator accounts and groups; and manage IMC access through login controls and password strategies.

- **Group Management**—Manages IMC device groups, user groups and service groups.

- **Hierarchical NMS**—Manages the flow of data and alarms through IMC’s hierarchical alarm settings.

- **System Configuration**—Configures IMC system parameters, log details, data export, alarm and performance monitoring, SMS configuration, and mail server settings.

- **Data Analysis Management**—Analyzes the data collected by IMC and provides the analysis results to each IMC module. Typically it is not configured or operated by administrators and operators.

The navigation tree on the left for the **System** tab provides a shortcut to all system functions provided in the **System** tab.

For more information on using features and functions under the **System** tab, see "4 Configuring IMC for use" (page 73).
Quick Start

You can see a Quick Start link in the left navigation tree of some IMC components. Quick Start briefly describes the functions of the modules and their relations within a component, and offers name links to the configuration pages.

Floating menus of the navigation tree

The IMC navigation tree provides floating menus, as shown in Figure 29 (page 59).

Figure 29 Floating menus of the navigation tree

The floating menu displays the secondary links of the link that your mouse pointer lies on, so that you can quickly locate and expand a functional link. Point to a link marked with the icon and the floating menu of the link appears. Click a link on the floating menu to navigate to the corresponding functional page.

Navigating IMC using breadcrumb trails

A breadcrumb trail, shown in Figure 30 (page 60), is a secondary navigation method that supports you in accessing more easily features and functions of the IMC system.

They are also an effective visual aid that displays the operator’s location within the context of IMC’s web interface.

This feature also offers you a great resource of contextual information for knowing where they are and moving more quickly to where they want to be.
The breadcrumb trail shown above indicates that the administrator or operator is in the switch view under View Management option on the Resource tab. The administrator or operator can quickly navigate back to the All Devices page by clicking on the All Devices link in the Breadcrumb trail.

The first value for the breadcrumb trail in the IMC interface is most often one of the functional areas of IMC that are denoted by the tabs in the tabular navigation system. Thus the starting points for any navigation in IMC are these tabs and their breadcrumb counterpart:

- **Resource** →
- **User** →
- **Service** →
- **Report** →
- **System** →

The breadcrumb under Alarm tab is not started with Alarm→ . It displays only the name of the function.

The breadcrumb for operator group management that can be found under the system tab would be System→Operator Group.

All features and functions within IMC can be found under one of these tabs. An overview of these functional areas is provided in the previous section of this chapter. The breadcrumb navigation convention used in IMC and described here is used throughout the IMC manuals to describe the navigation path for IMC features and functions.

⚠️ **WARNING:**

IMC’s online help system also employs breadcrumb trails to support you in effectively and quickly navigating it.
Online help system

IMC offers two levels of online help, system wide help and context sensitive help.

System-wide help

System-wide help can be accessed by clicking the Help link, shown in Figure 31 (page 61), located in the upper right corner of the IMC page.

Figure 31 Help link

Clicking this link displays the main help page, shown in Figure 32 (page 62), with help organized by functional groups within IMC.
The main pain of the system-wide help includes useful resources for managing and using IMC. These resources include an overview of the IMC platform, a quick start guide, managing resources within IMC and more.

On the navigation tree located on the left of the Help page, help is organized by functional groups within IMC.

**Searching IMC system online help**

Operators can query the online help system using the **Search** field located at the upper left corner of the Help page by entering search criteria in the field provided. Results of the search query are displayed in the left pane of the IMC interface.

**Context sensitive help**

Context sensitive help can be accessed by clicking on the **Help** link located in the upper right corner of the main pane of IMC functional pages, shown in Figure 33 (page 63). The help system displays online help relevant to the operator’s current page.

The context sensitive help link is located below the system wide help link.
Global search

Global search includes basic query and advanced query. Basic query helps you search devices and users. Advanced query helps you search devices, interfaces, and users.

Performing a basic device search

To perform a basic device search:

1. Navigate to basic query.
   
   The basic query field can be found in the upper right corner of most IMC pages.

2. Select the Query Devices option from the list by clicking the search icon located to the left of the search field.

   IMC supports fuzzy matching for most search and filtering features.

3. Enter a full or partial device name or IP address in the field provided.

4. Click Go.

   All devices matching the specified criteria are displayed on the Device List.

5. Click Export Excel or Export CSV on the right of Device List to launch the Download Exported Data window, and click the Download Exported Data link to export the query result in the format of Excel or CSV.
Performing a basic user search

To perform a basic user search:
1. Navigate to basic query.
   
   The basic query field can be found in the upper right corner of most IMC pages.
2. Select the option from the list by clicking the search icon located to the left of the search field.
   IMC supports fuzzy matching for most search and filtering features.
3. Enter a full or partial user name in the field provided.
4. Click Go.

Performing an advanced search for a device

To perform an advanced device search:
1. Navigate to the Advanced Query page.
2. Click the link located in the upper right corner of the IMC page.
3. Click the radio button to the left of Query Devices to perform a device search.
4. Enter the following information in the Advanced Query page:
   - Device Label—IMC supports fuzzy matching for this field. You can enter a partial or complete name for the devices you want to locate in the Device Label field.
   - Device IP—Enter the IP address of the device you want to search for in the Device IP field. Select Fuzzy from the list located to the right of the Device IP if you want to enter a partial IP address. Select Exact from this list if you want IMC to search for an exact match for the IP address you have entered.
   - MAC—Enter the MAC address of the device you want to search for in the MAC field. IMC supports fuzzy matching for this field. You can enter a partial or complete MAC address for the devices you want to locate.
   - Bridge MAC—Enter the MAC address for the Bridge device that you want to query for in the Bridge Mac field.
   - Device Category—Select the device category from the Device Category list.
   - Device Status—Select the device status from the Device Status list.
   - Device Series—Select the device series from the Device Series list.
   - Contact—Enter the contact name information you want to search by. IMC supports fuzzy matching for this field, allowing you to enter a partial or complete string for the contact in the Contact field.
   - Location—Enter the location information you want to search by. IMC supports fuzzy matching for this field, allowing you to enter a partial or complete string for location in the Location field.
5. Device Reachability—Select device reachability status from the Device Reachability list.
6. Click Query.

All devices matching the specified criteria are displayed on the Device List.
7. Click Export Excel or Export CSV on the right of Device List to launch the Download Exported Data window, and click the Download Exported Data link to export the query result in the format of Excel or CSV.

Performing an advanced search for an interface

To perform an advanced interface search:

1. Navigate to the Advanced Query page.
2. Click the Advanced link located in the upper right corner of the IMC page.
3. Click the radio button for Query Interfaces to perform search for interfaces.
4. Enter the following information in the Advanced Query page:
   - Interface Alias—IMC supports fuzzy matching for this field. You can enter a partial or complete name for the interface alias you want to locate in the Interface Alias field.
   - Interface Type—Select the interface type you want to search from the Interface Type list.
   - Speed—Select the interfaces speed from the Speed list.
   - Interface IP—Enter the IP address of the interface you want to search for in the Interface IP field. Select Fuzzy from the list located to the right of the Interface IP if you want to enter a partial IP address. Select Exact from this list if you want IMC to search for an exact match for the IP address you have entered.
   - MAC Address—Enter the MAC address of the interface you want to search for in the MAC Address field. IMC supports fuzzy matching for this field, allowing you to enter a partial or complete MAC address for the interfaces you want to locate.
   - Device Label—Enter a partial or complete name of the device to which the interface belongs in the Device Label field. IMC supports fuzzy matching for this field, allowing you to enter a partial or complete string for the device name.
   - Device IP—Enter the IP address of the device to which the interface belongs in the Device IP field. Select Fuzzy from the list located to the right of the Device IP if you want to enter a partial IP address. Select Exact from this list if you want IMC to search for an exact match for the IP address you have entered.
   - Management Status—Select the management status of the interfaces you want to search for from the Management Status list.
   - Operational Status—Select the operational status of the interfaces you want to search for from the Operational Status list.
5. Click Query.
6. Click Save as Filter to save the query criteria as a filter, which you can view in the Filter List. The filter can be used by port groups to filter interfaces.

For more information on filters, see "Managing filters to filter interfaces" (page 101).

Performing an advanced search for a user

To perform an advanced user search:

1. Navigate to the Advanced Query page.
2. Click the Advanced link located in the upper right corner of the IMC page.
3. Click the radio button for Query Users to perform a user search.
4. Enter the following information in the **Advanced Query** page:
   o **User Name**—Enter the user’s name in the **User Name** field. IMC supports fuzzy matching for this field. Therefore, you can enter a partial or complete string for the users you want to locate.
   o **Identity Number**—Enter the Identity number for the user you want to search for in the **Identity Number** field. IMC supports fuzzy matching for this field. Therefore, you can enter a partial or complete string for the identify number for the users you want to locate.
   o **Contact Address**—Enter the contact address information for the user in the **Contact Address** field. IMC supports fuzzy matching for this field. Therefore, you can enter a partial or complete string for the contact address for the users you want to locate.
   o **Telephone**—Enter the telephone number of the user in the **Telephone** field. IMC supports fuzzy matching for this field. Therefore, you can enter a partial or complete telephone number for the users you want to locate.
   o **Email**—Enter the email address of the user in the **Email** field. IMC supports fuzzy matching for this field. Therefore, you can enter a partial or complete email address for the users you want to locate.
   o **User Group**—Click the user group icon to select the group to which this user belongs.

5. Click **Expand All** to expand all groups.
6. Click the radio button to the left of the group you want to search by.
7. Click **OK**.
8. Click **Query**.

**Personalizing the IMC web interface**

You can customize IMC’s web page by storing favorites for quick access to often-used pages within IMC.

**Accessing a favorite**

To access a favorite:

1. Point to the **My Shortcut** link located at the top of the left navigation tree.
   A list of predefined and user defined favorites appears.
2. Point to the **My Favorites** folder option.
   The list of favorites that have configured is displayed in a popup list to the right.
3. Click the favorite you want to access.

**Adding a favorite**

To add a favorite:

1. Click the **Add to My Favorites** link located in the upper right corner of the main pane of most IMC pages.
2. Enter the new name of the favorite link in the **Name** field.
3. Click **OK** to confirm adding the link to my favorites.
4. Refresh or reload the page in your web browser to access the newly created favorite.
Modifying a favorite

To modify a favorite link:

1. Navigate to System→My Favorites.
2. Click the System tab from the tabular navigation system on the top.
3. Click System Configuration on the navigation tree on the left.
4. Click 🌟 My Favorites under System Configuration from the navigation system on the left. The Manage My Favorites list is displayed on the main page.
5. Click the icon located to the left of the folders and links displayed in Manage My Favorites list to expand the view to display all links under the selected folder.
6. Click the modify icon 📞 associated with the link you want to modify.
7. Enter the new name of the favorite link in the Name field.
8. Select the folder to which you want to move the link from the Folder list.
9. Click OK.
10. Click Refresh to refresh the Manage My Favorites list.

Sorting favorites

To change the display order of My Favorites links:

1. Navigate to System→My Favorites.
2. Click the System tab from the tabular navigation system on the top.
3. Click System Configuration on the navigation tree on the left.
4. Click 🌟 My Favorites under System Configuration from the navigation system on the left. The Manage My Favorites list is displayed on the main page.
5. Do one of the following:
   o Click the up arrow key icon ⬆️ associated with the link you want to move up one position, or
   o Click the up arrow key icon ⬆️ associated with the link you want to move to the top in the folder, or
   o Click the down arrow key icon ⬇️ associated with the link you want to move down one position, or
   o Click the down arrow key icon ⬇️ associated with the link you want to move to the bottom in the folder.

Deleting a favorite

To delete a favorite:

1. Navigate to System→My Favorites.
2. Click the System tab from the tabular navigation system on the top.
3. Click System Configuration on the navigation tree on the left.
4. Click 🌟 My Favorites under System Configuration from the navigation system on the left. The Manage My Favorites list is displayed on the main page.
5. Click the icon located to the left of the folders and links displayed in **Manage My Favorites** list to expand the view to display all links under the selected folder.

6. Click the delete icon in the **Manage My Favorites** list associated with the link you want to delete.

7. Click **OK** to confirm deletion of the selected link.

8. Click **Refresh** to refresh the **Manage My Favorites** list.

⚠️ **WARNING:**
If you delete a folder, all of its contents are also deleted. Once a folder has been deleted, it cannot be recovered.

---

**Wizard Center**

IMC provides a Wizard Center to configure common functions and third-party devices. You can enter the pages for configuring common functions through **Quick Start**, and enter the pages for configuring third-party devices through **Support third-party device**.

**Quick Start**

To enter the pages for configuring different functions through **Quick Start**:

1. Point to the **My Shortcut** link located at the top of the left navigation tree.
   A list of predefined and user-defined favorites appears.

2. Point to the **Wizard Center** folder option.

3. Click **Quick Start** in the popup list to the right.
   The **Quick Start** window, containing five pages, appears. You can click a page number to enter the target page. The following functions are available on the pages:
   - **Device access settings**
     - SNMP settings
     - Telnet settings
     - SSH settings
   - **Default performance monitor indexes**
     - Configure default performance monitor indexes
     - Configure performance monitor option
   - **Add device**
     - Auto discover device
     - Manually add device
   - **View and topology**
     - Add user-defined view and topology
     - Arrange topology elements and recover links
     - Add interface view
   - **Configuration backup**
     - Add auto backup plan
Modify backup policy option

**Custom home page**
Add new space and select interested widgets

4. To enter the next page, click 🔄.

5. To return to the previous page, click ←.

6. To enter the page for configuring a function, click the function name link.

7. To switch to the **Support third-party device** window, point to the ➕ link, and select **Support third-party device**.

**Support third-party device**

To enter the third-party device configuration page:

1. Point to the 🌍 **My Shortcut** link located at the top of the left navigation tree.
   A list of predefined and user-defined favorites appears.

2. Point to the 📁 **Wizard Center** folder option.

3. Click **Support third-party device** in the popup list to the right.
   The **Support third-party device** window, containing five pages, appears. You can click the page number to enter the target page. The following functions are available on the pages:

   **Register third-party device information**
   Add device vendor
   Add device series
   Add device model

   **Advanced alarm settings**
   Add trap events
   Import user-defined trap events from MIB file
   Escalate trap event to alarm

   **Advanced performance settings**
   Add performance index
   Display performance indexes in topology

   **Configuration management**
   Add telnet script

   **Compliance policy check**
   Add compliance policy
   Add check task

   **Customize device panel**
   Import third-part panels from device panel project files

4. To enter the next page, click 🔄.

5. To return to the previous page, click ←.

6. To enter the page for configuring a function, click the function name link.
7. To switch to the Quick Start window, point to the link, and select Quick Start.

Task Management

Task Management helps you easily view the status and execution result of tasks, and restore and suspend tasks. With the message delivery function, you can obtain task execution result and query message history.

Task Management supports ACL, iCC, General Config, Compliance, and VLAN.

Accessing Task Management

After you create the tasks for the components supported by Task Management, the tasks are displayed on the Task Management page. You can view the current status and execution result of each task, and restore or suspend specific tasks.

To access task management:

1. Point to the My Shortcut link located at the top of the left navigation tree.
   A list of predefined and user defined favorites appears.
2. Point to the Task Management folder option.
   The popup list appears.
3. Click Task Management in the popup list.
   The task management window appears.
   The window displays two properties by default.
4. Click on the top right corner to expand the window and display more properties.
5. Click the top of the window to display the next component.
6. Click the component name on the top of the window to enter the component task list.
   o Task Name—Displays the task name and creation time. Before a task name, ✅ means the task is executed successfully; ❌ means the task fails to be executed; ⬤ means the task is waiting to be executed or is being executed.
   o Status—Refers to the current task status, which can be Finished, Waiting for Execution, or Suspend. Finished means the task has been executed; Waiting for Execution means the task is waiting to be executed; Suspend means the tasks is suspended.
   o Execution Time—Displays the previous execution time.
   o Next Execution—Displays the next execution time.
   o Operation—Provides operations related to the task.
7. Depending on whether a task is waiting to be executed, suspended, or has been executed, select from the following:
   o If a task is waiting to be executed, ✤ is displayed in the Operation column. Click ✤ to suspend the task.
   o If a task is suspended, ✅ is displayed in the Operation column. Click ✅ to restore the task.
   o If a task has been executed, nothing is displayed in the Operation column.
8. If the Task list contains enough entries, the following navigational aids are displayed:
9. Enter part of a task name or a complete task name, and click Query to display matching tasks of the component on the task list.

10. Select a refresh interval, No Refresh, 1, 5, or 10, from the Refresh Interval (minutes) list. IMC then refreshes task status of all components at the specified interval.

Task Management displays only the following tasks:
- All periodical tasks.
- Tasks that start in 24 hours and have been executed.
- Tasks that start after 24 hours and have not been executed.

Message history

After you enable the message delivery function, Task Management sends task execution result messages to the administrator, and logs the event. You can view the message history through the Message History function.

To access message history:

1. Point to the My Shortcut link located at the top of the left navigation tree.
   A list of predefined and user defined favorites are displayed.

2. Point to the Task Management folder option.
   The popup list appears.

3. Click Message History in the popup list.
   The History Messages window appears.
   - Time: Displays the task execution time.
   - Message Type: Displays the task type, which can be iCC, ACL, VLAN, Generic Config, or Compliance.
   - Message: Indicate the summary information of the message.

If the Task list contains enough entries, the following navigational aids are displayed:

4. Select a message type from the Message Type list, and click Query.
   All matching entries are displayed.

Message options

To set message options:
1. Point to the **My Shortcut** link located at the top of the left navigation tree. A list of predefined and user defined favorites are displayed.

2. Point to the **Task Management** folder option. The popup list appears.

3. Click **Message Options** in the popup list to the right. The Push Settings window appears.

4. Select **Enable** or **Disable** from the **Enable Push** list.
   - If you select **Enable**, Task Management sends task execution result messages to the administrator.
   - If you select **Manual Close** from the **Message Display** list, you must manually close the message delivery window upon receiving a message.
   - If you select **Auto Close in 10 Seconds**, the message delivery window automatically closes in 10 seconds. This option takes effect when you enable the message delivery function.

5. Click **OK**.

**Logging out of IMC**

To log out of IMC:

1. Click **Logout** located in the upper right page of any IMC page.

2. Click **OK** when prompted to confirm logout.
4 Configuring IMC for use

Effective implementation and maintenance of IMC depends on pre-discovery planning and configuration. This chapter describes the functional areas of IMC that are most effectively used when configured and implemented prior to populating IMC with users, devices, and resources. In addition, the chapter includes basic IMC system-wide configuration and maintenance functions.

Securing IMC and access to managed resources

IMC offers you powerful control over network resources including network devices, network users, and services. Therefore, securing IMC is at the top of the list of priorities for configuring IMC for use. This section describes the security options available in IMC that secure its use, the access and control over resources it offers you, and the data IMC uses to manage resources. **Operator groups**: Operator groups enable you to assign or remove IMC management privileges by group. You can also create custom groups to further extend administrative control over access to IMC and the network resources managed by it. For configuring operator groups, see “Managing operator groups” (page 104).

**Operator roles**: You have the ability to assign various levels of rights to individual operator accounts with the ability to restrict access by views and groups. For configuring operator accounts, see “Managing IMC operators” (page 114).

**Login control templates**: You can permit or deny operator access to IMC by IP address. For configuring login control templates, see “Securing IMC through operator login control templates” (page 111).

**Integration with authentication services**: IMC supports secure access to IMC through integration with RADIUS and LDAP for operator authentication to IMC. For more information, see “Securing IMC access via authentication services” (page 108).

**Password strategy**: IMC enables you to define system-wide password requirements for all operators that have access to IMC. For configuring password strategies, see “Establishing IMC password strategies” (page 113).

**Online operators**: You can view current IMC access and activity through the Online Operators feature. Through this feature, you can log operators off as well as block access to IMC in real time. For more information on this feature, see “Managing online IMC operator access” (page 124).

**SNMP configuration**: For secure communications between IMC and managed devices, IMC supports SNMPv1, v2c and various forms of v3. In addition, IMC also supports global SNMP community string management for all managed devices once devices are configured to be managed by IMC. For configuring SNMP through templates, see “SNMP (page 74).

**Telnet and SSH device access**: IMC also supports remote device access through Telnet and SSH with the ability to use templates to configure Telnet and SSH settings. For configuring Telnet and SSH templates, see “Device access templates” (page 74).
Resource Management: managing network resources with global settings

IMC incorporates many services and features that enable you to easily and effectively manage global network resources.

Resource Management covers the configuration of templates and device vendor, series and model definitions that support you in easily managing access to network devices.

In addition, Resource Management also includes the configuration of filters, which are used by port groups to filter interfaces.

Device access templates

Device access templates enable you to save SNMP, Telnet, SSH, SOAP, PowerShell, and WMI configuration settings that IMC uses to access network devices. You can apply these templates when adding devices to IMC, performing auto discovery to populate IMC with newly discovered devices, or to configure device parameters in individual device or batch mode.

SNMP templates

IMC uses SNMP to query and manage remote network devices. The SNMP template feature allows you to save SNMP configuration settings in IMC, which can then be applied when adding new devices to IMC. SNMP templates store IMC’s SNMP configurations for devices to support IMC’s communication with the device. SNMP Templates do not configure the SNMP settings on the device itself.

This feature is particularly useful for organizations that use a variety of SNMP configurations, such as using different SNMP configurations based on device type, geographical location, or organizational support models.

Viewing the SNMP template list

To view the SNMP templates list:

1. Navigate to System→SNMP Template.
   a. Click the System tab from the tabular navigation system on the top.
   b. Click Resource Management on the navigation tree on the left.
   c. Click SNMP Template under Resource Management from the navigation system on the left.

IMC displays all SNMP templates in the SNMP Template List displayed in the main pane of the System SNMP Template window.

SNMP Template List

- **Name**: Contains the SNMP template name.
- **Parameter type**: Identifies which version of SNMP this template is configured for.
- **Timeout (seconds)**: Contains the SNMP timeout value for the associated template. The Timeout counter determines how long IMC will wait for an SNMP reply from the managed device before declaring that the request has timed out.
- **Retries**: Contains the SNMP retries value for the associated template. The retries parameter defines how many times the management system (IMC) will send SNMP retries in an attempt to communicate with the managed device before reporting a failure.
Modify: Contains an icon for navigating to the Modify SNMP Template page for the associated template.

Delete: Contains an icon for deleting the associated template.

If the SNMP template list contains enough entries, the following navigational aids are displayed:

- Click \(\text{\textless}\) to page forward in the SNMP Template List.
- Click \(\text{\textgreater}\) to page forward to the end of the SNMP Template List.
- Click \(\text{\textless}\) to page backward in the SNMP Template List.
- Click \(\text{\textless}\) to page backward to the front of the SNMP Template List.

2. Click 8, 15, 50, 100, or 200 from the right side of the main pane to configure how many items per page you want to view.

Adding an SNMPv1 or v2c template

To add a SNMPv1 or v2c template:

1. Navigate to System→SNMP Template.
2. Click the System tab from the tabular navigation system on the top.
3. Click Resource Management on the navigation tree on the left.
4. Click SNMP Template under Resource Management from the navigation system on the left.
   IMC displays all SNMP template entries in the SNMP Template List displayed in the main pane of the System SNMP Template window.
5. Click Add.
6. Enter the following information in the Add SNMP Template page.
7. Enter a unique name for the SNMP template name in the Name field.
   You cannot modify the name of a template once the template has been created. To modify the name, you must first delete the template and then recreate it with the new name.
8. Select the version of SNMP that is configured for use on the managed devices from the Parameter Type list.
9. Select SNMPv1, SNMPv2c, SNMPv3 and so on.
10. Enter the Read-Only community string that is configured on the managed devices in the Read-Only Community String field.
    The default is ‘public’.
11. Enter the Read-Write community string configured on the managed devices in the Read-Write Community String field.
    The default is ‘private’.
    SNMP configuration settings for each managed device must match the SNMP settings configured on it. For information on configuring SNMP settings on the managed devices, refer to your vendor documentation.
12. Enter the SNMP timeout value (1–60 seconds) in the Timeout field.
    This parameter determines how long IMC waits for an SNMP reply from the managed device before declaring that the request has timed out.
13. Enter the number of SNMP retries (1–20) in the Retries field.
The retries parameter defines how many times the management system (IMC) sends SNMP retries in an attempt to communicate with the managed device before reporting a failure. The default is 3.

14. Click OK.

Adding an SNMPv3 template

To add a SNMPv3 template:

15. Navigate to System→SNMP Template.
16. Click the System tab from the tabular navigation system on the top.
17. Click Resource Management on the navigation tree on the left.
18. Click SNMP Template under Resource Management from the navigation system on the left. IMC displays all SNMP template entries in the SNMP Template List displayed in the main pane of the System SNMP Template window.
19. Click Add.
20. Enter the following information in the Add SNMP Template page.
21. Enter a unique name for the SNMP template name in the Name field.
22. Select the SNMPv3 type that matches the version of SNMP configured on the devices to be managed by this template from the Parameter Type list, shown in Table 1 (page 76).

Table 1 SNMP parameters

<table>
<thead>
<tr>
<th>Parameter type option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMPv1</td>
<td>SNMP version 1</td>
</tr>
<tr>
<td>SNMPv2c</td>
<td>SNMP version 2c</td>
</tr>
<tr>
<td>SNMPv3 No-Priv No_Auth</td>
<td>SNMPv3 with no authentication and no encryption.</td>
</tr>
<tr>
<td>SNMPv3 No-Priv Auth-Md5</td>
<td>SNMPv3 with no encryption and with MD5 authentication.</td>
</tr>
<tr>
<td>SNMPv3 No-Priv Auth-Sha</td>
<td>SNMPv3 with no encryption and with SHA authentication.</td>
</tr>
<tr>
<td>SNMPv3 Priv-Des Auth-Md5</td>
<td>SNMPv3 with DES encryption and Md5 authentication.</td>
</tr>
<tr>
<td>SNMPv3 Priv-Des Auth-Sha</td>
<td>SNMPv3 with DES encryption and SHA authentication.</td>
</tr>
<tr>
<td>SNMPv3 Priv-Aes128 Auth-Md5</td>
<td>SNMPv3 with Aes 128 bit encryption and Md5 authentication.</td>
</tr>
<tr>
<td>SNMPv3 Priv-Aes128 Auth-Sha</td>
<td>SNMPv3 with Aes 128 bit encryption and SHA authentication.</td>
</tr>
<tr>
<td>SNMPv3 Priv-Aes192 Auth-Md5</td>
<td>SNMPv3 with Aes 192 bit encryption and Md5 authentication.</td>
</tr>
<tr>
<td>SNMPv3 Priv-Aes192 Auth-Sha</td>
<td>SNMPv3 with Aes 192 bit encryption and SHA authentication.</td>
</tr>
<tr>
<td>SNMPv3 Priv-Aes256 Auth-Md5</td>
<td>SNMPv3 with Aes 256 bit encryption and Md5 authentication.</td>
</tr>
<tr>
<td>SNMPv3 Priv-Aes256 Auth-Sha</td>
<td>SNMPv3 with Aes 256 bit encryption and SHA authentication.</td>
</tr>
</tbody>
</table>

23. Enter the username that is configured on the managed devices in the Username field.
24. If prompted, enter the authentication password that is configured on the managed devices in the Authentication Password field.
25. If prompted, enter the encryption password that is configured on the managed devices in the Encryption Password field.
26. Enter the SNMP timeout value in the Timeout field.
Valid range is 1–60 seconds. The timeout parameter defines how long the system will wait for the device to respond to SNMP requests before reporting that the request has timed out.

27. Enter the SNMP retries value in the **Retries** field.

Valid range is 1–20. The retries parameter defines how many times the management system (IMC) sends SNMP retries in an attempt to communicate with the managed device. The default is 3.

28. Click **OK**.

The SNMP templates you have created now appear as configuration options when adding devices to IMC by auto discovery, by batch mode or by adding devices individually. For more information, see "Adding devices in IMC" (page 154).

Modifying an SNMP template
To modify an SNMP template:

29. Navigate to **System→SNMP Template**:
   a. Click the **System** tab from the tabular navigation system on the top.
   b. Click **Resource Management** on the navigation tree on the left.
   c. Click **SNMP Template** under **Resource Management** from the navigation system on the left. IMC displays all SNMP template entries in the **SNMP Template List** displayed in the main pane of the **System→SNMP Template** window.

30. Click the **Modify** icon in the **SNMP Template List** associated with the SNMP template you want to modify.

31. Modify any of the configuration information displayed in the **Modify SNMP Template** page. For more information on template parameters, see "Adding an SNMPv1 or v2c" or "Adding an SNMPv3".

32. Click **OK**.

Deleting an SNMP template
To delete an SNMP template:

1. Navigate to **System→SNMP Template**:
   a. Click the **System** tab from the tabular navigation system on the top.
   b. Click **Resource Management** on the navigation tree on the left.
   c. Click **SNMP Template** under **Resource Management** from the navigation system on the left. IMC displays all SNMP template entries in the **SNMP Template List** displayed in the main pane of the **System SNMP Template** window.

2. Click the **Delete** icon in the **SNMP Template List** associated with the SNMP template you want to delete.

3. Click **OK** to confirm deletion of the selected SNMP template.

Telnet templates
IMC uses Telnet to provide you with remote access to managed devices. IMC also uses Telnet for certain network resource management functions.
The Telnet template feature allows you to save Telnet configuration settings in IMC, which can then be applied when adding new devices to IMC, performing an auto discovery, or configuring devices in individual or batch mode. Telnet templates store IMC’s Telnet configurations for devices to support IMC’s communication with the device. Telnet templates do not configure the Telnet settings on the device itself.

Viewing the Telnet template list

To view the Telnet template list:

1. Navigate to **System → Telnet Template**:
   a. Click the **System** tab from the tabular navigation system on the top.
   b. Click **Resource Management** on the navigation tree on the left.
   c. Click **Telnet Template** under **Resource Management** from the navigation system on the left.

IMC displays all Telnet templates in the **Telnet Template List** displayed in the main pane of the **System → Telnet Template** window.

**Telnet template list**

- **Name**: Contains the Telnet template name.
- **Authentication Mode**: Identifies which form of authentication this template is configured for.
- **Timeout (seconds)**: Contains the Telnet timeout value for the associated template. The **Timeout** counter defines how long the system will wait for the device to respond in seconds.
- **Modify**: Contains an icon for navigating to the **Modify Telnet Template** page for the associated template.
- **Delete**: Contains an icon for deleting the associated template.

If the Telnet template list contains enough entries, the following navigational aids are displayed:

- Click **→** to page forward in the **Telnet Template List**.
- Click **↓↓** to page forward to the end of the **Telnet Template List**.
- Click **←** to page backward in the **Telnet Template List**.
- Click **↑↑** to page backward to the front of the **Telnet Template List**.

2. Click 8, 15, 50, 100, or 200 from the right side of the main pane to configure how many items per page you want to view.

Adding a Telnet template

To add a Telnet template:

1. Navigate to **System → Telnet Template**:
   a. Click the **System** tab from the tabular navigation system on the top.
   b. Click **Resource Management** on the navigation tree on the left.
   c. Click **Telnet Template** under **Resource Management** from the navigation system on the left.

IMC displays all Telnet templates in the **Telnet Template List** displayed in the main pane of the **System → Telnet Template** window.

2. Click **Add**.

3. Enter the following information in the **Add Telnet Template** page.

4. Enter a unique name for the Telnet template in the **Name** field.
You cannot modify the name of a template once the template has been created. To modify the name, you must first delete the template and then recreate it with a new name.

5. Select the mode to match the telnet authentication mode configured on the managed devices from the Authentication Mode list.

Options include Password, Username + Password, Super Password, Password + Super Password, Username + Password + Super Password, No Username + No Password, and Username + No Password.

6. If prompted, enter the username that is configured on managed devices in the Username field.

7. If prompted, enter the password that is configured on the managed devices in the Password field.

8. If prompted, enter the super password that is configured on the managed devices in the Super Password field.

9. Enter the Telnet timeout value in the Timeout field.

Valid range is 1–60 seconds. The timeout parameter defines how long the system waits for the device to respond in seconds.

10. Click OK.

The Telnet templates you have added now appear as configuration options when configuring devices individually or in batch mode.

The Telnet configuration settings in IMC must match the Telnet settings configured on the managed devices. For information on configuring Telnet settings on the managed devices, refer your vendor’s documentation.

The Telnet templates also appear as configuration options when adding devices to IMC by auto discovery, by batch mode or by adding devices individually. For more information, see “Adding devices in IMC” (page 154).

Modifying a Telnet template

To modify a Telnet template:

1. Navigate to System→Telnet Template:
   a. Click the System tab from the tabular navigation system on the top.
   b. Click Resource Management on the navigation tree on the left.
   c. Click Telnet Template under Resource Management from the navigation system on the left.

IMC displays all Telnet templates in the Telnet Template List displayed in the main pane of the System→Telnet Template window.

2. Click the Modify icon in the Telnet Template List associated with the Telnet template you want to modify.

3. Modify the authentication mode setting to match the Telnet authentication mode configured on the managed devices.

Options include Password, Username + Password, Super Password, Password + Super Password, Username + Password + Super Password, No Username + No Password, and Username + No Password.

4. Modify the username to match the username configured on managed devices, if prompted.

5. Modify the password to match the password configured on the managed devices, if prompted.

6. Enter the super password to match the super password configured on the managed devices, if prompted.
7. Modify the **Telnet Timeout** value.
   Valid range is 1–60 seconds. The timeout parameter defines how long the system waits for the device to respond in seconds.

8. Click **OK**.

### Deleting a Telnet template

To delete a Telnet template:

1. Navigate to **System**→**Telnet Template**:
   a. Click the **System** tab from the tabular navigation system on the top.
   b. Click **Resource Management** on the navigation tree on the left.
   c. Click **Telnet Template** under **Resource Management** from the navigation system on the left.

   IMC displays all Telnet templates in the **Telnet Template List** displayed in the main pane of the **System**→**Telnet Template** window.

2. Click the **Delete** icon in the **Telnet Template List** associated with the Telnet template you want to delete.

3. Click **OK** to confirm deletion of the selected Telnet template.

### SSH templates

IMC uses SSH to enable secure remote access to managed devices. IMC also uses SSH for certain network resource management functions.

The SSH template feature allows you to save SSH configuration settings in IMC, which can then be applied when adding new devices to IMC, performing an auto discovery, or configuring devices in individual or batch mode. SSH templates store IMC’s SSH configurations for devices to support IMC’s communication with the device. SSH templates do not configure the SSH settings on the device itself.

### Viewing the SSH Template List

To view the SSH templates list:

1. Navigate to **System**→**SSH Template**:
   a. Click the **System** tab from the tabular navigation system on the top.
   b. Click **Resource Management** on the navigation tree on the left.
   c. Click **SSH Template** under **Resource Management** from the navigation system on the left.

   IMC displays all SSH templates in the **SSH Template List** displayed in the main pane of the **System**→**SSH Template** window.

### SSH template list

- **Name**: Contains the SSH template name.
- **Authentication Mode**: Identifies which form of authentication this template is configured for.
- **User Name**: Contains the user name.
- **Timeout (seconds)**: Contains the SSH timeout value for the associated template. The Timeout counter defines how long the system will wait for the device to respond in seconds.
Retries: Contains the SSH retries value for the associated template. The retries parameter defines how many times the management system (IMC) will send retries in an attempt to communicate with the managed device before reporting a failure.

Modify: Contains an icon for navigating to the Modify SSH Template page for the associated template.

Delete: Contains an icon for deleting the associated template.

If the SSH Template list contains enough entries, the following navigational aids are displayed:

- Click to page forward in the SSH Template List.
- Click to page forward to the end of the SSH Template List.
- Click to page backward in the SSH Template List.
- Click to page backward to the front of the SSH Template List.

2. Click 8, 15, 50, 100, or 200 from the right side of the main pane to configure how many items per page you want to view.

Adding an SSH template

To add an SSH template:

1. Navigate to System→SSH Template:
   a. Click the System tab from the tabular navigation system on the top.
   b. Click Resource Management on the navigation tree on the left.
   c. Click SSH Template under Resource Management from the navigation system on the left.

   IMC displays all SSH templates in the SSH Template List displayed in the main pane of the System→SSH Template window.

2. Click Add.

3. Enter the following information in the Add SSH Template page.

4. Enter a unique name for the SSH template name in the Name field.
   You cannot modify the name of a template once the template has been created. To modify the name, you must first delete the template and then recreate it with a new name.

5. Select the mode that matches the SSH configuration mode configured on the managed devices from the Authentication Mode list.
   Authentication mode options include Password, Private Key, Password + Private Key, Password+Super Password, Private Key+Super Password, and Password+Private Key+Super Password.

6. Enter the username that is configured on managed devices in the User Name field.

7. Enter the password that is configured on the managed devices in the Password field.
   If prompted, enter the path and filename of the private key file that contains the key that enables login in the Private Key File field.
   If prompted, enter the private key password for the private key file in the Private Key Password field.
   If prompted, enter the super password that is configured on the managed devices in the Super Password field.

8. Enter the TCP port for SSH configured on managed devices in the Port field. The default TCP port is 22.

9. Enter the SSH timeout value in the Timeout field.
Valid range is 1–120 seconds. The timeout parameter defines how long the system waits for the device to respond in seconds before declaring that the response has timed out. The default setting is 10 seconds.

10. Enter the number of SSH retries in the **Retries** field.
   Valid range is 1–5. The retries parameter defines how many times the management system (IMC) sends SSH retries in an attempt to communicate with the managed device before reporting a failure. The default setting is 3.

11. Click **OK**.
   The SSH templates you have added now appear as options when configuring devices individually or in batch mode.

The SSH configuration settings in IMC must match the SSH settings configured on the managed devices. For information on configuring SSH settings on the managed devices, refer your vendor’s documentation. The SSH templates also appear as configuration options when adding devices to IMC by auto discovery, by batch mode or by adding devices individually. For more information, see "Adding devices in IMC" (page 154).

**Modifying an SSH template**

To modify an SSH template:

1. Navigate to **System→SSH Template**:
   a. Click the **System** tab from the tabular navigation system on the top.
   b. Click **Resource Management** on the navigation tree on the left.
   c. Click **SSH Template** under **Resource Management** from the navigation system on the left.
      IMC displays all SSH templates in the **SSH Template List** displayed in the main pane of the **System→SSH Template** window.

2. Click the **Modify** icon in the **SSH Template List** associated with the SSH template you want to modify.

3. Select the authentication mode to match the SSH configuration on the managed devices from the **Authentication Mode** list.
   Authentication mode options include **Password**, **Password + Private Key**, and **Private Key**.

4. Modify the username to match the username that is configured on managed devices in the **User Name** field.

5. Modify the password to match the password that is configured on the managed devices in the **Password** field.
   If prompted, modify the path and filename of the private key file that contains the key that enables login in the **Private Key File** field.
   If prompted, modify the private key password for the private key file as needed in the **Private Key Password** field.
   If prompted, enter the super password that is configured on the managed devices in the **Super Password** field.

6. Modify the TCP port for SSH to match what is configured on managed devices in the **Port** field. The default TCP port is 22.

7. Modify the SSH timeout value as needed in the **Timeout** field.
Valid range is 1–120 seconds. The timeout parameter defines how long the system waits for the
device to respond in seconds before declaring that the response has timed out. The default setting is
10 seconds.

8. Modify the number of SSH retries as needed in the Retries field.
Valid range is 1–5. The retries parameter defines how many times the management system (IMC)
resends SSH retries in an attempt to communicate with the managed device before reporting a failure.
The default setting is 3.

9. Click OK.

Deleting an SSH template
To delete an SSH template:

1. Navigate to System→SSH Template:
   a. Click the System tab from the tabular navigation system on the top.
   b. Click Resource Management on the navigation tree on the left.
   c. Click SSH Template under Resource Management from the navigation system on the left.
      IMC displays all SSH templates in the SSH Template List displayed in the main pane of the
      System→SSH Template window.

2. Click the Delete icon in the SSH Template List associated with the SSH template you want to
delete.

3. Click OK to confirm deletion of the selected SSH template.

SOAP templates
With Virtual Network Manager deployed, the SOAP Template appears in the System tab. IMC uses SOAP
to enable secure remote access to managed VMware virtual network devices, including vManager and ESX
server.

The SOAP template feature allows you to save SOAP configuration settings in IMC, which can then be
applied when adding new virtual network devices to IMC, performing an auto discovery, or configuring
devices in individual or batch mode. SOAP templates store the IMC SOAP configurations for devices to
support IMC’s communication with the device. SOAP templates do not configure the SOAP settings on the
device itself.

Viewing the SOAP Template List
To view the SOAP templates list:

1. Navigate to System→SOAP Template:
   a. Click the System tab from the tabular navigation system on the top.
   b. Click Resource Management on the navigation tree on the left.
   c. Click SOAP Template under Resource Management from the navigation system on the left.
      IMC displays all SOAP templates in the SOAP Template List displayed in the main pane of the
      System→SOAP Template window.

SOAP template list
   o Template Name Contains the SOAP template name.
- **Access URL** contains the access URL for the configured SOAP template.
- **User Name** contains the user name.
- **Modify** contains an icon for navigating to the Modify SOAP Template page for the associated template.
- **Delete** contains an icon for deleting the associated template.

If the SOAP template list contains enough entries, the following navigational aids are displayed:

- Click to page forward in the SOAP Template List.
- Click to page forward to the end of the SOAP Template List.
- Click to page backward in the SOAP Template List.
- Click to page backward to the front of the SOAP Template List.

2. Click 8, 15, 50, 100, or 200 from the right side of the main pane to configure how many items per page you want to view.

You can sort the SOAP Template List by the Template Name and User Name fields. Click the column label to sort the list by the selected field. The column label is a toggle switch that allows you to toggle between the various sort options specific to each field.

### Adding an SOAP template

To add an SOAP template:

1. Navigate to System→SOAP Template:
   a. Click the System tab from the tabular navigation system on the top.
   b. Click Resource Management on the navigation tree on the left.
   c. Click SOAP Template under Resource Management from the navigation system on the left.
      IMC displays all SOAP templates in the SOAP Template List displayed in the main pane of the System→SOAP Template window.

2. Click Add.
3. Enter the following information in the Add SOAP Template page.
4. Enter a unique name for the SOAP template name in the Template Name field.
   You cannot modify the name of a template once the template has been created. To modify the name, you must first delete the template and then recreate it with the new name.
5. Select the protocol to match the SOAP configuration on the managed devices from the Protocol list.
   Protocol options include http and https.
6. Enter the port number that is configured on managed devices in the Port field.
   The default port number is 80 for http, or 443 for https.
7. Enter the root path that is configured on managed devices in the Root Path field.
   The default setting is sdk.
8. Enter the username that is configured on managed devices in the Username field.
9. Enter the password that is configured on the managed devices in the Password field.
10. If you want to test whether the configured SOAP Template can connect to a vManager/physical server, click the Test connection to vManager/physical server checkbox, and the Select button appears.
11. Click the **Select** button to select a vManager/physical server.

**Adding devices by View**

**To add devices by view:**

1. From the **Select Devices** dialog box, click the **By View** tab.
2. Expand the view you want to select devices from by clicking on the arrow to the left of the three view options, **IP View**, **Device View**, or **Custom View**.
3. Click the view you want to select devices from the navigation tree on the left. The devices from the group you click appear in the **Devices Found** field to the right of the navigation tree. You can select devices from more than one group by clicking more than one group.
4. Highlight the devices you want to select from the **Devices Found** list and click the **Add selected** button to add them to the selected devices list.
5. To remove one or more devices, select them and click **Remove selected**.
6. Confirm that the devices you have found have been added by reviewing the **Selected Devices** list.
7. Click **OK**.
8. Confirm that the devices now appear in the **Devices List** field.

**Adding devices by Advanced query**

You can also add devices using the **Advanced** query option to search IMC using various criteria and use the results of the search to add devices. To do so:

1. Click **Select** located to the right of the **Selected Devices** field.
2. From the **Select Devices** dialog box, click the **Advanced** tab.
3. Enter values in one or more of the search parameters listed here:
   - **Device IP**: Enter the IP address you want to query for. Click on the **Exact Query** checkbox if you want IMC to search for the exact IP address you have entered. Leave the **Exact Query** box unchecked if you want IMC to match only a certain portion of the IP address.
   - **Device IP List**: Configure multiple device IP addresses to be searched. Click the **link**. Then, the **Device IP List Configuration** window appears. Enter one or multiple device IP addresses in the **Input Device IP** field (if you enter multiple IP addresses, enter one IP address on each line), and then click **Add** to add the entered IP addresses to the **Device IP List** field below. Repeat the steps above to add all device IP addresses to be searched. To delete an IP address in the **Device IP List** field, select the IP address and then click **Delete**. Click **OK** to complete the operation. Make sure that the device IP addresses to be searched have been added to the **Device IP List** field. To clear the **Device IP List** field, click the **link**.
   - **Device Label**: Enter the device name for the devices you want to add. IMC supports fuzzy matching for device labels. Therefore, you can enter the entire device label for the device you want to locate, or you can enter just a portion of it. IMC displays all matches that contain the portion you enter.
   - **Device Status**: Select device status from the **Device Status** list.
   - **Device Category**: Select a device category from the **Device Category** list.
   - **Device Series**: Select a device series from the **Device Series** list.
   - **Contact**: Enter the contact name information by which you want to search. IMC supports fuzzy matching for this field. Therefore, you can enter a partial string for the contact or the complete string for the contact.
Location: Enter the location information by which you want to search. IMC supports fuzzy matching for this field. Therefore, you can enter a partial string for location or the complete string for location.

Device Reachability: Select device reachability status from the Device Reachability list.

4. Click Query to begin your search.

The results of your search appear in the Devices Found field.

5. Highlight the devices you want to select and click Add selected to add them to the selected devices list.

6. To remove one or more devices, select them and click Remove selected.

7. Confirm that the devices you have found have been added.

8. Click OK. Confirm that the devices now appear at the left of Select.

9. Click OK.

The SOAP configuration settings in IMC must match the SOAP settings configured on the managed devices. For information on configuring SOAP settings on the managed devices, refer to your vendor’s documentation.

If you select the Test connection to vManager/physical server option and add the devices, click OK. IMC then accesses the specified device by using the defined SOAP parameters. If the access succeeds, the SOAP Template is added to IMC; otherwise, the SOAP Template is not added to IMC.

The SOAP templates you have added now display as configuration options when configuring devices.

Modifying an SOAP template

To modify an SOAP template:

1. Navigate to System→SOAP Template:

   a. Click the System tab from the tabular navigation system on the top.

   b. Click Resource Management on the navigation tree on the left.

   c. Click SOAP Template under Resource Management from the navigation system on the left.

   IMC displays all SOAP templates in the SOAP Template List displayed in the main pane of the System→SOAP Template window.

2. Click the Modify icon in the SOAP Template List associated with the SOAP template you want to modify.

3. Select the protocol to match the SOAP configuration on the managed devices from the Protocol list. Protocol options include http and https.

4. Enter port number that is configured on managed devices in the Port field.

5. Enter the root path that is configured on managed devices in the Root Path field. The default setting is sdk.

6. Modify username to match the username that is configured on managed devices in the Username field.

7. Modify the password to match the password that is configured on the managed devices in the Password field.
8. If you want to test whether the configured SOAP Template can connect to a vManager/physical server, click the Test connection to vManager/physical server checkbox, and the Select button appears.

9. Click the Select button to select a vManager/physical server.

10. Add devices by using either the View or Advanced query option. See "Adding devices by View" (page 85) and "Adding devices by Advanced query" (page 85).

   If you select the Test connection to vManager/physical server option and add the devices, click OK. IMC will then access the specified device by using the defined SOAP parameters. If the access succeeds, the SOAP Template is added to IMC; otherwise, the SOAP Template is not added to IMC.

Deleting an SOAP template

To delete an SOAP template:

1. Navigate to System→SOAP Template:
   a. Click the System tab from the tabular navigation system on the top.
   b. Click Resource Management on the navigation tree on the left.
   c. Click SOAP Template under Resource Management from the navigation system on the left.

IMC displays all SOAP templates in the SOAP Template List displayed in the main pane of the System→SOAP Template window.

2. Click the Delete icon in the SOAP Template List associated with the SOAP template you want to delete.

3. Click OK to confirm deletion of the selected SOAP template.

PowerShell templates

With Virtual Network Manager deployed, the PowerShell Template appears in the System tab. IMC uses PowerShell to enable secure remote access to managed Microsoft Virtual Machine Manager server.

The PowerShell template feature allows you to save PowerShell configuration settings in IMC, which can then be applied when adding new virtual network devices to IMC, performing an auto discovery, or configuring devices in individual or batch mode. PowerShell templates store IMC’s PowerShell configurations for devices to support IMC’s communication with the device. PowerShell templates do not configure the PowerShell settings on the device itself.

Viewing the PowerShell template list

To view the PowerShell templates list:

1. Navigate to System→PowerShell Template:
   a. Click the System tab from the tabular navigation system on the top.
   b. Click Resource Management on the navigation tree on the left.
   c. Click PowerShell Template under Resource Management from the navigation system on the left.

IMC displays all PowerShell templates in the main pane of the PowerShell Template List page.

PowerShell template list

- **Template Name**: Contains the PowerShell template name.
- **User Name**: Contains the user name.
Port: PowerShell monitor port.

Modify: Contains an icon for navigating to the Modify PowerShell Template page for the associated template.

Delete: Contains an icon for deleting the associated template.

If the PowerShell template list contains enough entries, the following navigational aids are displayed:

- Click to page forward in the PowerShell Template List.
- Click to page forward to the end of the PowerShell Template List.
- Click to page backward in the PowerShell Template List.
- Click to page backward to the front of the PowerShell Template List.

2. Click 8, 15, 50, 100, or 200 from the right side of the main pane to configure how many items per page you want to view.

You can sort the PowerShell Template List by the Template Name, User Name, and Port fields. Click the column label to sort the list by the selected field. The column label is a toggle switch that allows you to toggle between the various sort options specific to each field.

Adding a PowerShell template

To add a PowerShell template:

1. Navigate to System→PowerShell Template:
   a. Click the System tab from the tabular navigation system on the top.
   b. Click Resource Management on the navigation tree on the left.
   c. Click PowerShell Template under Resource Management from the navigation system on the left.
      IMC displays all PowerShell templates in the main pane of the PowerShell Template List page.

2. Click Add.

3. Enter the following information in the Add PowerShell Template page.

4. Enter a unique name for the PowerShell template name in the Template Name field.

The PowerShell configuration settings in IMC must match the PowerShell settings configured on the managed devices. For information on configuring PowerShell settings on the managed devices, refer to your vendor’s documentation.

5. Enter the username that is configured on managed devices in the Username field.

6. Enter the password that is configured on the managed devices in the Password field.

7. Enter the port number that is configured on managed devices in the Port field.

8. If you want to test whether the configured PowerShell Template can connect to a vManager/physical server, click the Test connection to vManager/physical server checkbox. The Select button appears.

9. Click Select to select a vManager/physical server.

10. Add devices by using either the View or Advanced query option. See "Adding devices by View" (page 85) and "Adding devices by Advanced query" (page 85).

The PowerShell configuration settings in IMC must match the PowerShell settings configured on the managed devices. For information on configuring PowerShell settings on the managed devices, refer to your vendor’s documentation.
If you select the **Test connection to vManager/physical server** option and add the devices, click **OK**. IMC then accesses the specified device by using the defined PowerShell parameters. If the access succeeds, the PowerShell Template is added to IMC; otherwise, the PowerShell Template is not added to IMC.

The PowerShell templates you have added now appear as configuration options when configuring devices.

**Modifying a PowerShell template**

To modify a PowerShell template:

1. Navigate to **System → PowerShell Template**:
   a. Click the **System** tab from the tabular navigation system on the top.
   b. Click **Resource Management** on the navigation tree on the left.
   c. Click **PowerShell Template** under **Resource Management** from the navigation system on the left.

   IMC displays all PowerShell templates in the main pane of the **PowerShell Templates List** page.

2. Click the **Modify** icon in the **PowerShell Template List** associated with the PowerShell template you want to modify.

3. Modify username to match the username that is configured on managed devices in the **Username** field.

4. Modify the password to match the password that is configured on the managed devices in the **Password** field.

5. Enter port number that is configured on managed devices in the **Port** field.

6. Click **OK**.

7. If you select the **Test connection to vManager/physical server** option and add the devices, click **OK**.

IMC then accesses the specified device by using the defined PowerShell parameters. If the access succeeds, the PowerShell Template is added to IMC; otherwise, the PowerShell Template is not added to IMC.

**Deleting a PowerShell template**

To delete a PowerShell template:

1. Navigate to **System → PowerShell Template**:
   a. Click the **System** tab from the tabular navigation system on the top.
   b. Click **Resource Management** on the navigation tree on the left.
   c. Click **PowerShell Template** under **Resource Management** from the navigation system on the left.

   IMC displays all PowerShell templates in the main pane of the **PowerShell Templates List** page.

2. Click the **Delete** icon in the **PowerShell Template List** associated with the PowerShell template you want to delete.

3. Click **OK** to confirm deletion of the selected PowerShell template.
WMI templates

WMI refers to the Windows Management Instrumentation (WMI), and is a type of Windows management technology. With Virtual Network Manager deployed, the WMI Template appears in the System tab. IMC uses WMI to enable secure remote access to managed Hyper-V physical servers.

The WMI template feature allows you to save WMI configuration settings in IMC, which can then be applied when adding new virtual network devices to IMC, performing an auto discovery, or configuring devices in individual or batch mode. WMI templates store IMC’s WMI configurations for devices to support communication with the device. WMI templates do not configure the WMI settings on the device itself.

Viewing the WMI template list

To view the WMI templates list:

1. Navigate to System→WMI Template:
   a. Click the System tab from the tabular navigation system on the top.
   b. Click Resource Management on the navigation tree on the left.
   c. Click WMI Template under Resource Management from the navigation system on the left.

   IMC displays all WMI templates in the main pane of the WMI Template List displayed page.

   WMI template list
   o Template Name: Contains the WMI template name.
   o User Name: Contains the user name.
   o Impersonation Level can be Default, Anonymous, Identify, Impersonate, and Delegate.
   o Authentication Level can be Default, None, Connect, Call, Packet, PacketIntegrity, and PacketPrivacy.
   o Modify: Contains an icon for navigating to the Modify WMI Template page for the associated template.
   o Delete: Contains an icon for deleting the associated template.

   If the WMI template list contains enough entries, the following navigational aids are displayed:
   o Click to page forward in the WMI Template List.
   o Click to page forward to the end of the WMI Template List.
   o Click to page backward in the WMI Template List.
   o Click to page backward to the front of the WMI Template List.

2. Click 8, 15, 50, 100, or 200 from the right side of the main pane to configure how many items per page you want to view.

   You can sort the WMI Template List by the Template Name, User Name, Impersonation Level, and Authentication Level fields. Click the column label to sort the list by the selected field. The column label is a toggle switch that allows you to toggle between the various sort options specific to each field.

Adding a WMI template

To add a WMI template:

1. Navigate to System→WMI Template:
   a. Click the System tab from the tabular navigation system on the top.
b. Click **Resource Management** on the navigation tree on the left.

c. Click **WMI Template** under **Resource Management** from the navigation system on the left.
   IMC displays all WMI templates in the main pane of the **WMI Template List** page.

2. Click **Add**.

3. Enter the following information in the **Add WMI Template** page.

4. Enter a unique name for the WMI template name in the **Template Name** field.
   You cannot modify the name of a template once the template has been created. To modify the name, you must first delete the template and then recreate it with a new name.

5. Enter the username that is configured on managed devices in the **Username** field.

6. Enter the password that is configured on the managed devices in the **Password** field.

7. Select an impersonation level from the **Impersonation Level** list.

8. Select an authentication level from the **Authentication Level** list.

9. If you want to test whether the configured WMI parameters can connect to a vManager/physical server, click the **Test connection to vManager/physical server** checkbox.
   The **Select** button appears.

10. Click the **Select** button to select vManager/physical server.

11. Add devices by using either the **View** or **Advanced** query option. See "Adding devices by View" (page 85) and "Adding devices by Advanced query" (page 85).

   The WMI configuration settings in IMC must match the WMI settings configured on the managed devices. For information on configuring WMI settings on the managed devices, refer to your vendor’s documentation.

   If you select **Test connection to vManager/physical server** option, IMC accesses the specified device by using the configured WMI parameters. If the access succeeds, the WMI Template is added to IMC; otherwise, the WMI Template is not added to IMC.

   The WMI templates you have added now appear as configuration options when configuring devices.

### Modifying a WMI template

To modify a WMI template:

1. Navigate to **System→WMI Template**:
   
   a. Click the **System** tab from the tabular navigation system on the top.
   b. Click **Resource Management** on the navigation tree on the left.
   c. Click **WMI Template** under **Resource Management** from the navigation system on the left.
      IMC displays all WMI templates in the main pane of the **WMI Template List** page.

2. Click the **Modify** icon in the WMI Template List associated with the WMI template you want to modify.

3. Modify username to match the username that is configured on managed devices in the **Username** field.

4. Modify the password to match the password that is configured on the managed devices in the **Password** field.

5. Select an impersonation level from the **Impersonation Level** list.
6. Select an authentication level from the Authentication Level list.

7. Click the Test connection to vManager/physical server checkbox, if you want to test whether the configured WMI template can connect to a vManager/physical server.

The Select button appears.

8. Click the Select button to select a vManager/physical server.

9. Add devices by using either the View or Advanced query option. See "Adding devices by View" (page 85) and "Adding devices by Advanced query" (page 85).

If you select the Test connection to vManager/physical server option, IMC uses the configured WMI parameters to access the specified device. If the access succeeds, the WMI template is updated; otherwise, the WMI template is not updated.

Deleting a WMI template

To delete a WMI template:

1. Navigate to System→WMI Template:
   a. Click the System tab from the tabular navigation system on the top.
   b. Click Resource Management on the navigation tree on the left.
   c. Click WMI Template under Resource Management from the navigation system on the left. IMC displays all WMI templates in the main pane of the WMI Template List page.

2. Click the Delete icon in the WMI Template List associated with the WMI template you want to delete.

3. Click OK to confirm deletion of the selected WMI template.

Configuring vendor and device information

Vendor and device specific information is used by IMC for Resource, Change, and Configuration management functions and is integral to optimal IMC functioning. Vendor and device specific details are also displayed in device details views.

IMC auto-populates vendor and device information when the information is available. For some third party devices this information may not be available. If device information is not available, IMC cannot categorize these devices into the router, switch, server, wireless or voice groups to which they should belong. In such cases, IMC categorizes these devices as end stations. You can correct this by manually adding device vendor, series and model information.

Viewing and configuring device vendor information

You can store vendor information for devices in the network infrastructure. This section explains the Device Vendor List, which displays all entries in IMC for Device vendors, and how to add, modify, and delete device vendor information.

Viewing the device vendor list

To view the device vendor list:

1. Navigate to System→Device Vendor:
   a. Click the System tab from the tabular navigation system on the top.
   b. Click Resource Management on the navigation tree on the left.
c. Click 🔄 Device Vendor under Resource Management from the navigation system on the left. IMC displays all device vendor information in the Device Vendor List displayed in the main pane of the System→Device Vendor window.

**Device vendor list**
- **Vendor Name:** Contains the vendor’s name.
- **Vendor Type:** Identifies whether the vendor list entry is system or user-defined.
- **Phone Number:** Contains the vendor’s phone number.
- **Vendor Contact:** Contains the vendor’s contact name.
- **Description:** Contains a description of the vendor.
- **Modify:** Contains an icon for navigating to the Modify Device Vendor page for the associated device vendor entry.
- **Delete:** Contains an icon for deleting the associated device vendor entry.

You can sort the Device Vendor List by the Vendor Name and Vendor Type fields. Click the column label to sort the list by the selected field. The column label is a toggle switch that allows you to toggle between the various sort options specific to each field.

If the device vendor list contains enough entries, the following navigational aids are displayed:
- Click ⏎ to page forward in the Device Vendor List.
- Click ⏯️ to page forward to the end of the Device Vendor List.
- Click ⏏️ to page backward in the Device Vendor List.
- Click 🔄 to page backward to the front of the Device Vendor List.

2. Click 8, 15, 50, 100, or 200 from the right side of the main pane to configure how many items per page you want to view.

**Adding a device vendor**

To add a device vendor:

1. Navigate to System→Device Vendor:
   - a. Click the System tab from the tabular navigation system on the top.
   - b. Click Resource Management on the navigation tree on the left.
   - c. Click 🔄 Device Vendor under Resource Management from the navigation system on the left. IMC displays all device vendor information in the Device Vendor List displayed in the main pane of the System→Device Vendor window.

2. Click Add.
3. Enter the vendor’s name in the Vendor Name field.
4. Enter the phone number for this vendor in the Phone Number field.
5. Enter a brief description for this vendor in the Description field.
6. Enter the name of your contact person for this vendor in the Vendor Contact field.
7. Click Select Icon to select a vendor icon.
8. Click OK.
Modifying a device vendor

To modify a device vendor:

1. Navigate to **System → Device Vendor**:  
   a. Click the **System** tab from the tabular navigation system on the top.  
   b. Click **Resource Management** on the navigation tree on the left.  
   c. Click **Device Vendor** under **Resource Management** from the navigation system on the left.  
      IMC displays all device vendor information in the **Device Vendor List** displayed in the main pane of the **System → Device Vendor** window.

2. Click the **Modify** icon in the **Device Vendor List** associated with the vendor name you want to modify.

3. Modify the vendor’s name as needed in the **Vendor Name** field.

4. Modify the phone number for this vendor as needed in the **Phone Number** field.

5. Modify the description for this vendor as needed in the **Description** field.

6. Modify the name of your contact person for this vendor as needed in the **Vendor Contact** field.

7. Modify the vendor icon as needed in the **Vendor Icon** field.

8. Click **OK**.

   You can modify all device vendor settings for manually added vendors, but cannot modify the **Vendor Name** and **Icon** settings for system-defined vendors.

Deleting a device vendor

To delete a device vendor:

1. Navigate to **System → Device Vendor**:  
   a. Click the **System** tab from the tabular navigation system on the top.  
   b. Click **Resource Management** on the navigation tree on the left.  
   c. Click **Device Vendor** under **Resource Management** from the navigation system on the left.  
      IMC displays all device vendor information in the **Device Vendor List** displayed in the main pane of the **System → Device Vendor** window.

2. Click the **Delete** icon in the **Device Vendor List** associated with the vendor name you want to delete.

3. Click **OK** to confirm deletion of the selected device vendor.

Configuring device series

Device series information is a required field when creating a new device model, device model information is used in IMC to categorize devices and device categorization is used in many IMC functions including discovery, alarming and reporting. Therefore, managing device series information is an essential element of IMC management and one that you should maintain for optimal use of IMC functions.

Viewing the device series list

To view the device series list:
1. Navigate to **System→Device Series**:
   a. Click the **System** tab from the tabular navigation system on the top.
   b. Click **Resource Management** on the navigation tree on the left.
   c. Click Device Series under **Resource Management** from the navigation system on the left.
   IMC displays all device series information in the **Device Series List** displayed in the main pane of the **System→Device Series** window.

**Device Series List**

- **Series Name**: Contains the device series name.
- **Vendor**: Contains the vendor’s name.
- **Series Type**: Identifies whether the device series list entry is system or user-defined.
- **Description**: Contains a description of the device series.
- **Modify**: Contains an icon for navigating to the **Modify Device Series** page for the associated device series entry.
- **Delete**: Contains an icon for deleting the associated device series entry.

You can sort the **Device Series List** by the **Series Name**, **Vendor**, and **Series Type** fields. Click the column label to sort the list by the selected field. The column label is a toggle switch that allows you to toggle between the various sort options specific to each field.

If the device series list contains enough entries, the following navigational aids are displayed:

- Click to page forward in the **Device Series List**.
- Click to page forward to the end of the **Device Series List**.
- Click to page backward in the **Device Series List**.
- Click to page backward to the front of the **Device Series List**.

2. Click **8, 15, 50, 100, or 200** from the right side of the main pane to configure how many items per page you want to view.

**Adding a device series**

To add device series:

1. Navigate to **System→Device Series**:
   a. Click the **System** tab from the tabular navigation system on the top.
   b. Click **Resource Management** on the navigation tree on the left.
   c. Click Device Series under **Resource Management** from the navigation system on the left.
   IMC displays all device series information in the **Device Series List** displayed in the main pane of the **System→Device Series** window.

2. Click **Add**.

Enter the following information in the **Add Device Series** page:

3. Enter the name of the series in the **Series Name** field.

4. Select the vendor for this device series from the **Vendor** list.
   If the vendor does not exist, you can add it.
5. To add vendors, see "Adding a device vendor" (page 93).
6. Enter a description of the device series in the **Description** field.
7. Click **OK**.

### Modifying a device series

To modify a device series:

1. Navigate to **System→Device Series**:
   a. Click the **System** tab from the tabular navigation system on the top.
   b. Click **Resource Management** on the navigation tree on the left.
   c. Click **Device Series** under **Resource Management** from the navigation system on the left.
      IMC displays all device series information in the **Device Series List** displayed in the main pane of the **System→Device Series** window.
2. Click the **Modify** icon in the **Device Series List** associated with the device series you want to modify.
3. Modify the name for the series in the **Series Name** field as needed.
4. Select the vendor for this device series from the **Vendor** list.
   If the vendor does not exist, you can add it.
5. To add vendors, see the previous section of this chapter on "Adding a device vendor" (page 93).
6. Modify the description of the device series in the **Description** field.
7. Click **OK**.

### Deleting a device series

To delete a device series:

1. Navigate to **System→Device Series**:
   a. Click the **System** tab from the tabular navigation system on the top.
   b. Click **Resource Management** on the navigation tree on the left.
   c. Click **Device Series** under **Resource Management** from the navigation system on the left.
      IMC displays all device series information in the **Device Series List** displayed in the main pane of the **System→Device Series** window.
2. Click the **Delete** icon in the **Device Series List** associated with the device series you want to delete.
3. Click **OK** to confirm deletion of the selected device series.

### Configuring device models

IMC uses device model information to categorize devices. These categories are used throughout IMC to discover, manage and report on network resources. You can manage IMC’s categories by adding device model information for devices in the network infrastructure.

In this section, we will explore the **Device Model List** that displays all devices models in IMC before examining how to add, modify, and delete device models.
Viewing the device model list

To view the device model list:

1. Navigate to **System→Device Model**:
   - a. Click the **System** tab from the tabular navigation system on the top.
   - b. Click **Resource Management** on the navigation tree on the left.
   - c. Click **Device Model** under **Resource Management** from the navigation system on the left.

IMC displays all device model information in the **Device Model List** displayed in the main pane of the **System→Device Model** window.

**Device model list**

- **Model Name**: Contains the device model name.
- **sysOID**: Contains the sysOID or system Object ID for the device model.
- **Series**: Identifies the Device Series family that the device model belongs to.
- **Category**: Identifies IMC’s classification for the device model.
- **Type**: Identifies whether the associated device model is system or user-defined.
- **Modify**: Contains an icon for navigating to the **Modify Device Model** page for the associated device model entry.
- **Delete**: Contains an icon for deleting the associated device model entry.

You can sort the **Device Model List** by the **Model Name**, **sysOID**, **Series**, **Category**, and **Type** fields. Click the column label to sort the list by the selected field. The column label is a toggle switch that allows you to toggle between the various sort options specific to each field.

If the device model list contains enough entries, the following navigational aids are displayed:

- Click **»** to page forward in the **Device Model List**.
- Click **«** to page backward in the **Device Model List**.
- Click **«** to page backward to the front of the **Device Model List**.
- Click **»** to page forward to the end of the **Device Model List**.

2. Click **8**, **15**, **50**, **100**, or **200** from the right side of the main pane to configure how many items per page you want to view.

Adding a device model

To add a device model:

1. Navigate to **System→Device Model**:
   - a. Click the **System** tab from the tabular navigation system on the top.
   - b. Click **Resource Management** on the navigation tree on the left.
   - c. Click **Device Model** under **Resource Management** from the navigation system on the left.

IMC displays all device model information in the **Device Model List** displayed in the main pane of the **System→Device Model** window.

2. Click **Add**.
3. Enter the vendor’s name for the device model in the **Model Name** field.
4. Enter the system object ID in the **sysOID** field or use the **Query Device** feature in IMC to auto populate the **sysOID** field.

There are two ways to query in the **Query Device** feature – **By View** or through **Advanced** query.

5. To auto populate the **sysOID** field using the Query **By View** feature, see "Adding devices by View" (page 85) and "Adding devices by Advanced query" (page 85). You can also auto populate the **sysOID** field by using the **Advanced** query option.

To use the **Query Device** option, the device must already exist.

6. To add devices, see "Adding devices in IMC" (page 154).

7. Select the vendor name from the **Vendor** list.

If the vendor does not exist, you can add it.

8. To add vendors, see "Adding a device vendor" (page 93).

9. Select the device series from the **Series** list.

If the device series does not exist, you can add it.

10. To add a device series, see "Adding a device series" (page 95).

11. Select the device category from the **Category** list.

12. Enter a brief description for this device model in the **Description** field.

13. Click **OK**.

**Modifying a device model**

To modify a device model:

1. Navigate to **System**→**Device Model**:
   a. Click the **System** tab from the tabular navigation system on the top.
   b. Click **Resource Management** on the navigation tree on the left.
   c. Click **Device Model** under **Resource Management** from the navigation system on the left.
   IMC displays all device model information in the **Device Model List** displayed in the main pane of the **System**→**Device Model** window.

2. Click the **Modify** icon in the **Device Model List** associated with the device model you want to modify.

3. Modify the vendor’s name for the device model in the **Model Name** field.

4. Modify the system object ID in the **sysOID** field or use the **Query Device** feature in IMC to auto populate the **sysOID** field.

There are two ways to query in the **Query Device** feature – **By View** or through **Advanced** query.

5. To auto populate the **sysOID** field using the Query **By View** feature, see "Adding devices by View" (page 85) and "Adding devices by Advanced query" (page 85).

6. To change the vendor name, select the vendor name from the **Vendor** list.

If the vendor does not exist, you can add it.

7. To add vendors, see "Adding a device vendor" (page 93).

8. To change the device series, select the device series from the **Series** list.

If the device series does not exist, you can add it.
9. To add a device series, see "Adding a device series" (page 95).

10. To change the device category, select the device category from the Category list.

11. Modify the description for this device model in the Description field.

12. Click OK.

Deleting a device model

To delete a device model:

1. Navigate to System→Device Model:
   a. Click the System tab from the tabular navigation system on the top.
   b. Click Resource Management on the navigation tree on the left.
   c. Click ➕ Device Model under Resource Management from the navigation system on the left.
      IMC displays all device model information in the Device Model List displayed in the main pane of the System→Device Model window.

2. Click the Delete icon in the Device Model List associated with the device model you want to delete.

3. Click OK to confirm deletion of the selected device model.

Configuring device categories

IMC divides devices into 14 categories, including Desktops, Switches, Printers, and Routers. You can define other categories as needed.

Viewing the device category list

To view the device category list:

1. Navigate to System→Device Category:
   a. Click the System tab from the tabular navigation system on the top.
   b. Click Resource Management on the navigation tree on the left.
   c. Click ➕ Device Category under Resource Management from the navigation system on the left.
      IMC displays all device category information in the Device Category List displayed in the main pane of the System→Device Category window.

Device Category List

- **Category Name**: Contains the device category name.
- **Type**: Identifies whether the associated device category is system or user-defined.
- **Display Default**: Identifies whether the device category is displayed by default under Device View in the navigation tree.
- **Display Picture**: Contains the picture of the associated device category.
- **Modify**: Contains an icon for navigating to the Modify Device Category page for the associated device series entry.
- **Delete**: Contains an icon for deleting the associated device series entry.
You can sort the **Device Category List** by the **Category Name**, **Type**, **Display Default** fields. Click the column label to sort the list by the selected field. The column label is a toggle switch that allows you to toggle between the various sort options specific to each field.

If the device category list contains enough entries, the following navigational aids are displayed:

- Click to page forward in the **Device Category List**.
- Click to page forward to the end of the **Device Category List**.
- Click to page backward in the **Device Category List**.
- Click to page backward to the front of the **Device Category List**.

2. Click **8, 15, 50, 100, or 200** from the right side of the main pane to configure how many items per page you want to view.

### Adding a device category

To add a device category:

1. Navigate to **System→Device Category**:
   a. Click the **System** tab from the tabular navigation system on the top.
   b. Click **Resource Management** on the navigation tree on the left.
   c. Click **Device Category** under **Resource Management** from the navigation system on the left.

   IMC displays all device series information in the **Device Category List** displayed in the main pane of the **System→Device Category** window.

2. Click **Add**.
3. Enter the category’s name for the device model in the **Category Name** field.
4. Click the icon or the **Select Icon** button, and select an icon from the list.
5. Click **OK**.

### Modifying a device category

To modify a device category:

1. Navigate to **System→Device Category**:
   a. Click the **System** tab from the tabular navigation system on the top.
   b. Click **Resource Management** on the navigation tree on the left.
   c. Click **Device Category** under **Resource Management** from the navigation system on the left.

   IMC displays all device series information in the **Device Category List** displayed in the main pane of the **System→Device Category** window.

2. Click the **Modify** icon in the **Device Category List** associated with the device category you want to modify.
3. Modify the category’s name for the device category in the **Category Name** field.
4. Click the icon or the **Select Icon** button, and select an icon from the list.
5. Click **OK**.

### Deleting a device category

To delete a device category:
1. Navigate to System→Device Category:
   a. Click the System tab from the tabular navigation system on the top.
   b. Click Resource Management on the navigation tree on the left.
   c. Click Device Category under Resource Management from the navigation system on the left.
   IMC displays all device series information in the Device Category List displayed in the main pane of the System→Device Category window.

2. Click the Delete icon in the Device Category List associated with the device category you want to delete.

3. Click OK to confirm deletion of the selected device category.

Managing filters to filter interfaces

A filter is used by port groups to filter interfaces.

Viewing filter list

To view the filter list:

1. Navigate to System→Filter List:
   a. Click the System tab from the tabular navigation system on the top.
   b. Click Resource Management on the navigation tree on the left.
   c. Click Filter under Resource Management from the navigation system on the left.
   IMC displays information about all filters in the Filter List in the main pane of the System→Filter List window.

Filter List

- **Name**: Contains the name of the associated filter.
- **Object**: Contains the object to be filtered, which is Interface.
- **Type**: Contains the type of the associated filter. Options include System-Defined and User-Defined.
- **Created by**: Contains the name of the operator who created the associated filter.
- **Created at**: Contains the time when the associated filter was created.
- **Description**: Contains a description for the associated filter.
- **Delete**: Contains an icon for deleting the associated filter.

You can sort the Filter List by the Name, Object, Type, Created by, and Created at fields. Click the column label to sort the list by the selected field. The column label is a toggle switch that allows you to toggle between the various sort options specific to each field.

The name you assign to a filter is used to identify the filter. Therefore, assigning a descriptive and meaningful name to a filter aids you in navigating quickly and easily to filter the interface list.

If the filter list contains enough entries, the following navigational aids are displayed:

- Click to page forward in the Filter List.
- Click to page forward to the end of the Filter List.
- Click to page backward in the Filter List.
- Click to page backward to the front of the Filter List.
2. Click 8, 15, 50, 100, or 200 from the right side of the main pane to configure how many items per page you want to view.

Adding a filter

IMC does not offer the function of directly adding filters to the Filter List. Instead, you can save interface query criteria as a filter when using the Advanced Query option.

To add a filter:

1. Navigate to the Advanced Query page:
2. Click the Advanced link located in the upper right corner of the IMC page.
3. Click the radio button ☑️ to the left of Query Interfaces to perform search for interfaces.
4. Enter the following information in the Advanced Query page:
   - Interface Alias—IMC supports fuzzy matching for this field. You can enter a partial or complete name for the interface alias you want to locate in the Interface Alias field.
   - Interface Type—Select the interface type you want to search from the Interface Type list.
   - Speed—Select the interfaces speed from the Speed list.
   - Interface IP—Enter the IP address of the interface you want to search for in the Interface IP field. Select Fuzzy from the list located to the right of the Interface IP if you want to enter a partial IP address. Select Exact from this list if you want IMC to search for an exact match for the IP address you have entered.
   - MAC Address—Enter the MAC address of the interface you want to search for in the MAC Address field. IMC supports fuzzy matching for this field. You can enter a partial or complete MAC address for the interfaces you want to locate.
   - Device Label—Enter the name of the device to which the interface belongs in the Device Label field. IMC supports fuzzy matching for this field. Therefore, you can enter a partial or complete string for the device name.
   - Device IP—Enter the IP address of the device to which the interface belongs in the Device IP field. Select Fuzzy from the list located to the right of the Device IP if you want to enter a partial IP address. Select Exact from this list if you want IMC to search for an exact match for the IP address you have entered.
   - Management Status—Select the management status of the interfaces you want to search for from the Management Status list.
   - Operational Status—Select the operational status of the interfaces you want to search for from the Operational Status list.
5. Click Save as Filter to save a filter.
   The Save as Filter dialog box appears.
6. Enter the filter name in Name field.
7. Enter the description for the associated filter in the Description field.
8. Click OK.

Deleting a filter

To delete a filter:

1. Navigate to System→Filter List:
   a. Click the System tab from the tabular navigation system on the top.
   b. Click Resource Management on the navigation tree on the left.
c. Click Filter under Resource Management from the navigation system on the left. IMC displays information about all filters in the Filter List in the main pane of the System→Filter List window.

2. Click the Delete icon in the Filter List associated with the filter you want to delete.

3. Click OK to confirm deletion of the selected filter.

Operator management: managing secure access to IMC

Operator Management offers you powerful control over resources in the network infrastructure. Sound network infrastructure security policy and practice should include securing IMC through effective use of the IMC security features and functions found in Operator Management under the System tab.

Access and management rights to network resources granted to or rescinded from IMC operators through the use of three features: Operator Groups, Device Groups, and Device Views. It is through the configuration of the operator account itself that these three features converge to define the specific set of access and management rights and restrictions for each operator.

**Operator groups** allow you to grant or restrict access and rights to IMC features and functions. You can create custom operator groups and grant or restrict operator access to the following IMC functions: Resource Manager, Alarm Management, Intelligent Configuration Center, Report Management, Performance Management, Network Asset Management, Security Control Center, Data Analysis, Guest Access Management, ACL Management, VLAN Management, Syslog Management, NE Management, and VNM Management. Once groups are created, you can add operators to an operator group to grant or restrict their access to these IMC features.

**Custom views** allow you to grant or restrict access to devices by creating custom views. Custom Views serve two purposes: to grant or restrict access and management rights to a set of devices; and to provide operators with a logical view of devices for quick and efficient access to managed devices. You create custom views that group devices logically. These views become available through the Resource tab to operators when they have been granted rights to them. You then grant or restrict operator access to one or more custom views when configuring individual operator accounts.

**Device groups** give you a layer of refinement for granting or restricting operator access and rights to devices managed by IMC. While Device Views allow you to group devices logically, device groups enable you to group devices by device type or by any other logical grouping. You can create custom groups and add one or more devices to a group. Once device groups are created, you can assign operators to a device group, thus granting them access and rights to manage the devices in that group. Operators have access only to those devices that are included in the device groups that they have been granted rights to. In other words, operators do not have access and cannot even view devices that are not included in the groups that they have been granted access to. Device Groups serve to grant access to devices only; they are not visible as device groups in IMC features and functions.

Once you have created operator groups, custom views, and device groups and populated device views and groups with devices, you are then ready to assign or restrict access and management rights to network resources through the configuration of operator accounts. In operator accounts, you assign to each operator membership in an operator group and access and management rights to device views and groups. Adding an operator to the Administrator Group grants that operator rights to all devices, all device groups and all views, without exception. Thus, to use views and device groups to manage rights and restrictions to IMC, you must add operators to either the maintainer or the viewer group.
The sum of operator privileges and restrictions configured in add or modify operator account pages determines ultimately what devices become visible to each operator in IMC through custom views or IMC’s system defined views. The rights and restrictions in operator accounts also determine which performance reports, alarms, and other IMC management and reporting views and features operators see as operators only view information and features for devices over which they have rights.

In addition to access and rights management features discussed above, IMC offers other features to secure access to IMC and the resources managed by it. You have three options for operator authentication to IMC: local IMC password management, RADIUS or LDAP authentication. You can configure authentication services via RADIUS or LDAP using the Authentication Server feature found under Operator Management.

You can control login access to IMC via IP address access control lists in the Login Control Template function under Operator Management.

You can also set password strategies that apply to all operators in the Password Strategy function under Operator Management.

Finally, IMC you apply these configurations individually when creating operator accounts.

Managing operator groups

In IMC, you can create custom defined operator groups that assign or restrict IMC service and component level privileges to members of the operator groups. Once created, custom groups then appear as configuration options when adding operators to IMC.

You can create custom operator groups and grant or restrict operator access to the following IMC functions: Resource Management, Alarm Management, Intelligent Configuration Center, Report Management, Performance Management, Network Asset Management, Security Control Center, Guest Access Management, ACL Management, VLAN Management, Syslog Management, Data Analysis Management, and Data Analyzer. Once groups are created, you can add operators to an operator group to grant or restrict their access to these IMC features.

Securing IMC therefore begins with defining and implementing operator groups that map the roles and responsibilities of individuals and groups within the organization to the services and components within IMC.

Once you have identified the various groups within your support organization and their roles and responsibilities and how they map to IMC services and components, you are ready to begin creating operator groups.

Viewing the operator group list

To view the operator group list:

   a. Click the System tab from the tabular navigation system on the top.
   b. Click Operator Management on the navigation tree on the left.
   c. Click Operator Group under Operator Management from the navigation system on the left. IMC displays all operator groups in the Operator Group List displayed in the main pane of the System→Operator Group window.

Operator group list
- Group Name: Contains the operator group name.
Privilege: Contains privilege level for the associated group. There are three privilege levels in IMC: ADMIN, Maintainer, and Viewer.

Description: Contains a description for the associated operator group.

Copy: Contains an icon for navigating to the Add Operator Group page for the associated device series entry.

Modify: Contains an icon for navigating to the Modify Operator Group page for the associated device series entry.

Delete: Contains an icon for deleting the associated device series entry.

You can sort the Operator Group List by the Group Name, Privilege, and Description fields. Click the column label to sort the list by the selected field. The column label is a toggle switch that allows you to toggle between the various sort options specific to each field.

If the operator group list contains enough entries, the following navigational aids appear.

- Click  to page forward in the Operator Group List.
- Click  to page forward to the end of the Operator Group List.
- Click  to page backward in the Operator Group List.
- Click  to page backward to the front of the Operator Group List.

2. Click 8, 15, 50, 100, or 200 from the right side of the main pane to configure how many items per page you want to view.

### Adding an operator group

To add an operator group:

   a. Click the System tab from the tabular navigation system on the top.
   b. Click Operator Management on the navigation tree on the left.
   c. Click Operator Group under Operator Management from the navigation system on the left.

   IMC displays all operator groups in the Operator Group List displayed in the main pane of the System→Operator Group window.

2. Click Add.

3. Enter a unique name for the group you want to create in the Group Name field.

4. Select the group’s privilege level from the Privilege list.

Options include:

- **ADMIN**: Operators with the ADMIN level privilege has access to all operations and resources available in IMC. Only the admin account that is created during installation and operators who have been assigned to the Administrator Group and therefore given the ADMIN privilege level have control over the following IMC functions: operator management, device group management, user group management, login control template management, password strategy management and system parameter settings. Select this option if you want to grant access to all IMC features and functions as well as all devices, users, and services managed by IMC to all operators that will be members of this group.

- **Maintainer**: Operators who have or will be assigned to the Maintainer group and therefore have the Maintainer privilege level rights and control over all operations for devices, users, and services within the groups and custom views assigned to the Maintainer Group. Select this option if you
want to grant access to IMC features and functions and devices, users, and services managed by IMC to all operators that will be members of this group.

- **Viewer**: Operators who have been or will be assigned to the Viewer group and therefore have a Viewer privilege level have read-only access devices, users, and services within the groups and views assigned to its Viewer Group. Select this option if you want to grant read-only access to IMC features and managed resources to all operators of this group.

5. Enter a description for the operator group in the **Description** field.

6. Click the **Expand ALL** icon to view all **Operator Privileges**.

   This step grants or restricts access to IMC features for the **Operator Group**.

7. Deselect any privileges you want to revoke for this operator group by clicking the checked box to remove the check mark.

8. Click **OK** to create the **Operator Group**.

   You cannot modify the name of an operator group once it has been created.

**Copying an Operator Group**

To copy an operator group:

1. Navigate to **System**→**Operator Group**.
   a. Click the **System** tab from the tabular navigation system on the top.
   b. Click **Operator Management** on the navigation tree on the left.
   c. Click **Operator Group** under **Operator Management** from the navigation system on the left. IMC displays all operator groups in the **Operator Group List** displayed in the main pane of the **System**→**Operator Group** window.

2. Click the **Copy** icon in the **Operator Group List** associated with the operator group you want to copy.

3. Modify the group name as needed in the **Group Name** field.

4. Select the group’s privilege level from the **Privilege** list.

   Options include:
   - **ADMIN**: Operators with the **ADMIN** level privilege has access to all operations and resources available in IMC. Only the admin account that is created during installation and operators who have been assigned to the Administrator Group and therefore given the **ADMIN** privilege level have control over the following IMC functions: operator management, device group management, user group management, login control template management, password strategy management and system parameter settings. Select this option if you want to grant access to all IMC features and functions as well as all devices, users, and services managed by IMC to all operators that will be members of this group.
   - **Maintainer**: Operators who have or will be assigned to the Maintainer group and therefore have the **Maintainer** privilege level rights and control over all operations for devices, users, and services within the groups and custom views assigned to the **Maintainer Group**. Select this option if you want to grant access to IMC features and functions and devices, users, and services managed by IMC to all operators that will be members of this group.
   - **Viewer**: Operators who have been or will be assigned to the Viewer group and therefore have a Viewer privilege level have read-only access devices, users, and services within the groups and
views assigned to its **Viewer Group**. Select this option if you want to grant read-only access to IMC features and managed resources to all operators of this group.

5. Modify the description as needed in the **Description** field.

6. Click the **Expand All** icon  + to view all **Operator Privileges**.

7. Do one of the following:
   - Deselect any privileges you want to revoke for this operator group by clicking the checked box ✔ to remove the check mark, or
   - Select any privileges you want to add by clicking the check box  ✔ to enable the associated privilege.

8. Click **OK** to create a copy of the operator group.

**Modifying an operator group**

To modify an operator group:

1. Navigate to **System**→**Operator Group**.
   a. Click the **System** tab from the tabular navigation system on the top.
   b. Click **Operator Management** on the navigation tree on the left.
   c. Click **Operator Group** under **Operator Management** from the navigation system on the left. IMC displays all operator groups in the **Operator Group List** displayed in the main pane of the **System**→**Operator Group** window.

2. Click the **Modify** icon  📝 in the **Operator Group List** associated with the operator group you want to modify.

3. Select the group’s privilege level from the **Privilege** list.

   Options include:
   - **ADMIN**: Operators with the **ADMIN** level privilege has access to all operations and resources available in IMC. Only the admin account that is created during installation and operators who have been assigned to the Administrator Group and therefore given the **ADMIN** privilege level have control over the following IMC functions: operator management, device group management, user group management, login control template management, password strategy management and system parameter settings. Select this option if you want to grant access to all IMC features and functions as well as all devices, users, and services managed by IMC to all operators that will be members of this group.
   - **Maintainer**: Operators who have or will be assigned to the Maintainer group and therefore have the **Maintainer** privilege level rights and control over all operations for devices, users, and services within the groups and custom views assigned to the **Maintainer Group**. Select this option if you want to grant access to IMC features and functions and devices, users, and services managed by IMC to all operators that will be members of this group.
   - **Viewer**: Operators who have been or will be assigned to the Viewer group and therefore have a **Viewer** privilege level have read-only access devices, users, and services within the groups and views assigned to its **Viewer Group**. Select this option if you want to grant read-only access to IMC features and managed resources to all operators of this group.

4. Modify the description as needed in the **Description** field.
5. Click the **Expand All** icon to view all Operator Privileges.

6. Do one of the following:
   - Deselect any privileges you want to revoke for this operator group by clicking the checked box to remove the check mark, or
   - Select any privileges you want to add by clicking on the checkbox to enable that privilege.

7. Click **OK**.

⚠️ **WARNING:**

An operator group cannot be modified while members of the group are online. All members of a group must be logged off before changes to the Operator Group can be completed. Administrators or operators with ADMIN privileges can log users off using the Online Operators feature in IMC. For more information on this feature, see “Managing online IMC operator access” (page 124).

---

### Deleting an operator group

To delete an operator group:

1. Navigate to **System**→**Operator Group**.
   - Click the **System** tab from the tabular navigation system on the top.
   - Click **Operator Management** on the navigation tree on the left.
   - Click **Operator Group** under **Operator Management** from the navigation system on the left. IMC displays all operator groups in the **Operator Group List** displayed in the main pane of the **System**→**Operator Group** window.

2. Click the **Delete** icon in the **Operator Group List** associated with the operator group you want to delete.

3. Click **OK** to confirm deletion of the selected operator group.

⚠️ **WARNING:**

An operator group cannot be deleted while members of the group are online. All members of a group must be logged off before any changes to the Operator Group can be completed. For more information on logging operators off, see “Managing online IMC operator access” (page 124).

---

### Securing IMC access via authentication services

To further secure access to IMC and to support unified username and password management, IMC supports the use of login authentication services for both RADIUS and LDAP.

#### Configuring IMC to use RADIUS authentication services

Only administrators or operators who are members of a group with the ADMIN privilege level can configure RADIUS authentication services. To configure RADIUS authentication:

1. Navigate to **System**→**Authentication Server**.
   - Click the **System** tab from the tabular navigation system on the top.
   - Click **Operator Management** on the navigation tree on the left.
c. Click Authentication Server under Operator Management from the navigation system on the left. The Authentication Server configuration page appears.

2. Enter the following information in RADIUS Server portion of the Authentication Server page:
   a. Authentication Type: Select the RADIUS authentication type, PAP or CHAP from the list under RADIUS Server. This choice must match the authentication type configured on the RADIUS server.
   b. Primary Server: Enter the IP address or host name of the primary RADIUS Server.
   c. Secondary Server: Enter the IP address or host name of the secondary RADIUS Server.
   d. Authentication Port: Enter the port number used by the RADIUS server for authentication in the field. The default port number is 1812.
   e. Shared Secret: Enter the shared secret for authentication packets. What is configured here must match what is configured on the RADIUS server.

3. Click OK to confirm the RADIUS service authentication configuration.

Modifying RADIUS authentication service configuration

To modify an existing RADIUS configuration:

1. Navigate to System→Authentication Server.
   a. Click the System tab from the tabular navigation system on the top.
   b. Click Operator Management on the navigation tree on the left.
   c. Click Authentication Server under Operator Management from the navigation system on the left.

The Authentication Server configuration page appears.

2. Enter the following information in the Authentication Server page:
   a. Authentication Type: Modify the RADIUS authentication type, PAP or CHAP from the list under RADIUS Server. This choice must match the authentication type configured on the RADIUS server.
   b. Primary Server: Modify the IP address or host name of the primary RADIUS Server.
   c. Secondary Server: Modify the IP address or host name of the secondary RADIUS Server.
   d. Authentication Port: Modify the port number used by the RADIUS server for authentication in the field. The default port number is 1812.
   e. Shared Secret: Modify the shared secret for authentication packets. What is configured here must match what is configured on the RADIUS server.

3. Click OK to confirm your modifications to the RADIUS service authentication configuration.

Configuring IMC to use LDAP authentication services

Only administrators or operators who are members of a group with the ADMIN privilege level can configure LDAP authentication services. To configure LDAP authentication:

1. Navigate to System→Authentication Server.
   a. Click the System tab from the tabular navigation system on the top.
   b. Click Operator Management on the navigation tree on the left.
   c. Click Authentication Server under Operator Management from the navigation system on the left.
The Authentication Server configuration page appears.

2. Enter the following information in the Authentication Server page:
   - **LDAP Version**: Select the LDAP version, 2 or 3 from the list. The option selected here must match the configuration of the LDAP server.
   - **Server Type**: Select LDAP server type from the list. IMC supports **Generic LDAP Services** as well as **Microsoft Active Directory**.
   - **Server Address**: Enter the IP address or host name of the LDAP Server in the field provided.
   - **Server Port**: Enter the port number used by the LDAP server for authentication in this field. The default port number is 389.
   - **Base DN**: Enter the Base DN value to be used for communication with the LDAP server. The Base DN must match what is configured on the LDAP authentication server.
   - **Admin DN**: Enter the Admin DN value to be used for communication with the LDAP server. The Administrator DN must match what is configured on the LDAP authentication server.
   - **Admin Password**: Enter the Admin password to be used for communication with the LDAP server. The admin password must match what is configured on the LDAP authentication server.
   - **Username Attribute**: Enter the username attribute to be used for obtaining user information from the LDAP server. The username attribute must match what is configured on the LDAP authentication server.

3. Click **OK** to confirm the LDAP service authentication configuration.

**Modifying LDAP authentication service configuration**

To modify an existing LDAP authentication service configuration:

1. Navigate to **System → Authentication Server**.
   - Click the **System** tab from the tabular navigation system on the top.
   - Click **Operator Management** on the navigation tree on the left.
   - Click **Authentication Server** under **Operator Management** from the navigation system on the left.

   The Authentication Server configuration page appears.

2. Enter the following information in the Authentication Server page:
   - **LDAP Version**: Modify the LDAP version, by selecting V2 or V3 from the list. This must match the configuration on the LDAP server.
   - **Server Type**: Modify the LDAP server type by selecting the type from the list. IMC supports **Generic LDAP Services** as well as **Microsoft Active Directory**.
   - **Server Address**: Modify the IP address or host name of the LDAP Server in the field provided.
   - **Server Port**: Modify the port number used by the LDAP server for authentication in this field. The default port number is 389.
   - **Base DN**: Modify the Base DN value to be used for communication with the LDAP server. The Base DN must match what is configured on the LDAP authentication server.
   - **Admin DN**: Modify the Admin DN value to be used for communication with the LDAP server. The Administrator DN must match what is configured on the LDAP authentication server.
   - **Admin Password**: Modify the Admin password to be used for communication with the LDAP server. The admin password must match what is configured on the LDAP authentication server.
- **Username Attribute**: Modify the Username attribute to be used for obtaining user information from the LDAP server. The username attribute must match what is configured on the LDAP authentication server.

3. Click **OK** to confirm the LDAP service authentication configuration.

**Securing IMC through operator login control templates**

IMC extends the concept of access control to the desktop by enabling you to permit or deny operator access to IMC based on individual IP addresses as well as IP address ranges. These login control templates can then be applied to operator accounts to permit or deny IMC access to IMC based on the individual operator’s IP address.

**Viewing the login control template list**

To view the login control template list:

1. Navigate to **System→Login Control Template**.
   a. Click the **System** tab from the tabular navigation system on the top.
   b. Click **Operator Management** on the navigation tree on the left.
   c. Click **Login Control Template** under **Operator Management** from the navigation system on the left.
      
      The **Login Control Template** page appears.

**Login control template list**

- **Login Control Name**: Contains the name assigned to the login control template.
- **Start IP**: Contains the IP address that defines the first IP address in the range of IP addresses controlled by this template.
- **End IP**: Contains the IP address that defines the last IP address in the range of IP addresses controlled by this template.
- **Action**: Identifies what action is taken by the login control template. The two options for login control templates are **Permit** and **Deny**.
- **Description**: Contains a description for the associated login control template.
- **Modify**: Contains an icon for navigating to the **Modify** page for the associated login control template.
- **Delete**: Contains an icon for navigating to the **Delete** page for the associated login control template.

If the login control template list contains enough entries, the following navigational aids appear.

- Click **next** to page forward in the **Login Control Template List**.
- Click **last** to page forward to the end of the **Login Control Template List**.
- Click **first** to page backward in the **Login Control Template List**.
- Click **previous** to page backward to the front of the **Login Control Template List**.

2. Click **8, 15, 50, 100, or 200** from the right side of the main pane to configure how many items per page you want to view.
Adding a login control template

Only you or operators who are members of a group with the ADMIN privilege level can manage Login Control Templates. To add a login control template:

1. Navigate to System → Login Control Template.
   a. Click the System tab from the tabular navigation system on the top.
   b. Click Operator Management on the navigation tree on the left.
   c. Click Login Control Template under Operator Management from the navigation system on the left.

      The Login Control Template page appears.

2. Click Add.

3. Enter the following information in the Login Control Template window:
   a. Enter the name of the login control template in the Login Control Name field.
   b. Enter the first IP address in the address range you want to permit or deny access to in the Start IP field. If you are entering a single IP address, enter the same address in the Start IP and the End IP address fields.
   c. Enter the last IP address in the address range you want to permit or deny access to in the End IP field. If you are entering a single IP address, enter the same address in the Start IP and the End IP address fields.
   d. Select the action you want to implement for this IP address or IP address range from the Action list. Options include Permit, which enables IMC access from any IP address in the specified range, and Deny, which prohibits IMC access from any IP address in the specified range.
   e. Enter a description for this login control template in the Description field provided.

4. Click OK.

Modifying a login control template

Changes to login control lists take effect the next time the operators affected by the template log in. To modify a login control template:

1. Navigate to System → Login Control Template.
   a. Click the System tab from the tabular navigation system on the top.
   b. Click Operator Management on the navigation tree on the left.
   c. Click Login Control Template under Operator Management from the navigation system on the left.

      The Login Control Template page appears.

2. Click the Modify icon in the Login Control Template List associated with the login control template you want to modify.

      Login Control Template names cannot be changed once the template has been created.

3. Modify the first IP address in the address range as needed in the Start IP field. If you are entering a single IP address, enter the same address in the Start IP and the End IP address fields.

4. Modify the last IP address in the address range as needed in the End IP field.
If you are entering a single IP address, enter the same address in the **Start IP** and the **End IP** address fields.

5. Select the action you want to implement for this IP address or IP address range from the **Action** list. Options include **Permit**, which enables IMC access from any IP address in the specified range, and **Deny**, which prohibits IMC access from any IP address in the specified range.

6. Modify the description for this login control template in the **Description** field provided.

7. Click **OK**.

### Deleting a login control template

To delete a login control template:

1. Navigate to **System → Login Control**.
   a. Click the **System** tab from the tabular navigation system on the top.
   b. Click **Operator Management** on the navigation tree on the left.
   c. Click **Login Control Template** under **Operator Management** from the navigation system on the left.

   The **Login Control Template** page appears.

2. Click the **Delete** icon in the **Login Control Template** list associated with the login control template you want to delete.

3. Click **OK** to confirm deletion of the selected template.

⚠️ **WARNING:**

Deleting a login control template does not affect operators who are already logged in.

### Establishing IMC password strategies

IMC provides you with the ability to globally define password policies for IMC passwords when local or IMC passwords are used to authenticate operators to IMC.

With IMC’s password strategy feature, you can apply minimum length, password complexity and expiration to all passwords globally. Once applied, password strategies apply to all newly created operators of IMC, effective immediately.

Password expiration policies do not apply to the IMC Administrator account that is created at installation. Administrator passwords never expire.

### Configuring a password strategy

To configure a password strategy:

1. Navigate to **System → Password Strategy**.
2. Click the **System** tab from the tabular navigation system on the top.
3. Click **Operator Management** on the navigation tree on the left.
4. Click **Password Strategy** under **Operator Management** from the navigation system on the left.

   The **Configure Password Strategy** page appears.

5. Enter the following information in the **Configure Password Strategy** page.
a. Select the desired password minimum length from the Min. Length list. Options include passwords that have a length of 6, 8, or 10 characters as well as passwords that cannot have zero length or Cannot Be Zero. The default setting is Cannot Be Zero.

b. Select the desired password complexity strategy from the Complexity list. Options include 1) No Requirement, 2) Must Contain Letters and Numbers, 3) Must Contain Special Characters, shown in Table 2 (page 114) and 4) Must Contain Letters, Numbers, and Special Characters. The default setting is No Requirement.

c. Validity Period: Select the length of time for which passwords are valid in the Validity Period list. Options are Permanent, 30 days, 60 days, 90 days, and 12 Months. The default setting is Permanent.

6. Click OK.

Changes to password strategies do not affect operators who have established accounts prior to the implementation of or changes to IMC password strategies. However, changes take effect immediately for all newly created operators.

Table 2 Special characters

<table>
<thead>
<tr>
<th>Character</th>
<th>Name</th>
<th>Character</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>~</td>
<td>Tilde</td>
<td>'</td>
<td>Apostrophe or single quotation</td>
</tr>
<tr>
<td>!</td>
<td>Exclamation mark</td>
<td>@</td>
<td>At sign</td>
</tr>
<tr>
<td>#</td>
<td>Pound sign</td>
<td>$</td>
<td>Dollar sign</td>
</tr>
<tr>
<td>%</td>
<td>Percent sign</td>
<td>^</td>
<td>Caret</td>
</tr>
<tr>
<td>&amp;</td>
<td>Ampersand</td>
<td>*</td>
<td>Asterisk</td>
</tr>
<tr>
<td>( )</td>
<td>Parenthesis</td>
<td>=</td>
<td>Equal sign</td>
</tr>
<tr>
<td>+</td>
<td>Plus sign</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-</td>
<td>Hyphen</td>
<td></td>
<td>Underscore</td>
</tr>
<tr>
<td>[ ]</td>
<td>Square brackets</td>
<td>{ }</td>
<td>Braces</td>
</tr>
<tr>
<td>:</td>
<td>Colon</td>
<td>;</td>
<td>Semicolon</td>
</tr>
<tr>
<td>\</td>
<td>Backslash</td>
<td>&quot;</td>
<td>Double quotation</td>
</tr>
<tr>
<td>,</td>
<td>Comma</td>
<td>/</td>
<td>Forward slash</td>
</tr>
<tr>
<td>.</td>
<td>Dot</td>
<td>&lt; &gt;</td>
<td>Angle brackets</td>
</tr>
<tr>
<td>?</td>
<td>Question mark</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Managing IMC operators

The individual operator account is where all of the features you have used to grant or restrict access to operator accounts converge. These features include the creation of operator groups, custom views, and device groups. Once these are created, you can grant or restrict access and management rights to network resources using them when they configure individual operator accounts.

With operator accounts, you assign to each operator membership in an operator group and access and management rights to device views and groups. Adding an operator to the administrator group grants that operator rights to all devices, all device groups and all views, without exception. Thus, to use views and
device groups to manage rights and restrictions to IMC, you must add operators to either the maintainer or the viewer group.

The sum of operator privileges and restrictions configured in add or modify operator account pages determines ultimately what devices become visible to each operator in IMC through custom device views or IMC’s system defined views. The rights and restrictions in operator accounts also determine which performance reports, alarms, and other IMC management and reporting views and features operators see as operators only view information and features for devices over which they have rights.

To summarize, once you

1. have created the operator groups that grant or restrict access to IMC features that match the IMC access requirements of your support organization;
2. know which operators need rights to manage which network resources, users and services;
3. have created the device groups and Level 1 custom views as needed.

You are ready to begin creating individual operator accounts. For more information on adding devices and views, see "5 Resource management " (page 153).

Viewing the operator list

To view the operator list:

1. Navigate to System--Operator:
   a. Click the System tab from the tabular navigation system on the top.
   b. Click Operator Management on the navigation tree on the left.
   c. Click Operator under Operator Management from the navigation system on the left.

The Operator page is displayed and a list of all operators is displayed on this page.

- **Login Name**: Contains the IMC user ID or name of the operator.
- **Full Name**: Contains the first and last name for the associated operator.
- **Authentication Type**: Contains the method of authentication configured for the associated operator. Possible values for this field include a local IMC password or Password, RADIUS, or LDAP.
- **Operator Group**: Identifies to which IMC operator group the associated operator belongs.
- **Description**: Contains a description for the associated operator.
- **Modify**: Contains an icon for navigating to the Modify page for the associated operator.
- **Delete**: Contains an icon for navigating to the Delete page for the associated operator.

You can sort the Operator List by the Login Name, Full Name, Authentication Type, Operator Group, and Description fields. Click the column label to sort the list by the selected field. The column label is a toggle switch that allows you to toggle between the various sort options specific to each field.

If the operator list contains enough entries, the following navigational aids are displayed:

- Click ➡️ to page forward in the Operator List.
- Click ⏋️ to page forward to the end of the Operator List.
- Click ⏂️ to page backward in the Operator List.
- Click ⏋️ to page backward to the front of the Operator List.

2. Click 8, 15, 50, 100, or 200 from the right side of the main pane to configure how many items per page you want to view.
Adding an administrator group operator

To add an IMC administrator group operator:

1. Navigate to System → Operator:
   a. Click the System tab from the tabular navigation system on the top.
   b. Click Operator Management on the navigation tree on the left.
   c. Click Operator under Operator Management from the navigation system on the left.
      The Operator page is displayed and a list of all operators is displayed on this page.

2. Click Add.

3. Enter a valid login name in the Login Name field.
   Login name can include alphanumeric characters, underscores (_), and hyphens (-). Although spaces are allowed, HP does not recommend the use of any spaces in a login name as this can cause problems with LDAP and RADIUS authentication.

4. Enter the operator’s first and last name in the Full Name field.

5. Select the password authentication type from the Authentication Type list.
   Options are: IMC local Password, RADIUS, and LDAP.
   You must configure the IMC Authentication Service module for LDAP and RADIUS before operators can authenticate using either one of these forms of authentication.

6. If you are using IMC’s local password feature, enter the operator’s password in the Password field.

7. If you are using IMC’s local password feature, re-enter the operator’s password in the Confirm Password field.
   The Idle Timeout (Minutes) option allows you to configure how long IMC sessions remain open and active while not in use.

8. Select Same as System Settings if you want to apply system wide settings to this operator account.

9. Select Configure Individually.
   The page updates to include a field to the right of the Idle Timeout list.

10. Enter the idle timeout in minutes in this field.

11. Select the Administrator Group from the Operator Group list.

12. Select from the pre-defined IMC operator groups or configure your own.
    To create and configure your own operator group, see "Adding an operator group" (page 105).

WARNING:

When assigning an operator to the Administrator Group only, you are assigning that operator all IMC privileges to all services within IMC and to all devices groups and views. This does not apply when creating operators that belong to the Maintainer or Viewer group as rights to views and groups can be assigned in the individual operator account.

13. Enter a brief description for this operator in the Description field.

14. Select the Default Access Control Strategy you want to apply to this operator by clicking the appropriate radio button.

15. If you want to apply a login control template or rule to this operator, click Add.
16. If you have already created a login control template, click the radio button  to the left of Select from Existing Templates.

17. Select the login control template you wish to apply to this operator by clicking the radio button  to the left of the Login Control Name you want to select.

18. Click OK.

19. If you have not already created a login control template, click the radio button  to the left of Manually Add to add an access control rule.

   For more information on creating a login control template, see "Securing IMC through operator login control " (page 111).

20. Enter the following information in the Add Access Control Rule dialog box:
   a. Start IP: Enter the first IP address in address range you want to permit or deny access to in the field. If you are entering a single IP address, enter the same address in the Start IP and the End IP address fields.
   b. End IP: Enter the last IP address in address range you want to permit or deny access to in the field. If you are entering a single IP address, enter the same address in the Start IP and the End IP address fields.
   c. Action: Select the action you want to implement for this IP address or IP address range, Permit or Deny from the list.
   d. Description: Enter a description for this login control template in the field provided.

21. Click OK to complete the Login Control List configuration.

   If you enter more than one login control into the Login Control List for an operator, the web page updates to include a Change Priority field. This field allows you to define the order or priority for execution of login control list entries.

   Entries at the top of the list are treated with a higher priority than those below it.

22. To move a login control entry up or down in priority, do one of the following:
   o To move a login control entry up in priority, click the up arrow associated with that entry, or
   o To move it down, click the down arrow associated with that entry.

23. Click OK to accept the operator configuration.

   You cannot change the logging name once you create the operator account.

Modifying an administrator group operator

To modify an IMC administrator group operator:

1. Navigate to System → Operator:
   a. Click the System tab from the tabular navigation system on the top.
   b. Click Operator Management on the navigation tree on the left.
   c. Click Operator under Operator Management from the navigation system on the left.

   The Operator page is displayed and a list of all operators is displayed on this page.

2. Click the Modify icon in the Operator list associated with the operator you want to modify.

   You cannot change the login name once you create the operator account.

3. Modify the operator’s first and last name in the Full Name field.
4. Modify your selection for password authentication type from the Authentication Type list as needed. Options are IMC local Password, RADIUS, or LDAP.

You must configure the IMC Authentication Service module for LDAP and RADIUS before operators can authenticate using either one of these forms of authentication.

5. If you are using IMC’s local password feature, modify the operator’s password in the Password field as needed.

6. If you are using IMC’s local password feature, re-enter the operator’s password in the Confirm Password field.

7. Modify the Idle Timeout (Minutes) option as needed.

8. Select Same as System Settings if you want to apply system wide settings to this operator account.

9. Select Configure Individually.

The page updates to include a field to the right of the Idle Timeout list. Enter the idle timeout in minutes in this field.

10. Modify the description for this operator in the Description field as needed.

11. Select the Default Access Control Strategy you want to apply to this operator by clicking the appropriate radio button.

12. If you want to apply a login control template or rule to this operator, click Add.

13. If you have already created a login control template, click the radio button to the left of Select from Existing Templates.

14. Select the login control template you wish to apply to this operator by clicking the radio button to the left of the Login Control Name you want to select.

15. Click OK.

16. If you have not already created a login control template, click the radio button to the left of Manually Add to add an access control rule.

For more information on creating a login control template, see “Securing IMC through operator login control templates” (page 111).

17. Enter the following information in the Add Access Control Rule page:

- **Start IP**: Enter the first IP address in address range you want to permit or deny access to in the field. If you are entering a single IP address, enter the same address in the Start IP and the End IP address fields.

- **End IP**: Enter the last IP address in address range you want to permit or deny access to in the field. If you are entering a single IP address, enter the same address in the Start IP and the End IP address fields.

- **Action**: Select the action you want to implement for this IP address or IP address range, Permit or Deny from the list.

- **Description**: Enter a description for this login control template in the field provided.

18. Click OK to complete the Login Control List configuration.

If you enter more than one login control into the Login Control List for an operator, the web page updates to include a Change Priority field. This field allows you to define the order or priority for execution of login control list entries. Entries at the top of the list will be treated with a higher priority than those below it.

19. To change the priority of a login control entry, do one of the following:

- To move a login control entry up in priority, click the up arrow associated with that entry, or
To move it down, click the down arrow associated with that entry.

20. Click OK to accept your changes to the operator configuration.

Adding an IMC maintainer or viewer group operator

You can limit access to network resources managed by operators within IMC by assigning maintainer and viewer roles to operators. Some of the features that you can limit access to with these roles are custom views, location views and AP groups.

To limit operator access to custom and location views, the views must be created prior to the creation of the operator account.

Alternatively, you can create the operator accounts first and then return to complete the operator configuration after devices have been discovered, custom and location views created, and devices added to these views.

To add a maintainer or viewer group operator:

1. Navigate to System → Operator:
   a. Click the System tab from the tabular navigation system on the top.
   b. Click Operator Management on the navigation tree on the left.
   c. Click Operator under Operator Management from the navigation system on the left.
      The Operator page is displayed and a list of all operators is displayed on this page.

2. Click Add.
   The Add Operator page appears.

3. Enter a valid login name in the Login Name field.
   Login name can include alphanumeric characters, underscores (_), and hyphens (-).

4. Enter the operator’s first and last name in the Full Name field.

5. Select the password authentication type from the Authentication Type list.
   Options are IMC local Password, RADIUS, or LDAP. You must configure the IMC Authentication Server module for LDAP and RADIUS before operators can authenticate using these methods of authentication.

6. If you have elected to use IMC’s local password feature by selecting Password from the Authentication Type list, enter the operator’s password in the Password field.

7. If you have elected to use IMC’s local password feature by selecting Password from the Authentication Type, re-enter the operator’s password in the Confirm Password field.
   The Idle Timeout option allows you to configure for how long IMC sessions remain open and active while not in use.

8. Select Same as System Settings if you want to apply system wide settings to this operator account.

9. Select Configure Individually if you want to configure the Idle Timeout for this operator. Enter the idle timeout in minutes for this operator in the field located to the right of the Idle Timeout list.

10. Select the Maintainer or Viewer Group from the Operator Group list.
    The Operator Group list displays all currently configured operator groups.

11. Select from the pre-defined IMC operator groups or configure your own.
    To create and configure your own operator group, see "Managing operator groups" (page 104) or to configure this operator as a member of the Administrator Group, see "Adding an administrator group operator" (page 116).
A **Maintainer** has access to all operations except those reserved exclusively for administrators. Maintainers also have access to maintainer specific resources and certain system level information and resources.

A **Viewer** also has access to specific resources but has read-only access to system level information and resources.

12. Enter a brief description for this operator in the **Description** field.

13. You can configure the device groups and user groups to which operators have access. If you want the operator to have the ability to manage all device and user groups, click the **Manage All Groups** radio button and skip to Step 18.

14. If you want the operator to manage only a subset of device and user groups that you choose, click the **Define Manageable Groups** radio button.

15. The page updates to display the list of **Managed Device Groups** and **Managed User Groups**.

16. Click the checkboxes next to the **Managed Device Groups** for which you want to grant the operator access and control.

17. Click the **Expand All** icon to view all **Managed User Groups**.

18. Click the checkboxes next to the **Managed User Groups** for which this operator has management access and control.

19. If you want the operator to have the ability to manage all Level 1 custom views, click the **Manage All Level 1 Custom Views** radio button and skip to Step 23.

20. If you want the operator to manage only a subset of Level 1 Custom Views that you choose, click the **Define Manageable Level 1 Custom Views** radio button.

21. The page updates to display the list of **Manageable Level 1 Custom Views**.

22. Click the checkboxes next to the **Manageable Level 1 Custom Views** to which you want to grant this operator access and control.

23. Select the **Default Access Control Strategy** you want to apply to this operator by clicking the appropriate radio button, **Permit** to permit access to IMC or **Deny** to deny access to IMC.

24. Click **Add** if you want to use a **Login Control Template** to manage the operator’s access to IMC.

   a. If you have already created a login control template, click the radio button to the left of **Select from Existing Templates**.

   b. Select the login control template you want to apply to this operator by clicking the radio button to the left of **Login Control Name**.

25. Click **OK**. Skip now to Step 24.

   a. If you have not already created a login control template, click the radio button to Manually Add manually create an access control rule.

26. Enter the following information in the **Add Access Control Rule** page:

   a. Enter the first IP address in address range you want to permit or deny access to in the **Start IP** field. If you are entering a single IP address, enter the same address in the **Start IP** and the **End IP** address fields.

   b. Enter the last IP address in address range you want to permit or deny access to in the **End IP** field. If you are entering a single IP address, enter the same address in the **Start IP** and the **End IP** address fields.
c. Select the action you want to implement for this IP address or IP address range, Permit or Deny from the Action list.

d. Enter a description for this login control template in the Description field provided.

e. Click OK to complete the access control rule configuration.

25. Click the checkbox to the right of Only NE Management could be used in the Network Element User section if you want to restrict operator access to network element management only.

26. If you want the operator to have the ability to manage all manageable Fit AP groups, click the Manage all Fit AP groups radio button and skip to Step 27.

   a. If you want to select which fit AP groups the operator has access to and control over, click the Specify manageable Fit AP groups radio button.

   b. Click the checkboxes to the left of Manageable Fit AP Groups for which this operator has management access and control.

27. If you want the operator to have the ability to manage all Level 1 location views and therefore the devices in these views, click the Manage all Level 1 Location Views radio button.

   a. If you want to select which Level 1 location views and the devices in them the operator has access to and control over, click the Specify manageable Level 1 Location Views radio button.

   b. Click the checkboxes to the left of Manageable Level 1 Location Views for which this operator has management access and control.

28. Click OK to accept the operator configuration.

You cannot change the login name once you create the operator account.

Modifying a maintainer or viewer group operator

To modify a maintainer or viewer group operator:

1. Navigate to System → Operator:

   a. Click the System tab from the tabular navigation system on the top.

   b. Click Operator Management on the navigation tree on the left.

   c. Click Operator under Operator Management from the navigation system on the left.

   The Operator page displays and a list of all operators displays on this page.

2. Click the Modify icon in the Operator list associated with the operator you want to modify. You cannot modify the name of an operator once you have created it.

3. Modify the operator’s first and last name in the Full Name field as needed.

4. Modify the password authentication type by selecting the new setting from the Authentication Type list. Options are IMC local Password, RADIUS, or LDAP. You must configure the IMC Authentication Service module for LDAP and RADIUS before operators can authenticate using these methods of authentication.

5. If you have elected to use IMC’s local password feature by selecting Password from the Authentication Type list, modify the operator’s password in the Password field.

6. If you have elected to use IMC’s local password feature by selecting Password from the Authentication Type, re-enter the operator’s new password in the Confirm Password field.
7. Modify the **Idle Timeout** setting as needed.
8. Select **Same as System Settings** if you want to apply system wide settings to this operator account.
9. Select **Configure Individually** if you want to configure the **Idle Timeout** for this operator.
10. Enter the idle timeout in minutes for this operator in the field located to the right of the **Idle Timeout** list.
11. Modify the operator group as needed, selecting either **Maintainer Group** or **Viewer Group**.
    The **Operator Group** list displays all currently configured operator groups.
12. Select from the pre-defined IMC operator groups or configure your own.
    To create and configure your own operator group, see "Managing operator groups" (page 104). To configure this operator as a member of the Administrator Group, see "Adding an administrator group operator" (page 116).
    A **Maintainer** has access to all operations except those reserved exclusively for administrators. Maintainers also have access to maintainer specific resources and certain system level information and resources.
    A **Viewer** also has access to specific resources but has read-only access to system level information and resources.
13. Modify the description for this operator as needed in the **Description** field.
14. Modify which device groups and user groups operators have access to in the **Managed Groups** section.
15. If you want the operator to have the ability to manage all device and user groups, click the **Manage All Groups** radio button and skip to Step 11.
16. If you want the operator to manage only a subset of device and user groups that you choose, click the **Define Manageable Groups** radio button.
    The page updates to display the list of **Managed Device Groups** and **Managed User Groups**.
17. Do one of the following:
    - Click the checkboxes next to the **Managed Device Groups** for which you want to grant operator access and control, or
    - Click the checked boxes next to the **Managed Device Groups** for which you want to revoke operator access and control, or
    - Click the **Expand All** icon to view all **Managed User Groups**, or
    - Click the checkboxes next to the **Managed User Groups** for which the operator has management access and control, or
    - Click the checked boxes next to the **Managed User Groups** for which you want to revoke operator access and control.
18. If you want the operator to have the ability to manage all Level 1 custom views, click the **Manage All Level 1 Custom Views** radio button and skip to Step 21.
19. If you want the operator to manage only a subset of Level 1 Custom Views that you choose, click the **Define Manageable Level 1 Custom Views** radio button.
    The page will update to display the list of **Manageable Level 1 Custom Views**.
20. Click the checkboxes next to the **Manageable Level 1 Custom Views** to which you want to grant this operator access and control.
21. Modify the Default Access Control Strategy setting as needed by clicking on the appropriate radio button, Permit to permit access to IMC or Deny to deny access to IMC.

22. Click Add if you want to use a Login Control Template to manage the operator’s access to IMC.

23. If you have already created a login control template, click the radio button to the left of Select from Existing Templates.

24. Select the login control template you want to apply to this operator by clicking on the radio button to the left of Login Control Name.

25. Click OK. Skip now to Step 28.

26. If you have not already created a login control template, click the radio button to Manually Add manually create an access control rule.

27. Enter the following information in the Add Access Control Rule page:
   a. Enter the first IP address in address range you want to permit or deny access to in the Start IP field. If you are entering a single IP address, enter the same address in the Start IP and the End IP address fields.
   b. Enter the last IP address in address range you want to permit or deny access to in the End IP field. If you are entering a single IP address, enter the same address in the Start IP and the End IP address fields.
   c. Select the action you want to implement for this IP address or IP address range, Permit or Deny from the Action list.
   d. Enter a description for this login control template in the Description field provided.
   e. Click OK to complete the access control rule configuration.

28. Click the checkbox to the left of Only NE Management could be used in the Network Element User section if you want to restrict operator access to network element management only.

29. If you want the operator to have the ability to manage all manageable Fit AP groups, click the Manage all Fit AP groups radio button.

30. If you want to select which fit AP groups the operator has access to and control over, click the Specify manageable Fit AP groups radio button.

31. Click the checkboxes to the left of Manageable all Fit AP groups for which this operator has management access and control.

32. Click the checked boxes next to the Manageable Fit AP Groups for which you want to revoke operator access and control.

33. If you want the operator to have the ability to manage all Level 1 location views and therefore the devices in these views, click the Manage all Level 1 Location Views radio button and skip to Step 36.

34. If you want to select which Level 1 location views and the devices in them the operator has access to and control over, click the Specify manageable Level 1 Location Views radio button.

35. Do one of the following:
   o Click the checkboxes to the left of Manageable Level 1 Location Views for which this operator has management access and control, or
   o Click the checked boxes next to the Manageable Level 1 Location Views for which you want to revoke operator access and control.

36. Click OK to accept the operator configuration.
Deleting an IMC operator

To delete an IMC operator:

1. Navigate to System→Operator:
   a. Click the System tab from the tabular navigation system on the top.
   b. Click Operator Management on the navigation tree on the left.
   c. Click Operator under Operator Management from the navigation system on the left. The Operator page is displayed with a list of all operators.

2. Click the Delete icon in the Operator list associated with the operator you want to delete.
3. Click OK to confirm deletion of the operator.

You cannot delete operators that are currently online nor can you ever delete the administrator account.

Modifying IMC passwords

Individual IMC operators manage their own passwords once the operator account has been established.

To change your password:

1. Navigate to System→Modify Password:
   a. Click the System tab from the tabular navigation system on the top.
   b. Click Operator Management on the navigation tree on the left.
   c. Click Modify Password under Operator Management from the navigation system on the left. The Modify Password page appears.

2. Enter the old password for the account that you are currently logged in as in the Old Password field.
3. Enter the new password for the account that you are currently logged in as in the New Password field.
4. Re-enter the new password for the account you are currently logged in as in the Confirm New Password field.
5. Click OK.

Managing online IMC operator access

IMC offers you the ability to view which IMC operators are online, to log online operators off and also to block operator access for specific IP addresses when necessary.

Viewing online operators

To view which operators are currently online:

1. Navigate to System→Online Operators:
   a. Click the System tab from the tabular navigation system on the top.
   b. Click Operator Management on the navigation tree on the left.
   c. Click Online Operators under Operator Management from the navigation system on the left. The Online Operators page displays with the list of online operators.

Online operator list
o **Login Name**: Contains the IMC user ID or name of the operator.

o **Session ID**: Contains the session ID number for the associated online operator.

o **Login Time**: Contains the date and time stamp for the beginning of the operator’s session.

o **Login IP**: Contains the IP address of the associated operator.

If the Operator list contains enough entries, the following navigational aids appear:

- Click ➜ to page forward in the Online Operator list.
- Click ➞ to page forward to the end of the Online Operator list.
- Click ◀ to page backward in the Online Operator list.
- Click ◄ to page backward to the front of the Online Operator list.

2. Click 8, 15, 50, 100, or 200 from the right side of the main pane to configure how many items per page you want to view.

Only administrators or operators who are members of a group with the ADMIN privilege level can manage online operators.

**Logging off online operators**

To log an online operator off:

1. Navigate to System→Online Operators:
   a. Click the System tab from the tabular navigation system on the top.
   b. Click Operator Management on the navigation tree on the left.
   c. Click Online Operators under Operator Management from the navigation system on the left.
      The Online Operators page is displayed with the list of online operators.

2. Click the checkbox □ next to the operator’s login name that you want to log off.

3. Click Log Off.

Only administrators or operators who are members of a group with the ADMIN privilege level can log online operators off. Logging an operator off takes effect immediately.

**Blocking online operators**

Denying online operator access by blocking IP addresses creates a login control template for the operator that is blocked. This login control template becomes part of the operator’s permanent configuration and once blocked, the operator no longer has access to IMC unless the login control template is removed from the operator account.

To deny current and future operator access to IMC by blocking an IP address or address range for an operator:

1. Navigate to System→Online Operators:
   a. Click the System tab from the tabular navigation system on the top.
   b. Click Operator Management on the navigation tree on the left.
   c. Click Online Operators under Operator Management from the navigation system on the left.
      The Online Operators page is displayed with the list of online operators.

2. Click the checkbox □ next to the operator’s login name that you want to block.

3. Click Block IP.
Only administrators or operators who are members of a group with the ADMIN privilege level can block IP addresses.

Removing blocking from an operator account

To remove blocking by IP address:

1. Navigate to System → Operator:
   a. Click the System tab from the tabular navigation system on the top.
   b. Click Operator Management on the navigation tree on the left.
   c. Click Operator under Operator Management from the navigation system on the left.
      The Operator page displays with a list of all operators.

2. Click the Modify icon  in the Operator list associated with the operator you want to remove IP address blocking for.

3. Locate the Login Control List section of the operator configuration.

4. Locate the login control entry with the starting and ending IP address that you want to unblock.

5. Click the Delete icon next to the login control list entry that you want to delete.

6. Click OK to complete the changes to the operator configuration.

Group Management: managing resources using groups in IMC

Group Management enables you to more simply and effectively organize and secure access and management rights over network resources managed by IMC. It also enables you to grant or restrict access to and management of network resources more easily by assigning operators rights by device, user, or service groups.

A device can belong to one or more device groups. Note also that more than one operator can manage one or more groups.

Device groups

Device groups allow you to organize network devices by logical groups that you define. Groups can consist of devices of the same type, in the same location, or devices to be managed by the same operator or team within the organization.

Device groups are one of the three features that IMC offers you for granting or restricting access to network resources managed by IMC. Create custom device groups and then add devices to the groups. Then assign operators rights to the device groups. This gives operators access and rights to manage only the devices in the groups to which they have been granted management access.

Viewing device groups

To view the list of all device groups in IMC:

1. Navigate to System → Device Group:
   a. Click the System tab from the tabular navigation system on the top.
   b. Click Group Management on the navigation tree on the left.
c. Click 📚 **Device Group** under **Group Management** from the navigation system on the left.

IMC displays all device groups in the **Device Group List** displayed in the main pane of the **System → Device Group** window.

**Device group**

- **Group Name**: Contains name for this device group. The Group name is an active link that navigates you to the **Device Group Details** page. The **Device Group Details** page contains information about the selected group including which operators have been granted privileges to the selected group. It also includes a list of all devices that are part of the selected group.
- **Description**: Contains a description of this device group.
- **Device List**: Contains a link for the list of devices in the selected group.
- **Modify**: Contains a link for modifying the selected device group.
- **Delete**: Contains an icon for deleting the selected group.

If the **Device Group List** contains enough entries, the following navigational aids appear.

- Click ← to page forward in the **Device Group List**.
- Click ‹† to page forward to the end of the **Device Group List**.
- Click ‹ to page backward in the **Device Group List**.
- Click ‹ to page backward to the front of the **Device Group List**.

2. Click 8, 15, 50, 100, or 200 from the right side of the main pane to configure how many items per page you want to view.

To view all devices in IMC click the 🔄 **All Devices** link located in the far right corner of the **Device Group List** window.

To view all devices in IMC that are not in a device group, click the 🔄 **Ungrouped Devices** link.

**Viewing the device list**

Device lists provide operators with a list of all devices in a device group.

To view the device list for a particular device group:

1. Navigate to **System → Device Group → Group Name → Device List**:
   a. Click the **System** tab from the tabular navigation system on the top.
   b. Click **Group Management** on the navigation tree on the left.
   c. Click 📚 **Device Group** under **Group Management** from the navigation system on the left.

2. Click the **Device List** icon 🔄 for the **Device Group** you want to view devices for.

The page updates to display the **Device List** for the associated device group.

**Device list**

- **Status**: Contains the current alarm status of the device.
- **Device Label**: Contains the IMC name for this device. By default, the device name is the sysName or the configured name on the device.
- **Device Category**: Contains the device category as categorized by IMC.
- **Device Model**: Contains the device model.
- **IP Address**: Contains the IP address of the device.
If the Device List contains enough entries, the following navigational aids appear.

- Click ‣ to page forward in the Device List.
- Click ‣ to page forward to the end of the Device List.
- Click ‣ to page backward in the Device List.
- Click ‣ to page backward to the front of the Device List.

3. Click 8, 15, 50, 100, or 200 from the right side of the main pane to configure how many items per page you want to view.

Adding a device group

To add a device group:

1. Navigate to System→Device Group:
   a. Click the System tab from the tabular navigation system on the top.
   b. Click Group Management on the navigation tree on the left.
   c. Click Device Group under Group Management from the navigation system on the left.

IMC displays all device groups in the Device Group List displayed in the main pane of the System→Device Group window.

2. Click Add.

3. Enter the name for this device group in the Group Name field.

4. Select an option from the Automatically Add New Devices list.
   The options include None, All, and From Network Segment.
   If you select None, newly added devices are not automatically added to the device group; if you select All, newly added devices are automatically added to the device group; if you select From Network Segment, newly added devices whose IP address fall into the specified address range are automatically added to the device group.
   If you select From Network Segment, go to Step 5; if you select None or All, go to Step 8.

5. Enter the first IP address of the IP address range in the Start IP field.

6. Enter the last IP address of the IP address range in the End IP field.

7. Click Add to add the IP address range to the Network Segment list.

8. Select an IP address range on the Network Segment list, and click Delete to delete the IP address range.

9. Enter a description for this device group in the Description field.

10. To grant rights to this device group, click the checkbox next to the operator’s login name in the Operator list.

11. Click OK.
   Only administrators or operators who are members of a group with the ADMIN privilege level can configure a device group.

Modifying a device group

To modify a device group:

1. Navigate to System→Device Group:
   a. Click the System tab from the tabular navigation system on the top.
b. Click Group Management on the navigation tree on the left.
c. Click 💻 Device Group under Group Management from the navigation system on the left.
   IMC displays all device groups in the Device Group List displayed in the main pane of the System →Device Group window.

2. Click the Modify icon 📝 in the Device Group List associated with the device group you want to modify.

   The Modify Device Group page appears. You cannot modify the name of a device group once you create it.

3. Modify the description for this device group in the Description field.

4. Do one of the following:
   o To grant rights to this device group, click the checkbox ☑️ next to the operator’s login name in the Operator list, or
   o To revoke rights, click the checked box ☑️ next to the operator’s name in the Operator list.

5. Click OK.

Deleting a device group

To delete a device group:

1. Navigate to System→Device Group:
   a. Click the System tab from the tabular navigation system on the top.
   b. Click Group Management on the navigation tree on the left.
   c. Click 💻 Device Group under Group Management from the navigation system on the left.
      IMC displays all device groups in the Device Group List displayed in the main pane of the System →Device Group window.

2. Click the Delete icon 🗑️ in the Device Group list associated with the device group you want to delete.

3. Click OK to confirm deletion of the selected device group.

Once you have created device groups, the next step is to add devices to them.

Adding devices to a device group

To add devices to a device group:

1. Navigate to System→Device Group:
   a. Click the System tab from the tabular navigation system on the top.
   b. Click Group Management on the navigation tree on the left.
   c. Click 💻 Device Group under Group Management from the navigation system on the left.
      IMC displays all device groups in the Device Group List displayed in the main pane of the System →Device Group window.

2. Click the Device List icon 📊 displayed in the Device List column associated with the device group you want to add devices to.

   The Device List page appears.

3. Click Add.
4. Select the devices you want to add to the device group. You can add devices by using either the View or Advanced query option. See "Adding devices by View" (page 85) and "Adding devices by Advanced query" (page 85).

**Removing a device from a device group**

To remove devices from a device group:

1. Navigate to System→Device Group.
   a. Click the System tab from the tabular navigation system on the top.
   b. Click Group Management on the navigation tree on the left.
   c. Click Device Group under Group Management from the navigation system on the left.
      IMC displays all device groups in the Device Group List displayed in the main pane of the System→Device Group window.

2. Click the Device List icon for the device group you want to remove devices from.
   The Device List page appears.

3. Click the Remove icon associated with the device you want to remove from the group.
4. Click OK to confirm deletion of the selected device.

**Removing multiple devices from a device group**

To remove multiple devices from a device group:

1. Navigate to System→Device Group:
   a. Click the System tab from the tabular navigation system on the top.
   b. Click Group Management on the navigation tree on the left.
   c. Click Device Group under Group Management from the navigation system on the left.
      IMC displays all device groups in the Device Group List displayed in the main pane of the System→Device Group window.

   The Device Group List appears.

2. Click the Device List icon for the device group you want to remove devices from.
   The Device List page appears.

3. Click the checkbox to the left of the device names in the Device List for the devices you want to remove.
4. Click Remove.
5. Click OK to confirm deletion of the selected devices.

**Viewing the ungrouped devices list**

Devices that have not been added to a group will be displayed in the Ungrouped Devices list. From this list, operators can add devices to groups, manage or unmanage devices, or delete them from IMC.

To view the ungrouped devices list:

1. Navigate to System→Device Group→Ungrouped Devices:
   a. Click the System tab from the tabular navigation system on the top.
   b. Click Group Management on the navigation tree on the left.
   c. Click Device Group under Group Management on the left navigation tree.
The Device Group List appears. This list displays all device groups.

2. Click the Ungrouped Devices link located in the far right corner of the Device Group List.

The Ungrouped Devices List appears. This list displays all devices that have not been added to a group.

Ungrouped devices list

- **Status**: Contains the current alarm status of the device.
- **Device Label**: Contains the IMC name for this device. By default, the device name is the sysName or the configured name on the device.
- **Device Category**: Contains the device category as categorized by IMC.
- **Device Model**: Contains the device model.
- **IP Address**: Contains the IP address of the device.

If the ungrouped devices list contains enough entries, the following navigational aids appear.

- Click to page forward in the Ungrouped Devices List.
- Click to page forward to the end of the Ungrouped Devices List.
- Click to page backward in the Ungrouped Devices List.
- Click to page backward to the front of the Ungrouped Devices List.

3. Click 8, 15, 50, 100, or 200 from the right side of the main pane to configure how many items per page you want to view.

Adding devices to groups in ungrouped devices

To add devices to groups the ungrouped devices list:

1. Navigate to System→Device Group→Ungrouped Devices:
   a. Click the System tab from the tabular navigation system on the top.
   b. Click Group Management on the navigation tree on the left.
   c. Click Device Group under Group Management on the left navigation tree.
   d. The Device Group List appears.
      This list displays all device groups.

2. Click the Ungrouped Devices link located in the far right corner of the Device Group List.

The Ungrouped Devices List appears. This list displays all devices that have not been added to a group.

3. Click the checkbox to the left of the devices you want to add to a device group.

The Join Group page is displayed along with all device groups in the Target Device Groups section of the Join Group page.

4. Click the checkbox to the left of the groups you want to add the devices to.

5. Click OK.

The page updates with the results of the join group task.
User groups

Network infrastructure users are considered resources on the network in much the same way as devices and services are. Users require effective management to ensure that they have access to the network infrastructure resources they need when they need them. Conversely, network administrators need to ensure the integrity and security of the network infrastructure by ensuring that only valid users have access to network devices and services.

Users groups within IMC simplify the administrator’s task by allowing the administrator to group users in ways that meet the administrator’s and the organizations needs.

Administrators can group users by access requirements, by location, by logical organization grouping, or more. And, administrators can create nested groups with multiple subgroups in much the same way that directory and file structures are organized. Nested groups automatically inherit the permissions of the parent group. Note however that a user can belong to one group only.

The best approach for managing user groups in IMC is to plan for and create user groups prior to adding users to IMC.

Viewing the user group list

To add a user group:

1. Navigate to System→User Group:
   a. Click the System tab from the tabular navigation system on the top.
   b. Click Group Management on the navigation tree on the left.
   c. Click User Group under Group Management from the navigation system on the left.
      IMC displays the top-level user groups in the User Group List displayed in the main pane of the System →User Group window.

User group list

- **Group Name**: Contains the name of the user group.
- **Description**: Contains a description for the associated user group.
- **User List**: Contains an icon for accessing the User List for the associated user group.
- **Subgroups**: Contains an icon for accessing the subgroups under this group.
- **Modify**: Contains a link for modifying the selected user group.
- **Delete**: Contains an icon for deleting the selected user group.

If the user group list contains enough entries, the following navigational aids appear:

- Click to page forward in the User Group List.
- Click to page forward to the end of the User Group List.
- Click to page backward in the User Group List.
- Click to page backward to the front of the User Group List.

2. Click 8, 15, 50, 100, or 200 from the right side of the main pane to configure how many items per page you want to view.

Adding a user group

To add a user group:

1. Navigate to System→User Group:
a. Click the **System** tab from the tabular navigation system on the top.
b. Click **Group Management** on the navigation tree on the left.
c. Click 🌐 **User Group** under **Group Management** from the navigation system on the left.

IMC displays the top-level user groups in the **User Group List** displayed in the main pane of the **System—User Group** window.

2. Click **Add**.
3. Enter the name for this user group in the **Group Name** field.
4. Enter a description for this user group in the **Description** field.
5. Click the checkbox next to the operators to be granted rights to this user group from the **Operators** list.
6. Click **OK**.

Only administrators or operators who are members of a group with the **ADMIN** privilege level can add, modify, or delete a user group.

### Adding a user subgroup

You can create nested subgroups under groups in much the same way that directory and file structures are organized. Note however that a user can belong to one group only.

1. Navigate to **System—User Group**:
   a. Click the **System** tab from the tabular navigation system on the top.
   b. Click **Group Management** on the navigation tree on the left.
   c. Click 🌐 **User Group** under **Group Management** from the navigation system on the left.

IMC displays the top-level user groups in the **User Group List** displayed in the main pane of the **System—User Group** window.

2. From the **User Group List**, click the **Subgroups** icon associated with the parent user group.
3. Drill down into the various levels of subgroups until you reach the subgroup that contains the subgroup you want to add a subgroup to.
4. Click **Add**.
5. Enter the name for this user group in the **Group Name** field.
6. Enter a description for this user group in the **Description** field.
7. Click the checkbox next to the operators to be granted rights to this user group from the **Operators** list.

You cannot revoke rights for operators that have been granted access to subfolders by rights they have inherited from the parent folder.

Only administrators or operators who are members of a group with the **ADMIN** privilege level can add, modify, or delete user groups and subgroups.

8. Click **OK**.

### Modifying a user group

To modify a user group:

1. Navigate to **System—User Group**:
a. Click the System tab from the tabular navigation system on the top.
b. Click Group Management on the navigation tree on the left.
c. Click 🆘 User Group under Group Management from the navigation system on the left.

IMC displays the top-level user groups in the User Group List displayed in the main pane of the System→User Group window.

2. Click the Modify icon 📋 in the User Group List associated with the user group you want to modify.
   You cannot modify the name of a user group once the group has been created.
3. Modify the description for this user group in the Description field as needed.
4. Click the checkbox ☑️ next to the operators to be granted rights to this user group from the Operators list.
5. To revoke operator rights, click the checked box ☑️ next to the operator’s login name from the Operators list.
6. Click OK.

Modifying a user subgroup

To modify a user subgroup:

1. Navigate to System→User Group:
   a. Click the System tab from the tabular navigation system on the top.
   b. Click Group Management on the navigation tree on the left.
   c. Click 🆘 User Group under Group Management from the navigation system on the left.

IMC displays the top-level user groups in the User Group List displayed in the main pane of the System→User Group window.

2. From the User Group List, click the Subgroups icon 📃 associated with the parent user group.
3. Drill down into the various levels of subgroups until you reach the subgroup that contains the subgroup you want to modify.
4. Click the Modify icon 📋 in the User Group List associated with the subgroup you want to modify.
   You cannot modify the name of a user group once the group has been created.
5. Modify the description for this user group in the Description field as needed.
6. Click the checkbox ☑️ next to the operators to be granted rights to this user group from the Operators list.
7. To revoke operator rights, click the checked box ☑️ next to the operator’s name from the Operators list.
8. Click OK.

Deleting a user group

To delete a user group:

1. Navigate to System→User Group:
   a. Click the System tab from the tabular navigation system on the top.
   b. Click Group Management on the navigation tree on the left.
c. Click 📚 User Group under Group Management from the navigation system on the left. IMC displays the top-level user groups in the User Group List displayed in the main pane of the System → User Group window.

2. Click the Delete icon ☓ in the User Group List associated with the user group you want to delete.
3. Click OK to confirm deletion of the user group.

Deleting a user subgroup

To delete a user subgroup:

1. Navigate to System → User Group:
   a. Click the System tab from the tabular navigation system on the top.
   b. Click Group Management on the navigation tree on the left.
   c. Click 📚 User Group under Group Management from the navigation system on the left. IMC displays the top-level user groups in the User Group List displayed in the main pane of the System → User Group window.

2. From the User Group List, click the Subgroups icon 📚 associated with the parent user group.
3. Drill down into the various levels of subgroups until you reach the subgroup that contains the subgroup you want to delete.
4. Click the Delete icon ☓ in the User Group List associated with the user subgroup you want to delete.
5. Click OK to confirm deletion of the user subgroup.

Configuring IMC for alarm notifications

One of IMC’s powerful features is real time alarm or event management and notification. In this section, we will cover the system settings that require review or configuration in order to meet your alarm notification and management needs.

Mail server settings

IMC can send email notifications when problems arise in the network infrastructure, including when problems arise in IMC. Before support teams can receive email notifications of such events from IMC, you must first configure the mail server settings.

Configuring IMC for email notification

You must configure the SMTP mail server settings for mail sent by IMC to be forwarded.

To configure SMTP mail server settings:

1. Navigate to System → Mail Server Settings:
   a. Click the System tab from the tabular navigation system on the top.
   b. Click 📨 Mail Server Settings located in the lower right corner of the System Configuration section of the System page.
      
      The page updates to display the Mail Server Settings page.

2. Enter the IP address or hostname of the SMTP server to which IMC mail will be forwarded in the Server Address field.
3. Click the checkbox to the left of Requires Security Connection (SSL) if the SMTP server requires SSL authentication.

4. Click the checkbox to the left of Requires Authentication if the SMTP server requires authentication.

5. If you have selected requires authentication, then enter the information for username and password. If you have not selected requires authentication, then skip these fields.
   a. Enter the username of the sender’s mailbox in the Username field.
   b. Enter the sender’s password in the Password field.
   c. Enter the email address of the sender in the Sender’s Mail Address field.
   d. Click Test Mailbox to confirm that the configuration you have entered works properly.

6. Click OK.

The authentication selection you make in IMC for SMTP mail server settings must match the configuration of the receiving SMTP server.

Once you have configured the SMTP parameters, you are ready to begin configuring Mail Notification rules by using the Alarm Notification feature that can be found on the left navigation tree under Alarm Settings, which can be found under the Alarm tab. For more information on configuring alarm message notifications via email, see "Managing email alarm notifications" (page 587).

SMSC settings

IMC also supports SMSC (Short Message Service Center) messaging for proactively alerting network administrators and support teams when problems in the network infrastructure arise.

Configuring IMC for SMSC messaging

To configure SMSC settings:

1. Navigate to System→SMSC Settings:
   a. Click the System tab from the tabular navigation system on the top.
   b. Click SMSC Settings located in the System Configuration section of the System page.

The page is updated to display the SMSC Settings page.

2. Select the COM port from the list that will be used to send SMS messages from the Connect Using list.

3. Select the baud rate from the Baudrate (bps) list to match the modem configuration that will be used for SMS messaging.

4. Enter the country code in the Country Code field.

5. Enter the SMS phone number in the SMSC Number field. The contents of this field must be all digits.

6. Click OK.

Once you have configured the SMSC parameters, you are ready to begin configuring SMS Notification rules by using the Alarm Notification feature found on the left navigation tree under Alarm Settings, under the Alarm tab. For more information on configuring alarm message notifications via SMS, see "Managing SMS alarm notifications" (page 594).
Integrating IMC alarms into other management systems

IMC offers the ability to integrate alarms generated by IMC into other management systems. This is done by creating alarm rules for the events or conditions that you would like to forward to other management systems. It is better to create alarm forwarding rules should be done after IMC has been configured with views, groups, and after devices have been added to IMC.

For more information on creating rules for forwarding alarms from IMC to other management systems, see "Managing alarm forwarding: Integrating with other management systems" (page 599).

IMC hierarchical alarm configuration

One architecture option that IMC offers is a hierarchical configuration where IMC servers are configured in parent/child relationships. Part of this configuration includes configuring child IMC instances to forward alarms of importance to parent IMC instances.

Configuring IMC for hierarchical alarm configuration

To configure IMC hierarchical alarm settings:

1. Navigate to Alarm→Hierarchical IMC Alarm Settings:
   a. Click the Alarm tab from the tabular navigation system on the top.
   b. Click Alarm Settings from the navigation tree on the left.
   c. Click Hierarchical IMC Alarm Settings under Alarm Settings from the navigation tree on the left.
2. Click the checkbox to the right of Enable Alarming field to enable alarming.
3. Enter the IP address of the IMC instance to which alarms will be forwarded in the Upper-Level IP field.
   It is better to add a lower-level IMC to an upper-level IMC configuration than to add an upper-level IMC to a lower-level IMC.
4. Enter the TCP port number for the IMC service running on the IMC instance to which alarms will be forwarded in the Upper-Level RxPort field.
5. Enter the IP address of the IMC instance forwarding alarms in the Lower-Level IP field.
6. Select All Devices or Selected Devices from the Interested Devices list.
   o All Devices: With this option, alarms for all devices are forwarded to the Upper Level IMC instance, or
   o Selected Devices: With this option, alarms for only the selected devices are forwarded to the upper-level IMC instance.
     – If you choose Selected Devices, you can select devices to forward alarms for. You can specify which devices by specific device IP address, or devices grouped by views.
   o Device IP: Enter the IP address for the device you want to forward alarms for.
     – You can add multiple devices by clicking Add after entering the IP address in the Device IP field for every device you want to add.
     – You can also add devices by using views or IMC’s Advanced query option. To do so, click Select.

⚠️ WARNING:
   The Upper-Level IP address cannot be the IP address of the current IMC or any of its lower-level IMCs.
The Select Devices dialog box appears.

7. Add devices by using either the View or Advanced query option. See "Adding devices by View" (page 85) and "Adding devices by Advanced query" (page 85).

8. Select the configuration setting for this rule from the Interested Alarms list to select all conditions that trigger alarms or only a specified subset of conditions that trigger alarms.
   - All Alarms: With this option, all alarms configured in IMC triggers an email notification to be sent if the alarm condition is triggered, or
   - Selected Alarms: With this option, only the alarms you select in alarm notification triggers an email notification if the alarm condition is triggered.
     - If you choose Selected Alarms, you can select which alarms generate email alarm notifications. You can specify which conditions triggers email alarm notifications.

   a. Click Select to configure which conditions to alarm on.
   b. In the Select Alarm dialog box, locate the MIB that contains an object or condition that you want to alarm on.
   c. To expand your view of the MIB, click the arrow key next to the MIB that contains an object or condition that you want to alarm on.
   d. Click the checkbox to select a MIB object that you want to add to this alarm rule.
   e. Click the checked box to remove a MIB object from the alarm rule.
   f. Scroll down to the bottom of the MIB list and click OK.
     - It may take a while for the Select Alarm dialog box to close. When it does, it updates the Concerned Alarms field with the configured object or alarm condition.
     - You can click multiple checkboxes to select multiple objects or conditions forward alarms for. Each alarm condition is listed in the Interested Alarms field below the list.

   ! WARNING:
   When you select multiple MIB objects or alarm conditions, the alarm conditions are evaluated and performed as an AND operation. In other words, all of the conditions that you selected must be true for the alarm notification rule to generate an email notification.
     - Confirm that the MIB objects or conditions you have either added or removed have populated the Interested Alarms field in the Hierarchical IMC Alarm Settings page.

9. Click OK.

Only administrators or operators who are members of a group with the ADMIN privilege level can configure hierarchical alarm settings.

**MIB management**

Adding MIBs to IMC supports custom alarming and performance monitoring. To support this and other SNMP administrative tasks, IMC includes an integrated SNMP MIB browser.

**Adding a compiled MIB to IMC**

For MIBs to be usable by IMC, they must first be compiled. IMC provides hundreds of standard and custom or enterprise MIBS pre-compiled and pre-loaded into IMC.
To add a compiled MIB to IMC:

1. Navigate to **System**:
   
a. Click the **System** tab from the tabular navigation system on the top.

   b. Click the **MIB Management** icon located under the **Resource Management** section of the **System** page.
      
      The dialog box for the SNMP MIB browser appears.

2. Click the **Load MIB Files** icon located in the navigation bar at the top of the MIB browser window.
   
   This displays the **Load MIB Files** dialog box.

3. From the **Compiled MIB File List**, click the arrow to expand the list of MIBs that are compiled but not currently loaded into IMC from the **Unloaded MIB Group** navigation tree located in the bottom half of the **Load MIB Files** dialog box.
   
   This displays the compiled unloaded MIB groups.

4. Click the arrow of the **Unloaded MIB Group** that contains the compiled MIB you want to add.

5. Highlight the MIBs from the **Unloaded MIB Group** in the **Compiled MIB file list** that you want to load.

6. Do one of the following:
   
   o Click the **** button to load them, or
   
   o Click the **** button to load all of the displayed MIBs.

   The total number of files in the MIB tree cannot exceed 40.

7. Click **Close**.

### Compiling a MIB in IMC

To compile a MIB in IMC:

1. Navigate to **System**:
   
a. Click the **System** tab from the tabular navigation system on the top.

   b. Click the **MIB Management** icon located under the **Resource Management** section of the **System** page.
      
      The dialog box for the SNMP MIB browser appears.

2. Click the **Load MIB Files** icon located in the navigation bar at the top of the MIB browser window.
   
   This displays the **Load MIB Files** dialog box.

3. Click the **Compile MIB Files** icon .

4. Click **Browser** to select the MIB you want to compile.

5. Locate the MIB file or the compressed MIB file you want to compile and click **Open** from the **File Upload** dialog box.
   
   IMC can automatically compile all MIB files from the compressed file.
6. Select the directory you want to store the compiled MIB in from the list of directories displayed in the Compile MIB Files dialog box.

7. Click Compile.

8. Review the results of the compiling process in the Compile Results dialog box.

9. Specifically, check the Total # of MIB files compiled and the In all # compilations succeeded entries.

If the compilation was not successful, fix the problems in the MIB file indicated by the Compile Results output and repeat the steps listed above until the MIB compiles successfully.

Once you have successfully compiled the MIB you can load it into IMC following the steps provided in the previous section, "Adding a compiled MIB to IMC. If the MIB does not compile, please contact the MIB vendor for technical support. To expedite the issue, document the error message returned by the compile process.

Removing a compiled MIB from IMC

To remove a compiled MIB from IMC:

1. Navigate to System:
   a. Click the System tab from the tabular navigation system on the top.
   b. Click the MIB Management icon located under the Resource Management section of the System page
      The web interface for the SNMP MIB browser appears.

2. Click the Load MIB Files icon located in the navigation bar at the top of the MIB browser window.
   This displays the Load MIB Files dialog box.

3. From the Compiled MIB file list, click the arrow to expand the list of MIBs that are currently loaded into IMC from the Loaded MIB Group navigation tree.
   This displays the compiled loaded MIB groups.

4. Click the arrow of the Loaded MIB Group that contains the compiled MIB you want to unload.

5. Highlight the MIBs from the Loaded MIB Group in the Loaded MIB file list that you want to unload.
   o Click the button to load the file you have highlighted, or
   o Click the button to unload all of the displayed MIBs.

6. Click Close.

⚠️ WARNING:
If you unload all MIBs, you need to manually reload them. The MIBs loaded by default at installation are located in the Default folder of the Compile MIB Files dialog box.
Configuration center options

File transfer mode options

Operators can configure the default transfer mode used in IMC’s configuration and change management tasks. Operators can choose FTP, TFTP, or SFTP as the default transfer method for all devices managed by IMC.

Operators can also configure individual devices for a specific transfer mode using the Options features in the Configuration Center.

To access and configure the transfer mode options for configuration and change management features in IMC:

1. Navigate to Service→Options:
   a. Click the Configuration Center icon located under the Resource and Configuration Management section of the Service page.
   b. Click Options under Configuration Center on the left navigation tree.
   c. On the Options page that appears, click the File Transfer Mode tab.

2. Click the radio button to the left of the transfer mode you want to configure as the default in the Default Transfer Mode section of the File Transfer Mode tab.

Options include:

- **TFTP**: This option can be used for devices whose maximum file size limit is no more than 32 MB.
- **FTP**: This option does not limit the maximum file size limit.

To use FTP, you must enable the FTP service on the managed device and configure the user name and password for logging in to the FTP server.

The user name and password configured in IMC must match what is configured on the FTP server for the managed device.

In addition, you must also set server\tmp under the IMC installation directory as the root directory of the FTP service.

Set the FTP server to be accessed with its IP address and the loopback address 127.0.0.1.

- **SFTP**: This option can be used for operators who prefer to use a secure transmission method. To transfer files using SFTP, you must enable the SFTP server on the managed device and configure the SSH parameters for the device in IMC.

To enable FTP transfer mode:

1. Click the checkbox to the left of Enable FTP Transfer Mode.
2. In the FTP User Name field, enter the user name for the FTP account configured on the managed devices that uses the Default Transfer Mode setting.
3. In the FTP Password field, enter the password for the FTP account configured on the managed devices that uses the Default Transfer Mode setting.

All devices that use the default transfer mode settings must have the same user name and passwords as configured in Step 2 and Step 3.
IMC provides you with the ability to configure exceptions to the Default Transfer Mode configuration. Using the Single Device Transfer Mode option, you can configure one or more devices to use a different transfer mode configuration than the default. To use this feature, follow the steps below.

4. Otherwise, click OK to complete your configuration of the Default Transfer Mode option for all devices in IMC.

5. Click Select Device to configure the selected devices with specific transfer mode configurations.

6. You can add devices by using either the View or Advanced query option. See "Adding devices by View" (page 85) and "Adding devices by Advanced query" (page 85).

To set or cancel the transfer mode option for one or more devices:

1. Click the checkbox to the left of each device.
2. Click Set Mode.
   The Select Transfer Mode dialog box appears.
3. Select the transfer mode you want to use for each of the selected devices from the Transfer Mode list.
4. Click OK.
   All devices that are not configured using the single device transfer mode adopt the default transfer mode.

To remove the single device transfer mode option from one or more devices:

1. Click the checkbox to the left of the device in the device list, and then click Cancel Mode.
2. Click OK to accept your default and device specific transfer mode options.

Backup policy options

Operators can configure the backup policy options for individual devices managed by IMC. Options include Alarm Generation Mode and Max. Backup Configuration Files.

Setting the alarm generation mode

This option enables IMC to generate alarms or disables IMC from generating any alarm for individual devices when their configurations to be backed up are different from the baseline configurations or last configuration backups. To access and configure the Alarm Generation Mode option for individual devices in IMC:

1. Navigate to Service→Options:
   a. Click the Configuration Center icon located under the Resource and Configuration Management section of the Service page.
   b. Click Options under Configuration Center on the left navigation tree.
      The Options page appears.
2. Click the Backup Policy tab.
3. Click the radio button to the left of Alarm Generation Mode in the Set Type section.
4. Do one of the following:
   o If you do not want to configure one or more devices, skip to Step 6, or
   o If you want to configure one or more devices to use the Generate alarms if the configuration to be backed up is different from the baseline backup policy, follow the steps below.
a. If you click the radio button ☐ to the left of **All devices except the selected ones will generate alarms** in the **Generate alarms if the configuration to be backed up is different from the baseline section**, IMC generates alarms for all devices that are not listed when their configurations to be backed up are different from the baseline configurations.

b. If you click the radio button ☐ to the left of **Only the selected devices will generate alarms** in the **Generate alarms if the configuration to be backed up is different from the baseline section**, IMC generates alarms for all listed devices when their configurations to be backed up are different from the baseline configurations.

c. Click **Select Device** to select devices for the backup policy.

5. Add devices by using either the **View** or **Advanced** query option. See "Adding devices by View" (page 85) and "Adding devices by Advanced query" (page 85).

To cancel the backup policy option for one or more devices:

6. Click the **Delete** icon ✗ to the right of each device.

   All the devices that are not configured separately with the special setting adopt the global backup policy.

7. Do one of the following:
   - If you do not want to configure one or more devices, skip to Step 9, or
   - If you want to configure one or more devices to use the **Generate alarms if the configuration to be backed up is different from the last backup** policy, follow the steps below.

   a. If you click the radio button ☐ to the left of **All devices except the selected ones will generate alarms** in the **Generate alarms if the configuration to be backed up is different from the last backup section**, IMC generates alarms for all devices that are not listed when their configurations to be backed up are different from the last configuration backups.

   b. If you click the radio button ☐ to the left of **Only the selected devices will generate alarms** in the **Generate alarms if the configuration to be backed up is different from the last backup section**, IMC generates alarms for all listed devices when their configurations to be backed up are different from the last configuration backups.

   c. Click **Select Device** to select devices for the backup policy.

8. Add devices by using either the **View** or **Advanced** query option. See "Adding devices by View" (page 85) and "Adding devices by Advanced query" (page 85).

To cancel the backup policy option for one or more devices:

9. Click the **Delete** icon ✗ to the right of each device.

10. Click **OK** to accept your default and device specific backup policy options.

**Setting the max backup configuration files**

This option specifies the maximum number of backed up configuration files that IMC retains. For example, if you specify 5, IMC retains five running configuration files and five startup configuration files. The settings take effect at the next backup of the device.

To access and configure the **Max Backup Configuration Files** option in IMC:

1. Navigate to **Service**→**Options**:

   a. Click the 🛠 **Configuration Center** icon located under the **Resource and Configuration Management** section of the **Service** page.

   b. Click 🛠 **Options** under **Configuration Center** on the left navigation tree.
The Options page is displayed, click the **Backup Policy** tab.

2. Click the radio button ☑ to the left of **Max. Backup Configuration Files** in the **Set Type** section.

3. Enter a value in the field to the right of **Max. Backup Configuration Files**.
   The value can be 0, or an integer ranging from 5 to 100. The value 0 indicates that the number of backed up configuration files is not limited.

4. Click **OK**.

**IMC system settings and maintenance functions**

To maintain the health and functioning of IMC, you may consider tasks that include configuring system settings, exporting data to maintain the health and performance of IMC, understanding how operation log files work, and customizing the IMC interface to meet your needs.

**System settings**

You can configure basic system settings to adjust basic IMC functioning and security.

**Modifying system settings**

To modify system settings:

1. Navigate to **System → System Settings**:
   a. Click the **System** tab from the tabular navigation system on the top.
   b. Click **System Settings** located in the **System Configuration** section of the **System** page.
      The page is updated to display the **SMSC Settings** page.

2. Modify the configuration information displayed on the **System Settings** page.

**Basic system settings**

- **Operator Idle Timeout**: This parameter allows the administrator to configure the default system-wide setting for how long IMC waits before logging out an operator account that is no longer active. The range is 1–9999999 minutes. The default setting is 30 minutes.
  - Enter the value in minutes for operator idle timeout.
  - Click **OK**.
- **Concurrent Logins with Same Operator Account**: This parameter allows the administrator to configure globally whether or not operators are allowed to have multiple, concurrent active sessions. The options are **Allow** and **Prohibit**. The default is **Allow**.
  - Select **Allow** to permit multiple concurrent active sessions from the list.
  - Select **Prohibit** to deny multiple, concurrent active sessions.
  - Click **OK**.
- **Device Info Display**: This parameter allows you to configure how device information is displayed: by IP address, by Device Label or both.
  - Select **Device Label (IP)** if you want IMC to display both device label and IP address from the list.
  - Select **Device Label Only** if you want IMC to display only the device label.
  - Select **IP Only** if you want IMC to display the IP address only.
  - Click **OK**.
• **Interface Info Display**: This parameter allows you to configure how interface information is displayed: by **Interface Description**, by **Interface Alias**.
  
  o Select **Interface Description** if you want IMC to display interface description.
  
  o Select **Interface Alias** if you want IMC to display the interface alias.

• **Lifetime of Deleted Users**: This parameter allows you to configure how long deleted users are retained before they are permanently removed from the system. The range is 1–360 days. The default setting is 60 days.
  
  1. Enter the value in days to retain deleted users before permanently removing them from IMC.
  
  o **Display Access Passwords**: This parameter allows you to display or hide passwords (for example, Telnet/SSH password), SNMP community strings, or SOAP parameters.

  2. Select **Plain Text** if you want the passwords to be displayed in clear or plain text.
  
  3. Select **Ciphertext** if you want the passwords to be hidden from view.
  
  4. Click **OK**.

**Web manager configuration**

• **Protocol**: This parameter allows you to configure which communication protocol IMC uses for Web access: HTTP or HTTPS. Changes to **Web Manager** configurations apply to devices added to IMC after these configuration changes have been made. In addition, any **Web Manager** settings configured on the device itself override this setting.

  1. Select **HTTP** or **HTTPS** from the **Protocol** list.

  o **Port**: This parameter allows you to configure which port IMC uses for HTTPs communications. The default port for HTTP is 80.

  2. Enter the port number in the **Port** field.

  3. Click **OK**.

**Ping Configuration**

• **Retry** (1–20): This parameter allows you to configure how many times, IMC sends a ping packet to the managed device after issuing a timeout. The default value is 3.

• **Timeout** (1–60 seconds): This parameter allows you to configure how long, in seconds, IMC waits to receive a ping response from the ping request from the managed device before issuing a timeout. After the final failed ping request, IMC sets the device in an alarm state. The default value is 2.

  1. Click **OK**.

**NNMi Configuration**

• **Server IP Address**: This parameter allows you to configure the server IP address of NNMi for communications with IMC.

• **Server Port**: This parameter allows you to configure which port NNMi uses for communications with IMC.

• **User Name**: This parameter allows you to configure the username of NNMi for communications with IMC.

• **Password**: This parameter allows you to configure the password of NNMi for communications with IMC.

• **Start a scheduled task to import devices from NNMi**: This parameter allows you to select whether to start a scheduled task to import devices from NNMi.
If a task is scheduled to import devices from NNMi, IMC obtains and imports device information from the NNMi server at the specified time.

1. To schedule the task, open file `client\conf\platAppContext.xml` in the installation path, search the `platNNMiDeviceImportTrigger` field, change the `cronExpression` attribute of the field, and restart IMC.

   The attribute supports the following parameters: second, minute, hour, date of a month, month of a year, and day of a week. An asterisk (*) means "all." A question mark (?) means "not set." By default, the task is executed at 01:10 every day, which corresponds to the `cronExpression` value `0 10 1 * * ?`.

2. Click OK.

Device registration configuration

- **Email**—Enters the Email address of the HP `my.procurve.com` website, so that you can register the device with HP by Email and get technical support from HP.
- **Password**—Enters login password of the Email box.

1. Click OK.

Internet connection configuration

- **Connection Type**: This parameter allows you to configure how IMC connects to the Internet.
  1. Select **Direct Connect**, **HTTP Proxy**, or **SOCKS Proxy** from the list.
  2. Select **Direct Connect** if IMC’s connection to the Internet is direct rather than through an Internet proxy server.

   If you are using a proxy server, whether it is an HTTP or SOCKS proxy, to provide access to the Internet, you must enter the proxy server IP address and port number. If the proxy server requires authentication, you must input the user name and password. The default is **Direct Connect**.

3. Click OK.

Interface Up/Down alarm

- **Alarms for PC-connect links**: This parameter allows you to select whether to filter interface UP/Down alarms for the interfaces that connect to PCs.
- **Alarms for server-connected links**: This parameter allows you to select whether to filter interface UP/Down alarms for the interfaces that connect to servers or are located on servers.
- **Alarms for disconnected links**: This parameter allows you to select whether to filter interface UP/Down alarms for the interfaces that have no physical connections.

1. Click OK.

Device label configuration

- **Device Label Type**: This parameter allows you to select **DNS Name** or **Sysname** as the default label for the device.
- **Update Existing Device Labels**: This parameter allows you to select whether to update all device labels by using the setting in the "Internet connection configuration" section.
- **Update Device Label When Sysname Changes**: This parameter allows you to select whether to update device labels when the devices’ sysNames change. This parameter is available when you select **Sysname** for the device label use in the "Internet connection configuration" section.

1. Click OK.
DNS server setting

- **DNS Server List**: This parameter allows you to configure the DNS address. When inputting multiple DNS addresses, separate them with semicolons (;).

1. Click **OK**.

DismanPing configuration

- **Enable DismanPing**: This parameter allows you to enable or disable the DismanPing feature in IMC’s Network Topology. Enabling DismanPing can improve topology correctness. Not all devices support the DismanPing feature. For more information about DismanPing feature, see the device configuration manual.

External tool settings

- **SFTP Client**: This parameter provides the complete directory of the executable SFTP client program on the IMC server. It identifies the location of the SFTP client program. IMC uses the SFTP client program to log in to the device and get or put files to the device. If this parameter is null, the default client program (`{IMC installation directory}/server/bin/psftp.exe` for Windows and `{IMC installation directory}/server/bin/psftp` for Linux) is used.

- **SSH Client**: This parameter provides the complete directory of the executable SSH client program on the IMC server. It identifies the location of the SSH client program. IMC uses the SSH client program to log in to the device. If this parameter is null, the default client program (`{IMC installation directory}/server/bin/plink.exe` for Windows and `{IMC installation directory}/server/bin/plink` for Linux) is used.

1. Click **OK**.

Data export

IMC stores event information in log files. Events turn to alarms, when there is a match in the content of a log to a system or user defined alarm rule. IMC enables you to manage the size of its database by writing alarms in the database to export logs and then storing exported data for a specified period of time.

Once events are exported, they are removed from the event logs and from IMC processing. This feature enables you to manage the size and the performance of IMC’s database while also storing valuable data for post-export analysis, if needed.

In addition to using Data Export to manage the size and performance of the IMC database, data from the Data Export process can be used as an input to other non-IMC data analysis processes. For example, you can import data exported by the Data Export process into a spreadsheet.

The base platform of IMC offers you the ability to export data from the following IMC services or log files:

- SCC – Attack Alarm
- Operation Log
- Alarm Export
- Trap Export
- Guest Access Log
- Syslog, in addition, data can be exported either to HTML or CSV formats.

To export IMC event logs:

1. Navigate to **System**→**Data Export Settings**:
   a. Click the **System** tab from the tabular navigation system on the top.
b. Click **Data Export** located in the **System Configuration** section of the **System** page.

The page is updated to display the **Data Export Settings** page.

2. To select the IMC log file source, click the appropriate tab located at the top of the **Data Export Settings** window.

3. Configure the following **Data Export** parameters as needed.

**Export triggers**

To limit the export of the selected log file to a specific number of entries:

1. Click the checkbox  to the left of **By Quantity**.

2. Enter the number of entries you want to export in the **Threshold** field.

3. To export all events with the exception of the last x number of entries, enter the number of entries you want to exclude from export in the **Export but the last** field.

4. Click the checkbox  to the left of **By Time** if you want to limit the export of the selected log file to a specific number of days.

5. Enter the number of days you want to export in the **Threshold** field.

6. To export all events with the exception of the last x number of days, enter the number of days you want to exclude from export in the **Export but those in last** field.

   If you select the **By Quantity** and **By Time** check boxes (which is the default configuration), IMC automatically uses the export criteria that contain more entries to export the data.

---

⚠ **WARNING:**

Modify the system time with caution. Modifying IMC’s system time may trigger a data export that removes events from IMC and therefore may impair normal alarming of events.

---

**Export settings**

1. Select the export file format you want to export from the **Target File Type** list.

2. Enter the length of time you would like to save this file for in the **Save File for** field.

3. If you want IMC to execute a command upon successful completion of the export, enter the command in the **Execute Command After Export** field.

   The command to be executed must be a batch file that does not invoke any GUI commands.

   The path and file name for the exported file can be found in the **Target File Path** field.

4. Click the **Change Export Directory** link on the upper right corner.

   A popup dialog box appears.

5. Enter the new file path in the **Export Data to** Field.

   Make sure that the new file path already exists on the IMC master server.

6. Click **OK**.

   The new file path appears in the **Target File Path** field.

7. To view information on the last successful export, refer to the **Last Export** field.

8. To execute a data export immediately, click the **Export Immediately** link located to the far right of the **Data Export Settings** window.
Data export considerations

Data exports take effect only after the support IMC components have been installed and deployed. For example, the alarm export function takes effect only after the basic network management components are installed and deployed.

Alarm exporting removes the recovered and acknowledged alarms from IMC. It does not remove unacknowledged or unrecovered alarms.

Events can be exported only when its corresponding alarms have been exported.

An example of the process for exporting By Quantity:

- When the Threshold parameter is configured for 8000 entries and the Export but the last is configured for 500 entries, when the number of entries reaches 8000, all but the most current 500 entries events are exported.

An example of the process for exporting By Time:

- When the Threshold parameter is configured for 60 days and the Export but those in last is configured for 30, when the number of days reaches 60 days, events for all but the last 30 days are exported.

Data exports by default occur at 02:00:00 every morning. Make sure that the system server has adequate resources at 02:00:00 to process exports. To modify the export time, contact HP Technical Support.

- To begin data exporting immediately, click the Export Immediately link.

A command executed after the data export runs in the background service mode. Thus, you cannot open any window with this command, which automatically exits once it has finished.

Log files

IMC writes valuable system level and operator level information to log files. One such file is the operation log, which contains information about IMC operator activity.

Viewing the operation logs

To view operation logs:

1. Navigate to System→Operation Log:
   a. Click the System tab from the tabular navigation system on the top.
   b. Click Operation Log located in the System Configuration section of the System page.

      The Operation Log list is displayed in the main pane.

      o Operator: Contains the name of the operator executing the operation documented in the log entry.
      o IP Address: Contains the IP address of the operator executing the operation documented in the log entry.
      o Module Name: Contains the name of the IMC module that generated the log entry.
      o Operation Time: Contains the date and time stamp for the log entry.
      o Operation: Contains a description of the operation, action, results, or text for the log entry.
      o Result: Contains the result of the operation documented in the log entry.
      o Details: Contains a hyperlink to more details regarding he specific log entry.

2. Click the Details icon to view details for a single operation log entry.
If the operation log list contains enough entries, the following navigational aids are displayed:

- Click  to page forward in the Operation Log.
- Click  to page forward to the end of the Operation Log.
- Click  to page backward in the Operation Log.
- Click  to page backward to the front of the Operation Log.

3. Click 8, 15, 50, 100, or 200 from the right side of the main pane to configure how many items per page you want to view.

**Querying operation logs**

To filter the operation log list:

1. Navigate to System→Operation Log:
   a. Click the System tab from the tabular navigation system on the top.
   b. Click  Operation Log located in the System Configuration section of the System page. The Operation Log list is displayed in the main pane.

2. Move the pointer over Query at the upper right corner of Operation Log list, and a search criteria dialog box appears.

3. Enter the following parameters in the dialog box:
   - **Operator**: The name of the operator executing the operation documented in the log entry.
   - **IP Address**: The IP address of the operator executing the operation documented in the log entry.
   - **Module Name**: The name of the IMC module that generated the log entry.
   - **Result**: The result of the operation documented in the log entry.
   - **Started at**: A start date and time by which you want to filter the operation log list in the text box. You can enter the date and time manually or you can enter it by clicking the calendar located to the right of the field. A popup calendar appears. Select the start date from the calendar. Adjust the hour value as needed in the Started at field.
   - **Ended at**: An end date and time by which you want to filter the operation log list in the text box. You can enter the date and time manually or you can enter it by clicking the calendar located to the right of the field. A popup calendar appears. Select the end date from the calendar. Adjust the hour value as needed in the Ended at field.
   - **Operation**: Enter the description of the operation, action, results, or text for the log entry.

4. Click Query to submit your filter criteria.

The results are displayed in the main pane.

**Data analysis management**

Projects are the IMC processes that analyze and process data gathered by IMC. Using the Data Analysis Management feature, you can view the projects or processes that are queued for processing. You can also monitor and manage the status of all the projects that are active as well as any tasks running underneath them. IMC lists data analysis projects by their project ID.

**Managing the data analysis project list**

To manage the data analysis project list:
1. Navigate to System—Data Analysis:
   a. Click the System tab from the tabular navigation system on the top.
   b. Click Data Analysis Project located in the Data Analysis section of the System page.

The page is updated to display the Data Analysis page. IMC lists all current processes or projects, their project ID, the IP address of the server and the project status in the Project List.

The project status viewed may contain the following status values:
   - Waiting: The project is idle and the execution time has not been reached.
   - Executing: The project is in the process of executing.
   - Pausing: The project is in the process of pausing.
   - Paused: The project has been paused.
   - Exception: An unrecoverable error occurred while the project was running. The project needs to be re-initiated manually.

2. To pause, click the checked box next to the project ID you want to pause.

The checked box moves to the resume column until the project has been resumed.

You can also view individual tasks under projects by clicking on the Project ID. This displays the Task List.

The Task List displays the task type, last execution time, last execution results and next execution time.

3. Click Back to return to the Project List.

Deleting a project cannot be undone. However, deleted project can be added manually.

My Favorites

IMC offers you the ability to customize IMC by storing frequently used IMC pages as favorites. For more information on this feature, see "Personalizing the IMC web interface" (page 66).

Configuring default monitor indices

IMC is configured to automatically poll all managed devices for specific system and performance metrics. You can customize this list of metrics or indices by adding or removing indices from the list.

To configure the default monitor indices:

1. Navigate to System—Default Monitoring Indices:
   a. Click the System tab from the tabular navigation system on the top.
   b. Click Default Monitor Indices located in the System Configuration section of the System page.

The page is updated to display the Default Monitoring Indices page.

2. Click the checkbox next to the monitor index you want to add to the Default Monitor Indices list in the Select Index page.

3. Click the checked box next to the monitor index you want to remove from the Default Monitor Indices list in the Select Index page.

4. Click OK.
Configuring network asset audit options

IMC enables you to add devices to network asset management when devices are added to IMC. In addition, IMC enables you to configure how frequently automatic asset audit synchronization occurs.

To configure the network asset audit settings:

1. Navigate to Resource→Network Assets:
   a. Click the Resource tab from the tabular navigation system on the top.
   b. Click Network Assets section of the navigation tree on the left.
   c. Click Options under Network Assets from the navigation system on the left.
   The Options page appears.

2. If you want to add all devices to the Network Asset Manager for asset auditing when you add devices to IMC, click the radio button ☑️ to the left of Yes in the Add devices to network asset when adding it to IMC platform.

3. Click OK to accept the configuration change.

4. To configure number of days between the automatic synchronization or polling for audit details:

5. Enter the number in days in the Auto Synchronization Interval field. The default is 1.

6. Click OK to accept the configuration change.
5 Resource management

The **Resource** tab provides you with a portal for the device monitoring and management features of IMC. From this portal, you can view and manage network resources including devices and IP addresses.

IMC offers you a variety of options for viewing and managing devices through views that organize by device type (**Device View**), IP address (**IP View**), topology (**Network Topology**) or the operator’s own organization of devices using **Custom Views**. Each of these views offers the ability to manage multiple devices from the device lists on these pages. In addition, each view offers drill down capabilities to the **Device Details** page, which includes a multitude of monitoring and management features for the selected device.

From the **Device Details** page, you can synchronize, refresh, manage or unmanage, or delete a device. From this view, devices can be accessed remotely via Telnet, SSH, the Device Panel, or Web Manager. You can also ping or traceroute to a device from the **Device Details** page that is accessed from all views.

In addition, you can configure devices. Configuration options include modifying a device label, system group attributes, SSH and Telnet settings, polling intervals, ping and Web Manager parameters. You can add or cancel performance monitoring for a selected device.

From IMC, you can also manage devices including resetting or rebooting a device remotely, saving device configuration, or system information. You can configure address binding, view hardware, OSPF, and IPv6 information and view and configure Power over Ethernet configuration on switches.

In addition, you can view protocol information for routers and switches, view and modify VLAN, RMON, and Spanning tree information on switches and IGMP Snooping configuration on wireless devices.

You can also view and manage interfaces on devices from IMC. Interface management options include managing and unmanaging interfaces, synchronizing, configuring management status and speed, loopback testing and adding ports to and removing ports from VLANs.

IMC also offers you the ability to manage multiple devices from views and in batch mode. From views, you can add, remove, delete, manage, unmanage, synchronize, and refresh devices. You can configure SNMP, SSH, and Telnet settings as well as check these settings on multiple devices. You can also configure polling intervals, save configurations, reboot devices, backup configurations, and deploy software for multiple devices.

Using batch mode, you can configure SNMP, Telnet, and SSH settings, polling intervals and modify login types. You can also check settings in batch mode for SNMP, Telnet, and SSH. You can save device configurations, reboot devices, check and configure management status on interfaces, implement PoE, configure trap destinations, Spanning Tree on switches and interfaces and configure LACP on switches.

You can also track the usage of and allocate IP addresses in IMC, bind IP addresses to MAC address, and bind MAC addresses to interfaces. You can search IMC in real time and historically for locations of IP addresses to pinpoint the location of a user/device. You can track network assets, and perform and configure asset auditing.
Adding devices in IMC

The most basic network resource management task is to add a device. IMC offers you several methods for adding devices in IMC. You can add devices manually. One or more devices can be added through auto discovery. Finally, devices can be added by importing the device data directly into IMC.

When you add a device, either manually, by import, or through auto discovery, IMC by default sets their status as managed. Managed devices consume node licenses in IMC and a warning dialog box appears. For a current license count, click the About link in the upper right corner of IMC.

Adding devices manually to IMC

You can add devices manually, one at a time. IMC automatically manages a device once a device has been added to IMC, whether it has been manually or automatically added.

Adding a device manually

To add a device manually:

1. Navigate to Resources → Add Device:
   a. Click the Resource tab from the tabular navigation system on the top.
   b. Click Resource Management on the navigation tree on the left.
   c. Click Add Device under Resource Management from the navigation system on the left.

2. Enter the node name or IP address of the network device you want to add in the Host Name/IP address field. This field is required.

3. Enter the name that is displayed on the IMC platform in the Device Label field.

4. Enter a valid IP subnet mask for the device to be added in the Mask field.

5. Select the device group to which you want to add this device from the Device Group list.
   If you do not want to add the device to a device group, leave this option blank.
   All devices that have not been added to a device group are displayed in the Ungrouped Devices List. You can add devices to groups from the Ungrouped Devices List after they have been added to IMC.
   You must create device groups before you can add devices to them. Once you have created the device groups, they appear in the Device Group list.

6. Select the access method for this device from the Login Type list.
   Options include Telnet, SSH, and None. The device to be added must be configured to support the access or login type selected here.

7. If you want IMC to process traps sent by this device for alarming and notification purposes, verify that the checkbox to the left of Automatically register to receive SNMP traps from supported devices is checked .
WARNING:
If the Automatically register to receive SNMP traps from supported devices checkbox is not checked, IMC does not process, display, or alarm on traps sent by this device.

8. Do one of the following:
   o If the device to be added responds to ping requests for monitoring reachability, verify that the checkbox to the left of Support Ping Operation is checked, or
   o If the device does not respond to ping requests, verify that the checkbox is unchecked.

9. If you want to add the device even if it does not respond to ping requests, click the checkbox to the left of Add the device regardless of the ping result.

10. If you want IMC to use the Loopback address for the management of the discovered device, check the box to the left of Use the loopback address as the management IP.

11. To view and configure SNMP settings for this device, click the SNMP Settings link.

12. To configure the SNMP settings for this device, click the Configure link located at the SNMP Settings section.

The SNMP Parameters dialog box appears.

You can either enter the SNMP settings in this dialog box or you can select an existing SNMP template that contains the SNMP settings for this device. SNMP templates are particularly useful when SNMP configurations are standardized. For more information on creating SNMP templates, see “SNMP templates” (page 74).

Editing SNMP settings manually

1. To edit the SNMP parameters, verify that the radio button to the left of Edit SNMP Parameters is selected.
   o Parameter Type: Select the version of SNMP (v1 or v2c) that is configured on the device to be added from the Parameter Type list. You can add devices that are configured with SNMPv3 using SNMP templates only. Therefore, you must create an SNMP template with the SNMPv3 parameters for this device before adding it.
   o Read-Only Community String: Enter the read-only community string for this device in the Read-Only Community String field. This value must match the read only community string that is configured on the device to be added.
   o Read-Write Community String: Enter the read-write community string for this device in the Read-Write Community String field. This value must match the read-write community string that is configured on the device to be added.
   o Timeout: Enter the SNMP timeout value (1–60 seconds) in the Timeout field. This parameter determines how long IMC waits for an SNMP reply from the managed device before declaring that the request has timed out. The default is 4.
   o Retries: Enter the number of SNMP retries (1–20) in the Retries field. The retries parameter defines how many times the management system (IMC) sends SNMP retries in an attempt to communicate with the managed device before reporting a failure. The default is 3.
Using existing SNMP template

To configure the SNMP settings for this device using an SNMP template:

2. Click the radio button ☑ to the left of **Select an Existing Template**.
3. Click the radio button ☑ to the left of the template you want to use.
4. Click **OK**.
5. Do one of the following:
   o To view and configure SNMP settings for this device, click the **SNMP Settings** link, or
   o To configure the SNMP settings for this device, click the **Configure** link located at the **Telnet Settings** section.
      The **SNMP Parameters** dialog box appears.
6. Do one of the following:
   o Enter the SNMP settings in this dialog box, or
   o Select an existing Telnet template that contains the SNMP settings for this device.

SNMP templates are particularly useful when SNMP configurations are standardized. For more information on creating SNMP templates, see “SSH templates” (page 80).

Editing Telnet parameters manually

1. To edit the Telnet parameters manually, verify that the radio button ☑ to the left of **Edit Telnet Parameters** is selected.
2. Do the following:
   a. **Authentication Mode**: Select the mode that matches the Telnet authentication mode configured on the managed devices from the **Authentication Mode** list.
   b. **Username**: Enter the username configured on managed devices in the **Username** field, if prompted.
   c. **Password**: Enter the password configured on the managed devices in the **Password** field, if prompted.
   d. **Super Password**: Enter the super password configured on the managed devices for the **Super Password**, if prompted.
   e. **Timeout**: Enter the Telnet timeout value configured on the managed device in the **Timeout** field.
      Valid range is 1–60 seconds.

Using an existing Telnet template

To configure the Telnet settings for this device using Telnet templates:

1. Click the radio button ☑ to the left of **Select an Existing Template**.
2. Click the radio button ☑ to the left of the Telnet template you want to use.
3. Click **OK**.
4. Do one of the following:
   o To view and configure Telnet settings for this device, click the **Telnet Settings** link.
To configure the Telnet settings for this device, click the **Configure** link located at the **Telnet Settings** section.

The **Telnet Parameters** dialog box appears.

5. Do one of the following:
   a. Enter the Telnet settings in this dialog box, or
   b. Select an existing Telnet template that contains the SSH settings for this device.

   Telnet templates are particularly useful when Telnet configurations are standardized. For more information on creating Telnet templates, see "Telnet templates" (page 77).

**Editing SSH settings manually**

1. To edit the SSH parameters, verify that the radio button to the left of **Edit SSH Parameters** is selected.
2. Do the following:
   a. **Authentication Mode**: Select the authentication mode that corresponds with the SSH configuration mode on the managed devices.
   
   The authentication mode selected must match the authentication mode configured on the device.
   b. **User Name**: Enter the username that is configured on the managed devices.
   c. **Password**: Enter the password that is configured on the managed devices, if prompted.
   d. **Private Key File**: Select the local path and filename of the private key file that contains the key that enables login, if prompted.
   e. **Private Key Password**: Enter the private key password for the private key file, if prompted.
   f. **Super Password**: Enter the super password that is configured on the managed devices, if prompted.
   g. **Port**: Enter the TCP port for SSH configured on managed devices. The default TCP port is 22.
   h. **Timeout**: Enter the SSH timeout value (1–120 seconds).
   
   The timeout parameter defines how long the system waits for the device to respond in seconds before declaring that the response has timed out. The default setting is 10 seconds.
   i. **Retries**: Enter the number of SSH retries (1–5).
   
   The retries parameter defines how many times the management system (IMC) sends SSH retries in an attempt to communicate with the managed device before reporting a failure. The default setting is 3.

**Using existing SSH templates**

To configure the SSH settings for this device using SSH templates:

1. Click the radio button to the left of **Select an Existing Template**.
2. Click the radio button to the left of the SSH template you want to use.
3. Click **OK** to accept the SSH configuration.
4. Click **OK** to add the device.

When you add a device, IMC automatically records your settings for the following parameters. When you add another device, IMC uses your settings as the default settings.
The parameters include:

- Login Type
- Automatically register to receive SNMP traps from supported devices
- Support Ping Operation
- Add the device regardless of the ping result
- Use the loopback address as the management IP

**WARNING:**

IMC automatically manages all devices that you add to IMC. Check your license count before adding devices to IMC to verify that you have enough licenses to manage all added devices.

### Auto discovering devices

Auto discovering in IMC allows you to search the network and add all found devices to IMC using two methods: basic and advanced. With the basic auto discovery method, you provide a start and end IP address that directs the discovery process. In addition, you provide SNMP and Telnet settings that support the addition of devices for these protocols. You have the option to run basic and advanced discoveries immediately or at a scheduled date and time.

With advanced auto discoveries, you can search the network using routing tables. With this option, you configure hop counts to determine how far IMC searches the infrastructure for new devices. In routing based discoveries, you also provide a Seed IP to direct the starting point for the auto discovery.

Another option for auto discovery of network devices is an ARP-based auto discovery. ARP-based auto discoveries search ARP tables to discover new devices. As with routing based discoveries, you also configure hop counts to determine how far IMC searches the infrastructure for new devices. In ARP-based discoveries, you also provide a Seed IP to direct the starting point for the auto discovery.

A third option is the IPsec VPN-based auto discovery method. With this option, IMC queries IPsec devices for new devices, again using hop counts to limit how far IMC searches the infrastructure. Seed IP addresses are also required for this method.

You can use the network segment-based advanced method for auto discovering new devices. With this method, you configure IMC with IP address segments, which IMC then searches for new devices. With this method, hop count and Seed IP addresses are not required.

### Adding devices through basic auto discovery

The device to be added must be configured to support the access or login type selected here. HP recommends configuring default monitor indices before performing an auto discovery. Monitor indices gather the metrics that IMC uses to measure performance of managed devices. Monitor indices are also used to generate alarms when they exceed configured thresholds. By configuring the default monitor indices first, IMC applies them to devices found in the discovery process. For more information, see "Configuring default monitor indices" (page 151).

To add devices to IMC using the basic auto discovery method:

1. Navigate to **Resources → Auto Discovery**:
   
   a. Click the **Resource** tab from the tabular navigation system on the top.
b. Click Resource Management on the navigation tree on the left.

2. Click 🔄 Auto Discovery under Resource Management from the navigation system on the left.

3. Confirm that you are in Basic mode.
   The main section of the page title should read Auto Discovery (Basic).

4. If the dialog box does not have this title and your breadcrumb trail is Resource → Auto Discovery (Advanced), then click 🔄 Go to Basic to navigate to the Auto Discovery (Basic) page. 🔄 Go to Basic can be found in the far right corner of the Auto Discovery page.

5. Enter the first IP address of the IP address range you want to search devices for in the Start IP field.

6. Enter the last IP address of the IP address range you want to search devices for in the End IP field.

7. Click Add to add the IP address range.

8. Configure the device group you want to add the discovered devices to by selecting it from the Device Group list.
   You must create the device groups before using them in the auto discovery process. For more information on creating device groups, see "Adding a device group" (page 128).

9. If you want to receive SNMP traps from the discovered devices that support SNMP trap generation, verify that the checkbox to the left of Automatically register to receive SNMP traps from supported devices is checked.

⚠️ WARNING:
If the Automatically register to receive SNMP traps from supported devices checkbox is not checked, IMC does not process, display, or alarm on traps sent by the discovered devices.

10. Enter the SNMP v1 read community string in the SNMP Read Community string field.

11. Enter the SNMP v1 write community string in the SNMP Write Community string field.
    The SNMP read and write community string configuration you enter here must match the SNMP configuration settings on the devices to be discovered and managed. Refer to each vendor’s manual for information on setting the SNMP configuration parameters for each device type.
    In the basic auto discovery mode, only SNMP v1 is supported.

12. Select the Telnet authentication mode that corresponds with the Telnet authentication mode configured on the managed devices from the Telnet Authentication Mode list.

13. Do the following:
    a. Telnet Username: Enter the username configured on managed devices in the Telnet Username field, if prompted.
    b. Telnet Password: Enter the password configured on the managed devices in the Telnet Password field, if prompted.
    c. Telnet Super Password: Enter the super password configured on the managed devices for the Telnet Super Password, if prompted.

14. If you want IMC to perform scheduled auto discoveries, select the frequency with which you want IMC to perform scheduled auto discoveries from the Schedule list.
Options include Never, Hour, Day, Week, and Month.

15. Select Never if you want IMC to perform the auto discovery immediately rather than on a scheduled basis.

IMC runs the auto discovery when you have completed the configuration and clicked on Auto Discovery.

16. If you choose to schedule an auto discovery for hour, you only need to enter the discover time.

17. If you choose to schedule an auto discovery for day, week, or month, enter the start date you want to begin the scheduled auto discovery in the Start Date field.

You can also use the calendar function to the right of the Start Date field to select and auto populate the field.

18. Select the hour and minute from the lists located to the right of the Discover Time field.

19. Click Save Only if you want IMC to save the auto discovery configuration and perform the auto discovery according to the schedule you have defined.

You can review summary results for all discoveries, including scheduled discoveries in the Discovery Report that is found under Resource Statistics Report.

For more information on accessing reports in IMC, see "My real time reports" (page 849).

20. Click Auto Discovery if you want to begin the auto discovery immediately.

21. If you clicked Auto Discovery, the Auto Discovery Running window is displayed along with details of the auto discovery process.

While the auto discovery is running, IMC displays a rotating icon.

22. Click Stop if you want to cancel the auto discovery process.

Once IMC has completed the auto discovery, IMC displays a status and summary of the auto discovery process at the top of the Auto Discovery Running window.

When completed, IMC displays a list of all discovered devices and the results in the Auto Discovery Running list.

23. Review the results of the discovery process.

You can also review the results of the auto discovery process by clicking the View Report link located below the Auto Discovery Running title bar, once the auto discovery process has completed.

The report is displayed in an Intelligent Analysis Report Viewer window.

Printing the report to PDF

To print the auto discovery report to PDF:

1. Click the print icon located on the toolbar on the top of the report.
2. Select the desired page range from Page Range.
3. Click Export.
Exporting the report

To export the auto discovery report:

1. Click the export icon located on the toolbar on the top of the report.
2. Select the desired export file format from the File Format list.
   Options include Crystal Reports (RPT), Adobe Acrobat (PDF), Microsoft Excel (97-2003),
   (RTF), and Comma Separated Values (CSV).
3. Click Export.

Advanced auto discovery: routing-based, ARP-based, or IPsec VPN-based, PPP-based

The following section describes the advanced method for auto discovering devices using four of the
five advanced discovery methods: routing-based, ARP-based, IPsec VPN-based or PPP-based. With
each of these methods, you configure hop counts to determine how far IMC searches the
infrastructure for new devices. In these discovery methods, you also provide one or more seed IP
addresses to direct the starting points for the auto discovery.

HP recommends configuring default monitor indices before performing an auto discovery. Monitor
indices gather the metrics that IMC uses to measure performance of managed devices. Monitor
indices are also used to generate alarms when they exceed configured thresholds. By configuring the
default monitor indices first, IMC applies them to devices found in the discovery process. For more
information, see “Configuring default monitor indices” (page 151).

1. Navigate to Resources→Auto Discovery:
   a. Click the Resource tab from the tabular navigation system on the top.
   b. Click Resource Management on the navigation tree on the left.
   c. Click Auto Discovery under Resource Management from the navigation system on the
      left.
2. Confirm that you are in Advanced mode.
   The dialog box title should read Select Auto Discovery Mode and the breadcrumb trail should
   read Resource → Auto Discovery (Advanced).
   If not, then click Go to Advanced located on the far right of the Auto Discovery page.
3. Select any one of the first three auto discovery options you want to use by clicking on the radio
   button to the left of the discovery mode.
   Options include:
   o Routing-Based: This option searches the routing tables of all reachable routers for
     manageable network devices.
   o ARP-Based: This option searches the Address Resolution Protocol or ARP tables for
     manageable network devices.
   o IPsec VPN-Based: This option searches IPsec VPN devices for manageable network
     devices.
   o Network Segment-Based: This option searches for manageable devices by the specified IP
     address range.
4. Click **Next**.
   - **PPP-Based**: This option searches the Peer-to-Peer Protocol for manageable network devices.
   - **Hop Count**: The **Hop Count** parameter defines the maximum number of network node hops IMC traverses in the discovery process.

⚠️ **WARNING:**

The larger the hop count, the more the discovery process consumes system and network resources, including bandwidth, and the longer the discovery process takes. Exercise the hop count configuration parameter with caution.

5. To configure the hop count, select the hop count number from the **Hop Count** list.
   - **Login Type**: This option defines how IMC logs into the discovered device. Options include **Telnet**, **SSH**, and **None**.
6. Select login type from the **Login Type** list.
   The discovered devices must be configured to support the login type you select.
7. **Loopback Address as Manager IP**: To select the Loopback address for the management of the discovered device, click the checkbox to the left of **Loopback Address as Manager IP**.
8. **Discover Non-SNMP Devices**: IMC can manage devices that do not support SNMP.
   - If you do not want IMC to manage these devices, click the checkbox to the left of **Discover Non-SNMP Devices**.

   The **Discover Non-SNMP Devices** option is not available for IPsec VPN-Based auto discovery.

   **Scan one by one in the Segment**: This option configures IMC to discover every device in the configured network segment. This option does not appear if you select the IPsec VPN-based or ARP-based auto discovery option. This is a very time consuming method for auto discovery, as IMC pings every IP address in the segment serially and adds only the devices that respond to the ping request.

9. To select the auto discovery option described above, click the checkbox to the left of **Scan one by one in the Segment**.
10. **Automatically register to receive SNMP traps from supported devices**: If you want IMC to receive and process traps from discovered devices, verify that the checkbox to the left of **Automatically register to receive SNMP traps from supported devices** is checked.

⚠️ **WARNING:**

If the **Automatically register to receive SNMP traps from supported devices** checkbox is not checked, IMC does not process, display, or alarm on traps sent by the discovered devices.

- **Seed IP**: A seed IP address in an auto discovery serves as a starting point for the discovery process.
11. Select, as the seed IP address, the device that enables IMC to discover as many devices to be managed as possible.

   Typically, routers and layer three switches are the most logical choice for routing and ARP based discoveries. For IPsec VPN-Based discoveries, options for the Seed IP include VPN gateways and routers supporting VPN.
12. Enter the IP address of the device to serve as a seed device for auto discovery purposes in the Seed IP field.

13. Click Add.
   You can add more than one IP address to serve as seed IP devices by clicking Add after entering the IP address in the Seed IP field.

14. Select the device group you want to add the discovered and managed devices to from the Device Group list.

You can choose not to add devices to any device group. If you choose this option, the discovered devices are not added to any group. You must create the device groups before using them in the auto discovery process. For more information on creating device groups, see "Adding a device group" (page 128).

15. To configure the SNMP settings, click the configure icon located to the right of SNMP Settings (Required).
   
   The SNMP Parameters dialog box appears.

16. Do one of the following:
   - Enter the SNMP settings in this dialog box, or
   - Use an SNMP template that contains the SNMP settings for this device.
   
   SNMP templates are particularly useful when SNMP configurations are standardized. For more information on creating SNMP templates, see "SNMP templates" (page 74).

   **Editing SNMP settings manually**

   1. To edit the SNMP parameters, verify that the radio button to the left of Edit SNMP Parameters is selected.

   2. Do the following:
      
      a. **Parameter Type:** Select the version of SNMP (v1 or v2c) that is configured on the device to be added from the Parameter Type list.
         
         You can only add devices that are configured with SNMPv3 using SNMP templates. Therefore, you must create an SNMP template with the SNMPv3 parameters for this device before adding this device. For more information, see "SNMP templates" (page 74).
      
      b. **Read-Only Community String:** Enter the read-only community string for this device in the Read-Only Community String field. This value must match the read only community string that is configured on the device to be added.
      
      c. **Read-Write Community String:** Enter the read-write community string for this device in the Read-Write Community String field. This value must match the read-write community string that is configured on the device to be added.
      
      d. **Timeout:** Enter the SNMP timeout value (1–60 seconds) in the Timeout field. This parameter determines how long IMC waits for an SNMP reply from the managed device before declaring that the request has timed out. The default is 4.
      
      e. **Retries:** Enter the number of SNMP retries (1–20) in the Retries field. The retries parameter defines how many times the management system (IMC) sends SNMP retries in an attempt to communicate with the managed device before reporting a failure. The default is 3.
Using existing SNMP template

To configure the SNMP settings for this device using an SNMP template:
1. Click the radio button to the left of Select an Existing Template.
2. Click the radio button to the left of the SNMP template you want to use.
3. Click OK.
4. To configure the Telnet settings, click the configure icon located at the Telnet Parameters section.
The Telnet Parameters dialog box appears.
5. Do one of the following:
   a. Enter the Telnet settings in this dialog box, or
   b. Create a Telnet template that contains the Telnet settings for this device.
   Telnet templates are particularly useful when Telnet configurations are standardized. For more information on creating Telnet templates, see "Telnet templates" (page 77).

Editing Telnet settings manually

1. To edit the Telnet parameters manually, verify that the radio button to the left of Edit Telnet Parameters is selected.
2. Do the following:
   a. **Authentication Mode**: Select the mode that corresponds with the Telnet authentication mode configured on the managed devices from the Authentication Mode list.
   b. **Username**: Enter the username configured on managed devices in the Username field, if prompted.
   c. **Password**: Enter the password configured on the managed devices in the Password field, if prompted.
   d. **Super Password**: Enter the super password configured on the managed devices for the Super Password, if prompted.
   e. **Timeout**: Enter the Telnet timeout value (1–60 seconds). The timeout parameter defines how long the system waits for the device to respond in seconds.

Using existing Telnet template

1. To configure the Telnet settings for this device using Telnet templates, click the radio button to the left of Select an Existing Template.
2. Click the radio button to the left of the Telnet template you want to use.
3. Click OK.
4. To configure the telnet settings, click the configure icon located to the right of Telnet Parameters.
The Telnet Parameters dialog box appears.
5. Do one of the following:
   a. Enter the Telnet settings in this dialog box, or
   b. Create a Telnet template that contains the SSH settings for this device.
Telnet templates are particularly useful when Telnet configurations are standardized. For more information on creating Telnet templates, see “SSH templates” (page 80).

**Editing SSH settings manually**

1. To edit the SSH parameters, verify that the radio button ☐ to the left of **Edit SSH Parameters** is selected.

2. Do the following:
   a. **Authentication Mode**: Select the authentication mode that corresponds with the SSH configuration mode on the managed devices from the list.
   b. **User Name**: Enter the username that is configured on managed devices.
   c. **Password**: If prompted, enter the password that is configured on the managed devices.
   d. A password is optional if the Private Key File option is selected.
   e. **Private Key File**: Select the path and filename of the private key file that contains the key that enables login, if prompted.
   f. **Private Key Password**: Enter the private key password for the private key file, if prompted.
   g. **Super Password**: Enter the super password that is configured on the managed devices.
   h. **Port**: Enter the TCP port for SSH configured on managed devices. The default TCP port is 22.
   i. **Timeout**: Enter the SSH timeout value (1–120 seconds). The timeout parameter defines how long the system waits for the device to respond in seconds before declaring that the response has timed out. The default setting is 10 seconds.
   j. **Retries**: Enter the number of SSH retries (1–5). The retries parameter defines how many times the management system (IMC) sends SSH retries in an attempt to communicate with the managed device before reporting a failure. The default setting is 3.

**Using existing SSH templates**

1. To configure the SSH settings for this device using SSH templates, click the radio button ☐ to the left of **Select an Existing Template**.

2. Click the radio button ☐ to the left of the SSH template you want to use.

3. Click **OK** to accept the SSH configuration.

   The filter settings offer you flexibility in determining which subnets and devices to either include in or exclude from the auto discovery process.

4. Enter the IP address subnet range and the subnet mask you want to filter by in the **Subnet IP** field.

5. Masks can be entered using either CIDR or dotted decimal notation.
   - For example, a valid network/subnet mask entry using CIDR notation would be `192.168.1.0/24`
   - where `/24` represents the number of bits allocated to the network portion of the address and implying that the remaining bits are allocated to the host portion.
   - Alternatively, a valid network/subnet mask using dotted decimal notation would be `192.168.1.0/255.255.255.0`

6. Do one of the following:
7. If you want IMC to perform scheduled auto discoveries, select the frequency with which you want IMC to perform scheduled auto discoveries from the Schedule list. Options include Never, Hour, Day, Week, and Month. Select Never if you want IMC to perform the auto discovery immediately rather than on a scheduled basis. IMC runs the auto discovery when you have completed the configuration and clicked Auto Discovery.

8. Do one of the following:
   - Choose to schedule an auto discovery for hour by entering the discover time.
   - Choose to schedule an auto discovery for a specific day, week, or month, enter the start date you want to begin the scheduled auto discovery in the Start Date field.
     You can also use the calendar function to the right of the Start Date field to select and auto populate the field.
     Select the hour and minutes from the lists located to the right of the Discover Time field.

9. Click Save Only if you want IMC to save the auto discovery configuration and perform the auto discovery according to the schedule you have defined.

10. Click Auto Discovery if you want to begin the auto discovery immediately.
    If you clicked Auto Discovery, the Auto Discovery Running window is displayed along with details of the auto discovery process.
    While the auto discovery is running, IMC displays a rotating icon.

11. Click Stop if you want to cancel the auto discovery process.
    Once IMC has completed the auto discovery, it displays a status and summary of the auto discovery process at the top of the Auto Discovery Running window as well as a list of all discovered devices and the results in the Auto Discovery Running list.

12. Review the results of the discovery process.
    You can also review the results of the auto discovery process by clicking the View Report link located below the Auto Discovery Running title bar.
    The report is displayed in an Intelligent Analysis Report Viewer window.

Printing the report to PDF
To print the report to PDF:
1. Click the print icon located on the toolbar on the top of the report.
2. Select the desired page range from Page Range.
3. Click Export.

Exporting the report
To export the report:
1. Click the export icon located on the toolbar on the top of the report.
2. Select the desired export file format from the File Format list.
   Options include Crystal Reports (RPT), Adobe Acrobat (PDF), Microsoft Excel (97-2003),
   (RTF), and Comma Separated Values (CSV).
3. Click Export.
   You can also review the results of the most recent auto discovery by clicking on the link Latest Result from the Resource → Auto Discovery page.

**Advanced Auto Discovery: network segment based discovery method**

You can also use the network segment based advanced method for auto discovering new devices. With this method, you configure IMC with one or more IP address segments, which IMC then searches for new devices. With this method, hop count and Seed IP addresses are not required. HP recommends configuring default monitor indices before performing an auto discovery. Monitor indices gather the metrics that IMC uses to measure performance of managed devices. Monitor indices are also used to generate alarms when they exceed configured thresholds. By configuring the default monitor indices first, IMC applies them to devices found in the discovery process. For more information, see "Configuring default monitor indices" (page 151).

To add devices to IMC using Advanced Auto Discovery method:

1. Navigate to Resources → Auto Discovery:
   a. Click the Resource tab from the tabular navigation system on the top.
   b. Click Resource Management on the navigation tree on the left.
   c. Click Auto Discovery under Resource Management from the navigation system on the left.
2. Confirm that you are in advanced mode.
   The dialog box title should be Select Auto Discovery Mode and the breadcrumb trail should be Resource → Auto Discovery (Advanced). If not, then click Go to Advanced located to the far right of the Auto Discovery page.
3. Select the auto discovery mode, Network Segment-Based discovery mode.
4. Click Next.
5. Enter the first IP address of the IP address range you want to search for new devices in this auto discovery in the Start IP field.
6. Enter the last IP address of the IP address range you want to search for new devices in this auto discovery in the End IP field.
7. Click Add to add the IP address range to the Configured Segment Address list.
   You can add more than one IP Segment to the list by repeating steps 3-4 for each segment you want to add.

**Importing network segment addresses**

You can also import the list of network segment addresses. To do so, the import file format must conform to the following rules:
- Import file must be a text file.
- Import file size must not exceed 5 MB.
- Start IP address and End IP address must be separated by ".".
- Every network segment address must be a newline.

The examples below are valid entries for an import file:

```
10.9.1.1-10.9.128.1
10.1.1.1-10.1.255.1
```

1. Once you have created the import file, click **Import** located to the right of the **Configured Segment Address** list.
2. Click **Browse** to locate your import file.
3. Click **OK** to accept the selected import file.
4. Confirm that the entries in your import file have been added to the **Configured Segment Address** list.
   
   **Login Type**: This option defines how IMC logs into the discovered device.
   
   Options include **Telnet**, **SSH**, and **None**. Select login type from the **Login Type** list. The discovered devices must be configured to support the login type you select.

5. **Use the loopback address as the management IP**: If you want IMC to use the Loopback address for the management of the discovered device, click the checkbox to the left of **Loopback Address as Manager IP**.

6. **Discover Non-SNMP Devices**: IMC can manage devices that do not support SNMP. If you want IMC to manage these devices, click the checkbox to the left of **Discover Non-SNMP Devices**.

7. **Scan one by one in the Segment**: This option configures IMC to discover every device in the configured network segment. However, this is a very time consuming option for auto discovery as IMC pings every IP address in the segment serially and then add the devices that respond to the ping request. If you want this auto discovery option, click the checkbox to the left of **Scan one by one in the Segment**.

8. **Automatically register to receive SNMP traps from supported devices**: If you want IMC to receive and process traps from discovered devices, verify that the checkbox to the left of **Automatically register to receive SNMP traps from supported devices** is checked.

   **WARNING:**
   
   If the **Automatically register to receive SNMP traps from supported devices** checkbox is not checked, IMC does not process, display, or alarm on traps sent by the discovered devices.

9. Select the device group you want to add the discovered and managed devices to from the **Device Group** list.
   
   You can choose not to add devices to any device group. If you choose this option, the discovered devices are not added to any group. You must create the device groups before using them in the auto discovery process. For more information, see "Adding a device group" (page 128).

10. To configure the SNMP settings, click the configure icon located at **SNMP Settings** *(Required)* section.
The **SNMP Parameters** dialog box appears.

You can either enter the SNMP settings in this dialog box or you can use an SNMP template that contains the SNMP settings for this device. SNMP templates are particularly useful when SNMP configurations are standardized. For more information on creating SNMP templates, see "SNMP templates" (page 74).

**Editing SNMP settings manually**

1. To edit the SNMP parameters, verify that the radio button to the left of **Edit SNMP Parameters** is selected.
2. Do the following:
   a. **Parameter Type**: Select the version of SNMP (v1 or v2c) that is configured on the device to be added from the **Parameter Type** list. You can only add devices that are configured with SNMPv3 using SNMP templates. Therefore, you must create an SNMP template with the SNMPv3 parameters for this device before adding this device. For more information on creating SNMP templates, see "SNMP templates" (page 73).
   b. **Read-Only Community String**: Enter the read-only community string for this device in the **Read-Only Community String** field. This value must match the read only community string that is configured on the device to be added.
   c. **Read-Write Community String**: Enter the read-write community string for this device in the **Read-Write Community String** field. This value must match the read only community string that is configured on the device to be added.
   d. **Timeout**: Enter the SNMP timeout value (1–60 seconds) in the **Timeout** field. This parameter determines how long IMC waits for an SNMP reply from the managed device before declaring that the request has timed out. The default is 4.
   e. **Retries**: Enter the number of SNMP retries (1–20) in the **Retries** field. The retries parameter defines how many times the management system (IMC) sends SNMP retries in an attempt to communicate with the managed device before reporting a failure. The default is 3.

**Using existing SNMP template**

1. To configure the SNMP settings for this device using an SNMP template, click the radio button to the left of **Select an Existing Template**.
2. Click the radio button to the left of the SNMP template you want to use.
3. Click OK.
4. To configure the SNMP settings, click the configure icon located at the **Telnet Parameters** section. The SNMP Parameters dialog box appears.
5. Do one of the following:
   - Enter the SNMP settings in this dialog box, or
   - Create a SNMP template that contains the Telnet settings for this device.

SNMP templates are particularly useful when SNMP configurations are standardized. For more information on creating SNMP templates, see "SSH templates" (page 80).
Editing Telnet settings manually

1. To edit the Telnet parameters manually, verify that the radio button ☐ to the left of **Edit Telnet Parameters** is selected.

2. Do the following:
   a. **Authentication Mode**: Select the mode that corresponds with the Telnet authentication mode configured on the managed devices from the **Authentication Mode** list.
   b. **Username**: Enter the username configured on managed devices in the **Username** field, if prompted.
   c. **Password**: Enter the password configured on the managed devices in the **Password** field, if prompted.
   d. **Super Password**: Enter the super password configured on the managed devices for the **Super Password**, if prompted.
   e. **Timeout**: Enter the Telnet timeout value configured on the managed device in the **Timeout** field.
      Valid range is 1–60 seconds.

Using existing Telnet template

1. To configure the Telnet settings for this device using Telnet templates, click the radio button ☐ to the left of **Select an Existing Template**.

2. Click the radio button ☐ to the left of the Telnet template you want to use.

3. Click **OK**.

4. To configure the Telnet settings, click the configure icon 💡 located at the **Telnet Parameters** section.

5. The **Telnet Parameters** dialog box appears.

6. Do one of the following:
   o Enter the Telnet settings in this dialog box, or
   o Create a Telnet template that contains the Telnet settings for this device.

Telnet templates are particularly useful when Telnet configurations are standardized. For more information on creating Telnet templates, refer see “Telnet templates” (page 77).

Editing SSH settings manually

1. To edit the SSH parameters, verify that the radio button ☐ to the left of **Edit SSH Parameters** is selected.

2. Do the following:
   a. **Authentication Mode**: Select the authentication mode that corresponds with the SSH configuration mode on the managed devices from the list.
   b. **User Name**: Enter the username that is configured on managed devices.
   c. **Password**: If prompted, enter the password that is configured on the managed devices.
   d. **Private Key File**: Enter the path and filename of the private key file that contains the key that enables login, if prompted.
   e. **Private Key Password**: Enter the private key password for the private key file, if prompted.
f. **Super Password**: Enter the super password that is configured on the managed devices.

g. **Port**: Enter the TCP port for SSH configured on managed devices. The default TCP port is 22.

h. **Timeout**: Enter the SSH timeout value (1–120 seconds).
   The timeout parameter defines how long the system waits for the device to respond in seconds before declaring that the response has timed out. The default setting is 10 seconds.

i. **Retries**: Enter the number of SSH retries (1–5).
   The retries parameter defines how many times the management system (IMC) sends SSH retries in an attempt to communicate with the managed device before reporting a failure. The default setting is 3.

**Using existing SSH template**

1. To configure the SSH settings for this device using SSH templates, click the radio button ☐ to the left of **Select an Existing Template**.

2. Click the radio button ☐ to the left of the SSH template you want to use.

3. Click **OK** to accept the SSH configuration.

4. The filter settings offer you flexibility in determining which subnets and devices to either include in or exclude from the auto discovery process.

5. Enter the IP address subnet range and the subnet mask you want to filter by in the **Subnet IP** field.

   Masks can be entered using either CIDR or dotted decimal notation.

   For example, a valid network/subnet mask entry using CIDR notation would be 192.168.1.0/24
   where /24 represents the bits allocated to the network portion of the address and implying the remaining bits allocated to the host portion.

   Alternatively, a valid network/subnet mask using dotted decimal notation would be 192.168.1.0/255.255.255.0

6. Do one of the following:
   - Click the radio button ☐ to the left of **Yes** if you want IMC’s discovery to include devices captured by the subnet list,
   - Click the radio button ☐ to the left of **No** if you want IMC’s discovery to exclude devices captured by the subnet list.

   You can add more than one IP address/subnet range by clicking **Add** after entering the IP address range in the **Subnet IP** field.

7. If you want IMC to perform scheduled auto discoveries, select the frequency with which you want IMC to perform scheduled auto discoveries from the **Schedule** list.

   Options include **Never**, **Hour**, **Day**, **Week**, and **Month**. Select **Never** if you do not want IMC to perform automatic auto discoveries.

   If you choose to schedule an auto discovery for hour, you only need to enter the discover time.
   If you choose to schedule an auto discovery for a specific day, week, or month, enter the start date you want to begin the scheduled auto discovery in the **Start Date** field.
You can also use the calendar function to the right of the Start Date field to select and auto populate the field. Select the hour and minutes from the lists located to the right of the Discover Time field.

8. Click Save Only if you want IMC to save the auto discovery configuration and perform the auto discovery according to the schedule you have defined.

9. Click Auto Discovery if you want to begin the auto discovery immediately.
   If you clicked Auto Discovery, the Auto Discovery Running window is displayed along with details of the auto discovery process.
   While the auto discovery is running, IMC displays a rotating icon.

10. Click Stop if you want to cancel the auto discovery process.
    Once IMC has completed the auto discovery, it displays a status and summary of the auto discovery process at the top of the Auto Discovery Running window as well as a list of all discovered devices and the results in the Auto Discovery running list.

11. Review the results of the discovery process.
    You can also review the results of the auto discovery process by clicking the View Report link located below the Auto Discovery Running title bar.
    The report is displayed in an Intelligent Analysis Report Viewer window.

**Printing the report to PDF**

To print the report to PDF:

1. Click the print icon located on the toolbar on the top of the report.
2. Select the desired page range from Page Range.
3. Click Export.

**Exporting the report**

To export the report:

1. Click the export icon located on the toolbar on the top of the report.
2. Select the desired export file format from the File Format list. Options include Crystal Reports (RPT), Adobe Acrobat (PDF), Microsoft Excel (97-2003), Microsoft Excel (97-2003) Data-Only, Microsoft Word (97-2003) – Editable, Rich Text Format (RTF), and Comma Separated Values (CSV).
3. Click Export.

You can also review the results of the most recent auto discovery by clicking on the link Latest Result from the Resource → Auto Discovery page.

**Adding devices by importing device information**

IMC supports the import and export of devices and information. You can quickly and easily import the devices you want IMC to manage by using a well-defined file format or from NNMi.

In addition, you can also export device information into a CSV format for easy import into other management or reporting systems.
This section describes the import process as a quick and easy way to quickly manage only those devices you want to manage with IMC.

**Importing devices into IMC**

To add devices to IMC via importing device information:

1. **Navigate to Resource→Import/Export Device:**
   a. Click the Resource tab from the tabular navigation system on the top.
   b. Click Resource Management on the navigation tree on the left. Click Import/Export Device under Resource Management from the navigation system on the left.

2. Click the Import tab in the Resource→Import/Export Device window.

3. In the Input File field, enter the file name you want to use to import devices or click Browse to browse for the file on your local computer.
   You must create a valid import file prior to importing devices. This section describes all possible columns that can be used in a valid data import file and the rules for constructing a valid import file using these column definitions.

The field definitions for all possible columns in an import file are listed in Table 3 (page 173):

**Table 3 Import file column definitions**

<table>
<thead>
<tr>
<th>Column label</th>
<th>Column contents/requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>DeviceIp</td>
<td>This field contains the device IP address, which must conform to standard dotted decimal IP address formatting. This field is required.</td>
</tr>
<tr>
<td>DeviceName</td>
<td>Device name, a string of up to 64 characters. This field is optional.</td>
</tr>
<tr>
<td>SnmpParaVersion</td>
<td>This field contains the SNMP version. Possible values include: 1 = SNMPv1, which is the default</td>
</tr>
<tr>
<td>Note: If the SnmpParaVersion field is 3, an SNMPv3 template is created.</td>
<td></td>
</tr>
<tr>
<td>SnmpParaRead</td>
<td>This field contains the SNMP read-only community name, a string of up to 32 characters. The default is public. This field is optional.</td>
</tr>
<tr>
<td>SnmpParaWrite</td>
<td>This field contains the SNMP write community name, a string of up to 32 characters. The default is private. This field is optional.</td>
</tr>
<tr>
<td>SnmpParaContextName</td>
<td>This field contains the SNMPv3 context name, a string of up to 32 characters. This field is optional.</td>
</tr>
<tr>
<td>Column label</td>
<td>Column contents/requirements</td>
</tr>
<tr>
<td>----------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SnmpParaSecurityUser</td>
<td>This field contains the SNMPv3 user name, a string of up to 32 characters. Two users with the same name are considered as belonging to the same SNMPv3 template. This field is applicable to only SNMPv3.</td>
</tr>
<tr>
<td></td>
<td>This field is optional.</td>
</tr>
<tr>
<td>SnmpParaSecuMode</td>
<td>This field contains the security mode. This value must match the SnmpParaAuthScheme and SnmpParaPrivScheme values.</td>
</tr>
<tr>
<td></td>
<td>1 = no authentication and no encryption</td>
</tr>
<tr>
<td></td>
<td>2 = authentication but no encryption</td>
</tr>
<tr>
<td></td>
<td>3 = authentication and encryption</td>
</tr>
<tr>
<td></td>
<td>This field is optional.</td>
</tr>
<tr>
<td>SnmpParaAuthScheme</td>
<td>This field contains the Authentication mode.</td>
</tr>
<tr>
<td></td>
<td>1 = none</td>
</tr>
<tr>
<td></td>
<td>2 = MD5</td>
</tr>
<tr>
<td></td>
<td>3 = sha</td>
</tr>
<tr>
<td></td>
<td>This field is optional.</td>
</tr>
<tr>
<td>SnmpParaAuthPassword</td>
<td>This field contains the authentication password, a string of up to 32 characters.</td>
</tr>
<tr>
<td></td>
<td>This field is optional.</td>
</tr>
<tr>
<td>SnmpParaPrivScheme</td>
<td>This field contains the encryption mode.</td>
</tr>
<tr>
<td></td>
<td>1 = none</td>
</tr>
<tr>
<td></td>
<td>2 = DES</td>
</tr>
<tr>
<td></td>
<td>19 = AES128</td>
</tr>
<tr>
<td></td>
<td>20 = AES192</td>
</tr>
<tr>
<td></td>
<td>21 = AES256</td>
</tr>
<tr>
<td></td>
<td>This field is optional.</td>
</tr>
<tr>
<td>SnmpParaPrivPassword</td>
<td>This field contains the encryption password, a string of up to 32 characters.</td>
</tr>
<tr>
<td></td>
<td>This field is optional.</td>
</tr>
<tr>
<td>SnmpParaTimeOut</td>
<td>This field contains the timeout value in seconds, which is 4 by default.</td>
</tr>
<tr>
<td></td>
<td>This field is optional.</td>
</tr>
<tr>
<td>SnmpParaRetry</td>
<td>This field contains the number of retries, which is 3 by default.</td>
</tr>
<tr>
<td></td>
<td>This field is optional.</td>
</tr>
<tr>
<td>PingDevType</td>
<td>This field identifies whether or not the device responds to ping requests. The field is 0 by default.</td>
</tr>
<tr>
<td></td>
<td>1 = the discovered device responds to Ping requests.</td>
</tr>
<tr>
<td></td>
<td>0 = the discovered device does not respond to Ping requests.</td>
</tr>
<tr>
<td></td>
<td>This field is optional.</td>
</tr>
</tbody>
</table>

**Import file format requirements**

The requirements for a device import file are:
The extension of an import file must be CSV.

The first line or row of an import file must contain the following text only:

```
[DEF]
```

The second line or row of an import file must contain at least one or more of the column labels separated by commas. Column labels with null values must also be separated by commas.

Only the first column label, DeviceIP, is required. All other columns are optional.

You must specify ONLY those columns in the second line or row that contain values in the device entry rows (line 3 and beyond) of the data import file. If, for example, you do not intend to include in your data import file, the public and private community strings for the devices you want to import, then do not include these column labels (SNMPParaRead and SnmpParaWrite) in the second line of your import file.

For example, a valid entry for the second line of an import file that includes some but not all column labels is provided below.

```
DeviceIp, DeviceName, SnmpParaVersion, SnmpParaRead, SnmpParaWrite,,,,,,
SnmpParaTimeOut, PingDevType.
```

The third line or row of an import file must contain the first entry for a device you want to add to IMC with field values (including fields with null values) separated by commas. All subsequent rows must follow the same conventions as the third line or row.

The third line or row must contain values only for the columns specified in line two of the data import file. In other words, if you did not specify a column label in line two, then you cannot specify the value in the third and all subsequent rows.

A valid entry for lines 3 and 4 of an import file for the line 2 example provided above would be:

```
DeviceIp,DeviceName,SnmpParaVersion,SnmpParaRead,SnmpParaWrite,,,,,,,,SnmpParaTimeOut,,PingDevType
192.168.0.1,router1,1,public,private,,,,,,,,3,,0
192.168.0.2,switch1,2,public,private,,,,,,,,3,,0
```

Notice that these two lines have values for only those columns that were specified in line two.

Here is a complete, sample import file using the examples provided above that use some but not all of the column definitions possible for data import.

```
[DEF]
DeviceIp,DeviceName,SnmpParaVersion,SnmpParaRead,SnmpParaWrite,,,,,,,,SnmpParaTimeOut,,PingDevType
192.168.0.1,router1,1,public,private,,,,,,,,3,,0
192.168.0.2,switch1,2,public,private,,,,,,,,3,,0
```

4. Click **Import** to begin the import process.
   The page is updated with the results of the device import.

5. Review the results found on the Device Import Results page to verify that all the devices have been imported successfully.

### Exporting device information

To export device information from IMC:

1. Navigate to **Resource→Import/Export Device**:
   a. Click the **Resource** tab from the tabular navigation system on the top.
b. Click **Resource Management** on the navigation tree on the left.

c. Click **Import/Export Device** under **Resource Management** from the navigation system on the left.

2. To export devices, click the **Export** tab in the **Resource → Import/Export Device** window.

3. Click **Export** to begin the export process.

4. To view and save the results of your export, click **Device Export Result** link located below the **Download File** portion of the **Resource → Export Result** page.

Follow the instructions to complete the process of saving the export results.

**Importing devices from NNMi**

To import device information to IMC via NNMi:

1. Navigate to **Resource → Import/Export Device**:
   a. Click the **Resource** tab from the tabular navigation system on the top.
   b. Click **Resource Management** on the navigation tree on the left.
   c. Click **Import/Export Device** under **Resource Management** from the navigation system on the left.

2. To import devices from NNMi, click the **Import Devices from NNMi** tab in the **Resource → Import/Export Device** window.

3. Enter the parameters of NNMi.
   - **Server IP Address**: Allows you to configure the server IP address of NNMi for communications with IMC.
   - **Server Port**: Allows you to configure which port NNMi uses for communicates with IMC.
   - **User Name**: Allows you to configure the username of NNMi for communicates with IMC.
   - **Password**: Allows you to configure the password of NNMi for communicates with IMC.

4. Click **Import** to begin the import process.

   The page is updated with device information imported from NNMi.

5. Review the results found on the **Device Import Results** page to verify that the devices have been imported successfully.

   IMC supports importing devices from NNMi 9.00 or higher.

   The passwords and private keys of the devices are not imported into IMC. You must configure them after the devices are imported.

**Viewing devices with Device, IP, and Topology Views**

IMC offers you a variety of options for viewing network resources and for drilling down into the features used to manage them. IMC provides you with a graphical representation of the physical network in the **Topology** view. Table views of the network are provided in the **Device View**, **IP View** and **Custom View**. Each of these three view types offer you a real time snapshot of the status of
devices in the network infrastructure. Also, all views offer drilldown capabilities to devices within the groups and ultimately to the device details for an individual device. The **Device Details** page provides you with access to IMC’s network device management features.

## Viewing devices via the Device View

In the **Device View**, you can easily locate network resources by device type – Routers, Switches, Servers, Security, Storage, Wireless, Voice, Desktops and Others. IMC classifies devices that respond to ICMP requests but not SNMP requests as "Desktop" devices. IMC classifies as "Other" devices that respond to both ICMP and SNMP but do not conform to any of IMC’s device classifications. IMC organizes devices into the **Device View** groupings by using the information stored in the **Device Category** field.

This view, like all IMC views, offers you a real time snapshot of the status of devices in the network infrastructure through color-coded icons that match the highest severity or alarm level for devices in the view. Also, all views offer you high-level groupings of devices with drilldown capabilities to devices within the groups and ultimately to the device details for an individual device. From the **Device Details** page, you can access IMC’s powerful management features that enable quick and easy access to network resources as well as the ability to manage them.

### Accessing the Device View

To access the **Device View**:

1. Navigate to **Resource→View Management→View-<Device Type>**:
   a. Click the **Resource** tab from the tabular navigation system on the top.
   b. Click **View Management** on the navigation tree on the left.
   c. Click **Device View** under **View Management** from the navigation system on the left.
2. Click the category of device view you want to access.
   The **Device List** for the device category you choose appears.
   To view all device groups under **Devices View**, you may need to click the expand icon 📦.
   - Click 📦**Routers** under **Devices View** from the navigation tree on the left for a summary view of all routers.
   - Click 📦**Switches** under **Devices View** from the navigation tree on the left for a summary view of all switches.
   - Click 📦**Servers** under **Devices View** from the navigation tree on the left for a summary view of all servers.
   - Click 📦**Security** under **Devices View** from the navigation tree on the left for a summary view of all security devices.
   - Click 📦**Voice** under **Devices View** from the navigation tree on the left for a summary view of all voice devices.
   - Click 📦**Desktops** under **Devices View** from the navigation tree on the left for a summary view of all desktop devices.
Click **Others** under **Devices View** from the navigation tree on the left for a summary view of all devices that were not classified by the categories listed above.

Each category of device in the **Device View** is followed by a number that is enclosed with square brackets []. This number represents the number of devices in that category.

The status of a **Device View** depends on the status of the devices in it. The color of the group icon represents the highest severity or alarm setting of all devices in the category. The icon of a device view is grayed out if there is no device in the view.

The device status in a router view reflects the severest status among all layer 3 interfaces of the router that have an IP address. For example, if any of the layer 3 interfaces is DOWN, the layer 3 interface status of the router is DOWN. Any disabled or unknown interface is blocked out for status calculation.

The device status in a switch view reflects the severest status among all interfaces of the switch. For example, if any of the interfaces is DOWN, the interface status shown in the list is DOWN. Any disabled or unknown interface is blocked out for status calculation.

IMC displays all **Device View** entries in the **Device List** displayed in the main pane of the **Device View** window.

The following list contains all of the fields that are displayed for all device categories. The list of each of the device categories may contain some or all of these fields:

- **Status**: Contains the most current status of the device. Status is determined by the highest severity or alarm level for the device, when the device has one or more current alarms that has not been cleared or recovered.

- **Device Label**: Contains the IMC name for the device, which, by default, is the name assigned to it by IMC in its device configuration. If a device is configured with a sysName, the sysName is used as the **Device Label** unless the **Device Label** is manually configured. This field also contains the IP address. The contents of the device label field serve as an active link for drilling down into the **Device Details** page. This offers you convenient access to device management features for the selected device.

  You can modify the device label from the **Device Details** page. This changes IMC’s name or label for the device in IMC only. It does not change the name of the device on the device itself.

- **Device Category**: Contains the device type, such as router, switch, and server.

- **Online Users**: Displayed for switches or routers only, contain a list of all online users who are currently authenticated and accessing the network through this device. Contains users only when the UAM module is installed and in use.

- **Contains information on the model of the device.**

- **IP Address**: Contains the IP address of the device.

- **Interface List**: Contains a link that displays a list of all interfaces on the device. This field appears on the **Device List** of the **View-<Device Type>** page, but does not appear on the **Device List-ALL** of the **Device View** page. This list includes interface status as well as a link to view and take action on specific interfaces. For more information on the **Interface Details** page, see “Interface details” (page 268).

- **Operation**: Contains an icon that displays links to operational tasks for the associated device.
You can sort the device list by a column by clicking the column label. Click the column label to sort the list by the selected field. The column label is a toggle switch that allows you to toggle between the various sort options specific to each field.

If the Device List contains enough entries, the following navigational aids are displayed:

- Click ° to page forward in the Device List.
- Click ° to page forward to the end of the Device List.
- Click ° to page backward in the Device List.
- Click ° to page backward to the front of the Device List.

3. Click 8, 15, 50, 100, or 200 from the right side of the main pane to configure how many items per page you want to view.

IMC enables you and you to manage multiple devices via the Device View. This includes deleting, synchronizing, managing and unmanaging devices. For information on managing multiple devices through these views, see "Managing multiple devices using batch operations" (page 276).

**Viewing devices via the IP View**

The IP View offers you a view of network resources by the IP address ranges found in the discovery process or added manually.

This view, like all IMC views, offers you a real time snapshot of the status of devices in the network infrastructure through color-coded icons that match the highest severity or alarm level for devices in the view.

Also, all views offer you high-level groupings of devices with drilldown capabilities to devices within the groups and ultimately to the device details for an individual device. From the Device Details page, you can access IMC’s powerful management features that enable quick and easy access to network resources as well as the ability to manage them.

**Accessing the IP View**

To access the IP View:

1. Navigate to Resource→View-IP View:
   a. Click the Resource tab from the tabular navigation system on the top.
   b. Click View Management on the navigation tree on the left.
   c. Click IP View under View Management from the navigation system on the left.

2. To view all IP subnets under IP View, you may need to click the expand icon ° to the left of IP View.

3. Click the IP address subnet view you want to view devices for.
   The Device List for the IP subnet you choose appears.

Each IP address subnet in the IP View is followed by a number that is enclosed with square brackets ([[]]). This value represents the number of devices in that subnet.

IMC displays all IP View entries, including subnets and individual devices in the IP View Device List displayed in the main page of the IP View window.
Device List contents

- **Status**: Contains the most current status of the group. Status is determined by the highest severity or alarm level for a device in the group, when the device has one or more current alarms that has not been cleared or recovered. Group icons with the color gray indicate that there are no managed devices in the view.

- **Device Label**: Contains the IMC name for the device, which, by default, is the name assigned to it by IMC in its device configuration. This field also contains the IP address. The device label serves as an active link for drilling down into an IP address subnet **Device List** or into the **Device Details** page of an individual device.

- **Device Category**: Contains the IMC device category for the associated device.

- **Device Model**: Contains device model information. If the device is managed for reachability using ICMP only and thus no device model information is available, this field contains "ICMP."

- **IP Address**: Contains the IP address of the device.

- **Operation**: Contains an icon that displays links to operational tasks for the associated device.

You can sort the **IP View List** by every field with the exception of the **Operation** fields. Click the column label to sort the list by the selected field. The column label is a toggle switch that allows you to toggle between the various sort options specific to each field.

The status of an **IP View** or IP subnet depends on the status of the devices in it. The color of the group icon represents the highest severity or alarm setting of all devices in the IP subnet. The icon of an IP view or subnet is grayed out if there is no device in the view.

If the **Device List** contains enough entries, the following navigational aids are displayed:

- Click ▶ to page forward in the **Device List**.

- Click ▶ to page forward to the end of the **Device List**.

- Click ◀ to page backward in the **Device List**.

- Click ◀ to page backward to the front of the **Device List**.

4. **Click 8, 15, 50, 100, or 200** from the right side of the main pane to configure how many items per page you want to view.

5. Do one of the following:

   - To hide empty IP subnets, click the hide empty subnets icon on the **IP View** navigation tree on the left, or

   - To display empty edge subnets, click the display empty edge subnets icon located on the **IP View** navigation tree on the left.

IMC enables you and you to manage multiple devices via the IP View. This includes deleting, synchronizing, managing and unmanaging devices. For information on managing multiple devices through these views, see “Managing multiple devices using batch operations” (page 276).
Viewing devices via the Network Topology

**Network Topology** provides you with a graphical view of the health and status of network connectivity and devices, allowing you to quickly and easily locate, monitor, modify, and manage network devices directly from this graphical representation of the network.

In addition to the standard drilldown capabilities of all views, the **Network Topology** offers special navigation capabilities accessed via left and right mouse clicks, allowing you to monitor network devices and gain quick access to the device management features of IMC, respectively. For more information on these capabilities, see “Topology Maps” (page 50).

Accessing the network topology

To access the network topology:

1. Click the **Resource** tab from the tabular navigation system on the top.
2. Click **View Management** on the navigation tree on the left.
3. Click **Network Topology** under **View Management** from the navigation system on the left.

Navigating the network topology interface

Upon a successful auto discovery, IMC automatically generates topology maps and organizes discovered devices into topology views based on the groupings found. The groupings are navigated using the topology navigation system located on the left of the **Network Topology** map. To expand the groupings displayed on the left navigation system, click the expand icon .

The created topology groupings include:

- **Custom Topology**: Contains topology views for the custom views that the operator has management rights to and contains the custom views that you have been granted access to as well as any custom views that have been created.
- **IP Topology**: Contains topology views of devices grouped by IP address.
- **Data Center Topology**: Contains user-defined views created by the administrator or operator. The Data Center Topology contains any custom data center maps that include floor plans and graphical representations of data centers down to individual racks and the devices in them.
- **VNM Topology**: Contains a view of the virtual network devices, including physical servers, hosts and vSwitches on each physical server, and how they are connected.
- **Access Service Topology**: Contains user access information that is generated by the add-on User Access Manager (UAM) module.
- **MPLS VPN**: Contains MPLS information that is generated by the add-on MPLS VPN Manager (MVM) module.
- **WSM Service Topology**: Contains wireless service information that is generated by the add-on Wireless Service Manager (WSM) module.

The navigation tree on the left allows you to move quickly to the particular view displayed in the navigation tree.

For example, clicking one of the custom views you have created opens a new tab in the main pane and displays all of the device icons for the devices in the selected **Custom Topology**.
Clicking one of the **IP Topology** opens a new tab in the main pane and displays all of the devices in the selected **IP Topology** group.

**Topology map toolbar**

The **Topology Maps** interface includes several menu options that support the use and customization of topology maps. These toolbar options are described below.

- **Displays the network in its original proportion.**
- **Enables you to zoom in on the topology view.**
- **Enables you to zoom out on the topology view.**
- **Enables you to fit the contents of the topology view into the window.**
- **Enables you to magnify the contents on the topology view. To exit magnify mode, click on the icon again.**
- **Provides a separate bird’s eye view window of the topology map.**
- **Enables you to grab and move one or multiple objects in the topology view within the confines of the pane. Click the icon to switch to the Pointer Tool, which allows you to move the entire topology view within the confines of the pane.**
- **Enables you to browse and load a background image into the topology view. You can import a Google Map as the background image.**
- **Enables you to remove a background image from the topology view.**
- **Allows you to save topology view settings.**
- **Expands the topology view to full screen. To exit full screen mode, right-click the topology view and select Exit Full Screen from the shortcut menu.**
- **Enables you to save the current topology view as an image (.png) file.**
- **Enables you to organize icons according to a pre-defined structure to the topology view. Options for organizing topology views include union length, tree, star, ring or grid.**
- **Navigates you to the Resource→Add Device dialog box for adding device to IMC. For more information on adding a device in IMC, see “Adding devices manually to IMC” (page 154).**
- **Allows you to add a cloud icon to the topology view.**
- **Enables you to add a note on the topology view.**
- **Allows you to add a link on the topology view.**
* Allows you to browse, add, and query links on the topology.
* Allows you to select a vManager to view the topology.
* Offers you the ability to search and retrieve devices in the topology view by IP address or by IMC label. In data center view, you can locate a device in the rack topology according to its asset number.
* Displays a legend for the topology view.
* Enables you to back to the upper-level topology.
* Allows you to select an MST instance.
* Allows you to view the MSTP Region Details.
* Displays a list on the right of all VLANs. Selecting a VLAN from this list filters the topology view to highlight only those devices that are members of the selected VLAN.
* Allows you to have a data center topology map automatically built. For more information on automatically building data center topology maps in IMC, see "Automatically building data center topology maps" (page 194).
* Displays the Traffic Topology. The Traffic Topology feature applies only to the current topology. For more information on the traffic topology, see "Viewing traffic with traffic topology" (page 199).
* Allows you to customize the topology view by defining the tree and grid layout, save, display and color options.

Left & right mouse clicks: Monitoring & management

Topology maps have special left and right-click mouse features. The left mouse click supports device monitoring options while the right mouse click supports device management options.

Device and link monitoring via the left mouse click

To display information about a node or link, left-click the selected node or link on the topology map. The information displayed varies based on the node or link type selected.

To select a node or link, click the node or link using the left mouse button. Some of the information displayed provides links that allow you to drill down into IMC features or perform certain actions:

- **Device Label:** This field contains the IMC name for the device that is assigned during the configuration. If the device has a sysName at the time of configuration, this name becomes the Device Label.

The device label serves as an active link for drilling down into the **Device Details** page, which provides convenient access to device management features. The **Device Details** page loads in the browser instance that originally launched the topology maps, not in the browser instance that has the topology maps loaded.

- **IP Address:** Contains the management IP address of the device.
• **Mask**: Contains the mask of the management IP address.

• **Device Status**: Contains the most current status of the device. Status is determined by the highest severity or alarm level for the device, when a device has more than one current alarm that has not been cleared or recovered. Gray device icons indicate the device is unmanaged.

• **SysName**: Contains the name that is configured on the device.

• **Vendor**: Contains the device vendor’s name.

• **Unrecovered Alarms**: Contains the number of unrecovered alarms by type. Click the alarm level to drill down to the **All Alarms** view for this device. The **All Alarms** page loads in the browser instance that originally launched the topology maps, not in the browser instance that has the topology maps loaded. For more information on viewing alarms from the **All Alarms** view, see “Browsing all alarms” (page 580).

• **Performance Metrics**: IMC also displays performance metrics via the left mouse click. The value displayed serves as a hyperlink for viewing a performance report for the last hour for the selected metric.

For links, the left mouse click includes the following:

• **Link Name**: Contains a name for the link if one is available. Otherwise, a device label displays.

• **Link Type**: Contains information about the link type.

• **Left Node**: Contains the device label for the device that is located on the left of the link as represented in the topology map.

• **Left Interface**: Contains the interface name for the device that connects on the left in the topology map.

• **Left Interface Alias**: Contains the interface alias for the device that connects on the left in the topology map.

• **Right Node**: Contains the device label for the device that is located on the right of the link as represented in the topology map.

• **Right Interface**: Contains the interface name for the device that connects on the right in the topology map.

• **Right Interface Alias**: Contains the interface alias for the device that connects on the right in the topology map.

• **Link Speed**: Contains the speed of the link in bits per second.

**Device management via the right mouse click**

A right mouse click with a node selected on the topology map displays a list of management options that can be used to manage the selected node or link and a right mouse click with nothing selected displays a menu for map configuration.

The right mouse click on a device includes one or more of the following management options, depending on the view and device model:

• **Create Subview**: Allows you to create logical subviews of devices that are displayed on the topology map for all users of the topology map. For more information on creating subviews, see "Customizing topology maps" (page 187).

• **Open Web-Based NMS**: Allows you to launch the Web Manager interface for the selected device directly from the topology map. Selecting this option opens the **Web Manager** in a new
browser window that can be accessed via the tabs located at the top of the main pane. From this window, you can manage the selected device. For more information on the Web Manager, see "Open web manager" (page 218).

- **Open Device Panel**: Allows you to launch the Device Panel interface for the selected device directly from the topology map. Selecting this option opens the Device Panel in a new pane in the topology window that can be accessed via the tabs located at the top of the main pane. From this window, you can manage the selected device. For more information on the Device Panel, see “Open device panel” (page 221).

- **Copy**: Allows you to copy a device.

- **Device Information**: Opens the Device Details page for the selected device. The Device Details page loads in the browser instance that originally launched the topology maps, not in the browser instance that has the topology maps loaded. For more information on the Device Details page, see “Managing one device via device details” (page 212).

- **Neighbor Topology**: Enables you to view a portion of the network from the perspective of the selected device. When prompted, select the number of hops you want to include. IMC opens a new pane in the topology window for this map, which can be accessed via the tabs located at the top of the main pane. From this window, you have access to the monitoring features available using the left mouse click only.

- **Spanning Tree**: Enables you to view Spanning Tree information for the selected device. Basic Spanning Tree information as well as instance level information is provided in this feature. For more information on configuring Spanning Tree for devices that support it, see "Managing MSTP options for routers and switches" (page 263).

- **Tools-Ping**: Enables you to launch a ping request sent from the IMC server to the selected device and launched from the topology map. IMC opens a new browser window for the ping operation and the results of the ping operation display in the new browser instance.

- **Tools-Telnet**: Enables you to launch a telnet session for the selected device directly from the topology map that prompts you for the application on the local computer that supports Telnet.

- **Tools-Traceroute**: Enables you to launch a traceroute request sent from the IMC server to the selected device and launched from the topology map. IMC opens a new browser window for the Traceroute operation and the results of the traceroute operation display in the new browser instance.

- **Tools-SSH**: Enables you to launch an SSH session for the selected device directly from the topology map that prompts you for the application on the local computer that supports SSH.

- **Delete**: Enables you to delete devices from IMC, removing the selected device from all views and all data associated with the device during the next scheduled Data Export, which by default is 2:00am daily.

⚠️ **WARNING:**

Once a device is deleted, it cannot be recovered. Use this feature with caution.

- **Delete from Subview**: Enables you to remove the selected device from its current subview and return it to the parent view. Note that deleting the last device from the subview removes the subview from the topology view. This option appears only on the device that belongs to a subview.
- **Delete Device from This View**: Enables you to remove the selected device from the current view if the device is not a member of any subview.

- **Modify Label**: Enables you to change IMC’s name for the selected device from the topology map. Note that changing the Device Label in IMC does not change the device name or sysName on the device itself.

- **Synchronize**: Enables you to update IMC views with current data for the selected device.

- **Unmanage/Manage**: Acts as a toggle switch, enabling you to unmanage or manage the selected device in IMC. During discovery, IMC adds all discovered devices to the IMC database and configures them to be managed. Managed devices contain features that are available for monitoring and managing the devices. Each device, managed or unmanaged, requires a node license.

- **Lock/Unlock**: Enables you to fix the position of a particular device on the topology map, rendering it unmovable until the device is unlocked. This feature is also a toggle switch that enables you to either lock or unlock the selected device.

- **Root Alarms**: Opens the **Current Alarms** page for the selected device, enabling you to view the current alarms for the selected device. The **Current Alarms** page loads in the browser instance that originally launched the topology maps, not in the browser instance that has the topology maps loaded. For more information on the **Current Alarms** page, see "Browsing root alarms" (page 575).

- **Performance at a Glance**: Launches the performance reporting feature of IMC and displays the most current data for the selected device. In this window, you can also configure a date and time window for viewing performance data for the selected device. The performance reports page loads in the browser instance that originally launched the topology maps, not in the browser instance that has the topology maps loaded. For more information on the **At a Glance** page, see "Performance at a glance" (page 230). The Performance at a Glance option on the right mouse click menu is available only if monitoring instances have been created for the selected device.

- **Configuration Center**: Launches the **Configuration Center** module for the selected device, enabling you to launch configuration management tasks from the topology view. The Configuration Management page loads in the browser instance that originally launched the topology maps, not in the browser instance that has the topology maps loaded. For more information on Configuration Management, see "7 Configuration and change management" (page 403).

- **MIB Management**: Launches the MIB management module for the selected device, enabling you to launch MIB browser tools from the topology view. The MIB Management page loads in the browser instance that originally launched the topology maps, not in the browser instance that the topology maps loaded. For more information on MIB Management, see "MIB management" (page 138).

- **Open Wireless Topology**: For wireless devices, opens a new page in the main pane of the topology window and displays the wireless devices with the same monitoring and management features as the network topology view. The wireless topology page can be accessed through tabs located at the top of the main pane of the topology page.

- **Add Device to Cabinet**: Creates custom maps through the Data Center Topology that depict data centers down to wiring closets and racks and the devices housed in them. This feature enables you to quickly and easily add the selected device to an existing cabinet. Note that this option is only available if the selected device has not yet been added to a cabinet. For more information
on customizing Data Center topology maps, see "Managing data center topology maps" (page 190).

- **Cabinet Location**: If a device has been added to a cabinet in the data center topology map, the Cabinet Location option becomes available on the right mouse click menu of the device. This feature launches a Rack Topology page displaying the rack with the selected device highlighted. The Rack Topology page can be accessed through tabs located at the top of the main pane of the topology page.

- **Open Stack Topology**: If the device is a stack device, the Open Stack Topology option becomes available on the right mouse click menu of the device. This feature launches a Stack Topology page displaying the internal structure of the stack with the selected stack device. The Stack Topology page can be accessed through tabs located at the top of the main pane of the topology page. For more information on the stack topology, see "Managing stack devices with the stack topology" (page 197).

**Link management via the right mouse click**

A right mouse click with a link selected on the topology map displays a list of management options that can be applied to the selected link and a right mouse click with nothing selected will display a menu for map configuration.

The right mouse click on the selected link includes one or more of the following management options for links:

- **Link Information**: Provides you with detailed information on the selected link, including basic information as well as information about the interfaces on either side of the link. Information includes link name, status, device information, operational and administrative status of each interface, IP address and subnet information and more. On the Left/Right Interface tab, you can view MP interfaces and PoE interfaces.
- **Modify Link Name**: Applies a label or name in IMC for the selected link.
- **Modify Interface**: Modifies the interface on either side of the selected link.
- **Delete Link**: Deletes the link.
- **Copy**: Copies a link.

**Customizing topology maps**

You can customize the topology maps. Options for customizing topology maps include creating subviews, adding clouds, adding devices, setting default topology views, configuring device and link labels and creating views of multiple levels which are not restricted.

**Custom topology management via the right mouse click**

The right mouse click menu allows you to re-load custom views, add custom views, add custom views, and set the default topology. The menu contains the following options:

- **Reload**: Refreshes the current topology view.
- **Add View**: Allows you to add a custom view.

To add a custom view:

1. Right-click a blank area in the Custom Topology, and select **Add View** from the shortcut menu. The **Add View** window appears.
2. Enter the view name.
3. Select an upper-level view for the custom view in the Up Level View list.
4. Specify whether to automatically add the newly added devices to the view.
   The options in the Automatically Add New Devices list include:
   - None: Not automatically adding the newly added devices to the view.
   - All: Automatically adding every newly added device to the view.
   - From Network Segment: Automatically adding newly added devices whose IP addresses are on the specified IP network segment to the view.
5. Click the check box to the left of Add all devices of the current system to add all devices in IMC to the view. Clear the check box to add the specified devices to the view.
6. Click Add to enter the Select Devices window.
7. Add devices using either the By View or the Advanced query option. See "Adding devices by View" (page 85) and "Adding devices by Advanced query" (page 85).
8. Highlight the devices you want to select and do one of the following:
   - To add them to the Selected Devices list, click Add selected, or
   - To select all of the devices displayed in the Devices Found list, click Add all, or
   - To remove one or more, select them and click Remove selected, or
   - To remove all of the selected devices, click Remove all.
9. Confirm that the devices you have found have been added.
10. Click OK.
11. To delete devices, select from the following options:
    - Make sure that the devices to be deleted are on the list, select the devices to be deleted, and click Delete to delete the devices from the list, or
    - If you select the From Network Segment option of the Automatically Add New Devices list, you can specify an IP address segment, so that the newly added devices whose IP addresses are on the specified IP network segment are automatically added to the view.
      a. Click Add to enter the Adding IP window.
      b. Enter the start IP address in the Start IP field.
      c. Enter the end IP address in the End IP field.
      d. Click OK.
12. Make sure that the start IP address and end IP address are displayed on the IP address list.
13. Select the IP address segment to be deleted, and click Delete to delete the selected IP address segment.
14. Click OK.
   - Set Default Topology View: Enables you to define which topology view loads when an operator selects the Network Topology link located on the navigation tree on the left of IMC’s web interface. By default, the Custom View is loaded.
   - Zoom: Enables you to zoom in or out of the topology view or to fit the contents of the topology map into the current window.
Topology map options

Right click your mouse on the topology background to access menus for using and customizing topology maps. The options for customizing topology maps include:

- **Create Subview**: Enables you to create logical device views. From the Create Subview dialog box, you can add devices to the subview using the View or Advanced query feature.
- **Add Cloud**: Enables you to add a cloud icon to the topology view.
- **Add Note**: Enables you to add a note for a topology view.
- **Add Device**: Enables you launch the Add Device page found under the Resource tab, Resource→Add Device. Using the Add Device feature, you can add devices to IMC. The Add Device page loads in the browser instance that originally launched the topology maps, not in the browser instance that has the topology maps loaded. For more information on using the Add Device feature, see "Adding devices manually to IMC" (page 154).
- **Add Device to This View**: Enables you to add one or more devices to this view.
- **Modify View**: Enables you to modify this view. This feature also enables you to modify the upper-level view of this view.
- **Add Link**: Enables you to add a link.
- **Link Management**: Provides a shortcut to the link management. This feature enables you to view all links in the view, and add, query, or delete a link. For other link management operations, see "Link management via the right mouse click" (page 187).
- **Find**: Launches a simple dialog box that enables you to search IMC for a device by IP address or device label. The results display in the Find Result dialog box in a tabular format.
- **Paste**: Enables you to paste the copied device nodes or links to the specified custom topology. This feature applies to only device nodes and links. Before pasting a link to a custom topology, you should copy the devices at both ends of the link to the custom topology. This feature is not available for IP topologies and Layer 2 topologies. In a custom topology, you can paste the copied device nodes or links to a subview.
- **Reload**: Refreshes the current topology view.
- **Path Topology**: Enables you to trace a path between any two devices by entering their IP addresses. The results of the path topology view displays in a new page in the main pane of the topology page. This view can be accessed through the tabs located at the top of the main pane.
- **Set Default Topology View**: Enables you to define which topology loads when an operator selects the Network Topology link located on the navigation tree on the left of IMC’s web interface. By default, the Custom View is loaded.
- **Device Label**: Allows you to decide which label is used to denote the various devices displayed on a topology map. Options include Show IP, Show Label, Show SysName, Show Vendor, Show Device Type, and No Label.
- **Link Label**: Allows you to decide which label is used to denote the various links displayed on a topology map. Options include Show Name, Show Type, Show Node (Device Name), Show Interface, Show Interface Alias, and No Label.
- **Hand**: Enables you to grab and move the topology view within the confines of the pane. To exit this mode, select Pointer Tool from the menu.
- **Zoom**: Enables you to zoom in or out of the topology view or to fit the contents of the topology map into the current window.
Managing data center topology maps

Data center topology maps enable you to create realistic maps of the data center down to the individual racks and cabinets and the devices that populate them. Upon installation, the Data Center Topology map is a blank page that allows you to customize the options that are available via right mouse clicks. You can create nested maps up to four layers deep (data center, building room, and cabinet or rack) displaying the physical layout of the data centers in the organization. For example, one or more buildings can be nested in the top level data center topology map, one or more rooms can be nested in a building, one or more wiring cabinets or racks can be nested in a room, and one or more devices can be added to the racks and cabinets as they actually exist in the data center. You can locate a device in the room topology according to its asset number. You can manually configure data center topology maps or have them automatically built.

Manually configuring data center topology maps

IMC provides a high-level data center topology map, which is a blank page upon which you can create a visual representation of your data center. On the data center page, you can add clouds, buildings or rooms.

You cannot add wiring cabinets or devices to the data center view. You must first create a building or room. You can only add wiring cabinets to rooms and devices to wiring cabinets. The following section describes the various data center map levels and their menu options.

Data center topology maps

There are many options for customizing the top-level map of the data center topology. You can create multi-level nested maps representing the physical layout of the data centers in your organization, add one or more clouds, or add one or more buildings to the data center map, however adding buildings to topology maps are optional. You can add one or more rooms to the data center map.

To access the data center topology map:
1. Click the Resource tab from the tabular navigation system on the top.
2. Click View Management on the navigation tree on the left.
3. Click Network Topology under View Management from the navigation system on the left.
   A new browser instance opens and an icon labeled Custom Topology displays in the main pane of the page. A navigation system displays on the left.
4. Double click Data Center Topology under Topology.
   A new page for the Data Center Topology displays in the main pane. Multiple pages in the main pane can be navigated using the tabs located at the top of the main pane.

You can access data center topology configuration options through right mouse clicks. Data center map menu options include:

- **Find**: This feature enables you to locate a device in the rack topology.
  a. To locate the device, right-click the Data Center Topology map.
  b. Select Find from the shortcut menu.
     - The Find window appears.
   c. Input the partial or full asset number of the device you want to find.
d. Click **Find**.
The matched devices are displayed on the **Find Result** window.

e. Click a device name to see the location of the device in the chassis topology.

- **Reload**: This option refreshes the page after you have made changes to it. Once you have added a building or room to the data center map, click **Reload** to view and access the cloud, building, or room containers you have added.

**Add data centers**

This option enables you to add one or more data center to the data center topology map.

To add a **Data Center**:

1. Right-click the data center topology map.
2. Select **Add Data Center** from the shortcut menu.
3. Enter a name for the data center.
4. Select the layer.
5. Click **OK**.
6. Select **Reload** from the right mouse click menu to refresh the data center map.

**Add room**

This option enables you to add one or more rooms to the data center topology map.

To add a room:

1. Right-click the data center topology map.
2. Select **Add Room** from the shortcut menu.
3. Enter a name for the room.
4. Select the background.
5. Click **OK**.
6. Select **Reload** from the right mouse click menu to refresh the data center map.

**Add cloud**

This option enables you to add one or more clouds to connect to data centers. The clouds represent the external networks.

To add a cloud:

1. Right-click the data center topology map.
2. Select **Add Cloud** from the shortcut menu.
3. Enter a name for the cloud.
4. Click **OK**.
5. Select **Reload** from the right mouse click menu to refresh the data center map.

- **Set Default Topology View**: Enables you to make this the view that is loaded when you click network topology view from **Resource**→**View Management**→**Network Topology**.
- **Hand**: Enables you to grab and move the topology view within the confines of the pane. To exit this mode, select **Pointer** from the menu.
- **Zoom**: Enables you to zoom in or out of the topology view or to fit the contents of the topology map into the current window.
- **Adjust Background**: Enables you to adjust background of the topology.

### Add building topology maps

You can add one or more rooms to a building topology map; however, you cannot add wiring cabinets or devices to the building map. You must create buildings first, then rooms and add wiring cabinets to rooms. While rooms are required to add wiring cabinets, buildings are optional. You can add rooms directly to the data center topology map.

To access a building map:

1. Click the **Resource** tab from the tabular navigation system on the top.
2. Click **View Management** on the navigation tree on the left.
3. Click **Network Topology** under **View Management** from the navigation system on the left. A new browser instance opens and an icon labeled **Custom Topology** displays in the main pane of the page. A navigation system displays on the left.
4. Double click **Data Center Topology** under **Topology**. A new page for the **Data Center Topology** displays in the main pane. Multiple pages in the main pane can be navigated using the tabs located at the top of the main pane.
5. To access a data center, do one of the following:
   - Double click the icon for the map you want to access, or
   - Right-click the data center icon and select **Expand** from the shortcut menu.
     A view of the data center expands in the existing page. Use the tabs at the top of the page to navigate between data center map options.
6. To close to a data center icon, right-click the data center icon and select **Collapse** from the shortcut menu.

The data center topology map also has right mouse click menu for configuring the data center map. Menu options for the data center map are:

- **Rename**: Renames the data center.
- **Delete**: Enables you to delete the current data center from the data center map. After you select **Delete**, right-click on **Reload** from the data center map to view the updated data center map.
- **Automatically Build DC Topology**: Enables you to have a data center topology map automatically built for the building. For more information on automatically building data center topology maps in IMC, see "Automatically building data center topology maps" (page 194).
- **Expand/Collapse**: Toggles to either expand or collapse the selected building icon.

### Access room topology maps

A room represents a small-scale data center. You can add one or more rooms to data centers or directly to data center topology maps. Room topology maps serve as containers for the wiring
cabinets that house managed devices. You can add one or more racks or cabinets to room topology maps.

To access a room topology map:
1. Click the **Resource** tab from the tabular navigation system on the top.
2. Click **View Management** on the navigation tree on the left.
3. Click **Network Topology** under **View Management** from the navigation system on the left.
   A new browser instance opens and an icon labeled **Custom Topology** displays in the main pane of the page. A navigation system displays on the left.
4. Double click **Data Center Topology** under **Topology**.
   A new page for the **Data Center Topology** displays in the main pane. Multiple pages in the main pane can be navigated using the tabs located at the top of the main pane.
5. To access a room, do one of the following:
   - Double click a room icon from a data center map, or
   - Right-click the room icon and select **Open** from the shortcut menu.
   A new page for the room map displays in the main pane.
6. Use the tabs located at the top of the page to navigate between topology maps.
   A toolbar is located to the left of the room topology map, including the zoom in and zoom out tools and the **Edit Room** icon.
7. Click the **Edit Room** icon to enter the object library.
   You can edit and add the objects as needed, and save frequently used objects in an object template, which allows you to quickly add those objects to the room topology maps.

The room topology map also has right mouse click menu for configuring the room map. Menu options for the room map are:
- **Reload**: Refreshes the page after you have made changes to it. Once you have added a room to the map, click **Reload** to view and access the new rooms.
- **Modify**: Enables you to modify basic information about the room topology map, including the name, rows, columns, colors, floor grid stroke and floor deep.
- **Object Template**: Enables you to manage object template.

**Access wiring cabinet**

Wiring cabinet or rack topology maps contain graphical representations of the managed network devices. In rack topology maps you can add one or more devices, cabinet supports, and objects to the selected wiring cabinet.

To access a wiring cabinet map:
1. Click the **Resource** tab from the tabular navigation system on the top.
2. Click **View Management** on the navigation tree on the left.
3. Click **Network Topology** under **View Management** from the navigation system on the left.
A new browser instance opens and an icon labeled Custom Topology displays in the main pane of the page. A navigation system displays on the left.

4. Double click **Data Center Topology** under **Topology**.
   
   A new page for the Data Center Topology displays in the main pane. Multiple pages in the main pane can be navigated using the tabs located at the top of the main pane.

5. To access a wiring cabinet, do one of the following:
   - Double click the room icon that contains the wiring cabinet icon you want to access, or
   - Right-click the room icon and select **Open** from the shortcut menu.

   A new page for the room map displays in the main pane.

6. Use the tabs located at the top of the page to navigate between topology maps:
   - Double click the cabinet icon you want to access, or
   - Right-click the wiring cabinet icon and select **Open** from the shortcut menu.

   A new page for the wiring cabinet map displays in the main pane.

7. Use the tabs located at the top of the page to navigate between topology maps.

The rack topology map also has right mouse click menu for configuring the map. Menu options for the map are:

- **Reload**: Refreshes the page after you have made changes to it. Once you have added a device to the wiring topology map, click **Reload** to view your changes.

- **Add Device to Cabinet**: Add a new device to the wiring cabinet. You can add devices using either the **By View** or the **Advanced** query. Method. See "Adding devices by View" (page 85) and "Adding devices by Advanced query" (page 85).

8. Click **OK**.

9. Right-click the rack and select **Reload** from the shortcut menu to update the map:
   - **Add Supports**: Add a new supports to the wiring cabinet.
   - **Add Object**: Adds a new object to the wiring cabinet.
     a. From the **Add Object** dialog box, enter the dimensions of the object.
     b. Click **OK**.
   - c. Select **Reload** from the right mouse click menu to update the map.
     - **Rename**: Enables you to rename the rack.
     - **Zoom**: Enables you to zoom in or out of the topology view or to fit the contents of the topology map into the current window.

Automatically building data center topology maps

You can create nested maps up to four layers, which display the physical layout of the data centers in the organization and have the cabinets automatically populated with the devices managed by IMC.

To automatically build Data Center Topology maps:
1. Click the **Resource** tab from the tabular navigation system on the top.
2. Click **View Management** on the navigation tree on the left.
3. Click **Network Topology** under **View Management** from the navigation system on the left.
A new browser instance opens and an icon labeled **Custom Topology** displays in the main pane of the page. A navigation system displays on the left.

4. Double click **Data Center Topology** under **Topology**.
   A new page for the **Data Center Topology** displays in the main pane. Multiple pages in the main pane can be navigated using the tabs located at the top of the main pane.

5. Click the icon in the topology map toolbar.
   The **Automatically Build a Data Center Topology** dialog box appears. The dialog box includes an **Automatically Build a Data Center Topology** list:
   - **Device Label**: Contains the device name in IMC. By default, the device name is the sysName of the device in IMC.
   - **IP Address**: Contains the IP address of the device.
   - **Height (U)**: Contains the height of the device, in units.
   - **Data Center**: Contains the data center where the device is located.
   - **Layer**: Contains the layer where the device is located in the data center. A data center can contain up to five layers.
   - **Room**: Contains the room where the device is located.
   - **Cabinet**: Contains the cabinet where the device is installed.

6. Click the **Select Devices** button located at the up right of the dialog box.
   The **Select Devices** dialog box appears. You can add devices using either the **By View** or the **Advanced** query method. See "Adding devices by View" (page 85) and "Adding devices by Advanced query" (page 85).

7. Click the **Height (U)** field for the associated device to modify the device height.
   The total height of all devices cannot exceed the capability of the cabinet.

8. Click the **Data Center** field for the associated device to configure the data center where the device is located.

9. Do one of the following:
   - If the data center already exists, click the button located at the right of the **Data Center** field to select the data center name from the list, or
   - If the data center does not exist, enter the data center name in the **Data Center** field. The data center is automatically created when the data center topology map is automatically built.

10. Click the **Layer** field for the associated device to configure the layer where the device is located.

11. Select the layer where the device is located.

12. Click the **Room** field for the associated device to configure the room where the device is located.

13. Do one of the following:
   - If the room already exists, click the button located at the right of the **Room** field to select the room from the list, or
   - If the room does not exist, enter the room name in the **Room** field. The room is automatically created when the data center topology map is automatically built.
14. Click the Cabinet field for the associated device to configure the cabinet or rack where the device is installed.

15. Do one of the following:
   - If the cabinet already exists, click the button located at the right of the Cabinet field to select the cabinet from the list, or
   - If the cabinet does not exist, enter the cabinet name in the Cabinet field. The cabinet is automatically created when the data center topology map is automatically built.

16. Click OK.
   The data center topology map is automatically built and the cabinets are automatically populated with devices.

Managing devices from the data center topology maps

The network topology maps also enable you to manage devices directly from the topology view. From the topology devices, you can view and perform management functions including viewing device information and performing actions such as ping, trace route and initiating Telnet or SSH sessions to the selected devices. To manage devices from the Data Center Topology map:

1. Click the Resource tab from the tabular navigation system on the top.

2. Click View Management on the navigation tree on the left.

3. Click Network Topology under View Management from the navigation system on the left.

4. Double click Data Center Topology under Topology.
   A new page for the Data Center Topology displays in the main pane. Multiple pages in the main pane can be navigated using the tabs located at the top of the main pane.

5. To access a wiring cabinet, do one of the following:
   - Double click the room icon that contains the wiring cabinet icon you want to access, or
   - Right-click the room icon and select Open from the shortcut menu.
   A new page for the room map displays in the main pane.

6. Use the tabs located at the top of the page to navigate between topology maps.

7. Do one of the following:
   - Double click the cabinet icon you want to access, or
   - Right-click the wiring cabinet icon and select Open from the shortcut menu.
   A new page for the wiring cabinet map displays in the main pane.

8. Use the tabs located at the top of the page to navigate between topology maps.

9. Select the device that you want to manage by clicking on it.

10. Right-click the device you have selected.
    The management menu appears. Menu options are:
    - **Configuration**: Enables you to configure the device specifications for the rack topology map. Enter the device dimensions in the Configuration dialog box.
    - **Delete**: Enables you to delete the selected device from the wiring cabinet.
    - **Topology Location**: Provides you with a list of other maps that the selected device can be found on.
11. To access the device on another map or view, click the **Owner** entry in the **Find Result** table for the associated device.

A new tab in the current browser opens and the view with the selected device appears.

- **Open Web-Based NMS**: Allows you to launch the **Web Manager** interface for the selected device directly from the topology map. Selecting this option opens the **Web Manager** in a new browser instance that can be accessed via the tabs located at the top of the main pane. From this window, you can manage more fully the selected device. For more information on the **Web Manager**, see "Open web manager" (page 218).

- **Open Device Panel**: Allows you to launch the **Device Panel** interface for the selected device directly from the topology map. Selecting this option opens the **Device Panel** in a new pane in the topology window that can be accessed via the tabs located at the top of the main pane, allowing you to more fully manage the selected device. For more information on the **Device Panel**, see “Open device panel” (page 221).

- **Device Information**: Opens the **Device Details** page for the selected device. The **Device Details** page loads in the browser instance that originally launched the topology maps, not in the browser instance that has the topology maps loaded. For more information on the **Device Details** page, see "Managing one device via device details" (page 212).

- **Tools-Ping**: Enables you to launch a ping request from the IMC server to the selected device from the topology map. IMC opens a new browser instance can be accessed via the tabs located at the top of the main pane.

- **Tools-Telnet**: Enables you to launch a telnet session for the selected device directly from the topology map. You are prompted for the application on the local computer that supports telnet.

- **Tools-Traceroute**: Enables you to launch a traceroute request from the IMC server to the selected device from the topology map. IMC opens a new browser instance that can be accessed via the tabs located at the top of the main pane.

- **Tools-SSH**: Enables you to launch an SSH session for the selected device directly from the topology map. You are prompted for the application on the local computer that supports SSH.

**Managing stack devices with the stack topology**

The stack topology enables you to manage stack devices directly from the topology view, by allowing you to view the stack members, link status among stack members, and link status among stack members and external devices, and delete invalid stack members.

To view stack devices from the stack topology:

1. Click the **Resource** tab from the tabular navigation system on the top.

2. Click **View Management** on the navigation tree on the left.

3. Click **Network Topology** under **View Management** from the navigation system on the left.

4. Double click any custom topology under **Custom Topology** or IP topology under **IP Topology**.

   A new page for the **Custom Topology** or **IP Topology** displays in the main pane. Multiple pages in the main pane can be navigated using the tabs located at the top of the main pane.

5. To access the stack topology, do one of the following:
Right-click the stack device icon and select Open Stack Topology from the shortcut menu, or

Double click the stack device icon.

A new page for the stack topology displays in the main pane.

6. Use the tabs located at the top of the page to navigate between topology maps.

7. Select the tab located at the top of the page for the stack topology you want to display.

The stack device icon expands as a rectangle. From this rectangle you can view the internal structure of the stack.

The device marked with the icon is the master device of the stack, and the other devices are all subordinate devices. The links among the stack members show the internal structure of the stack. The links among the stack members and external devices show how the stack is connected to external devices.

8. Double click the rectangle to collapse the stack device to a stack device icon.

9. Click a rectangle, stack member, or stack link.

The stack topology displays information about the selected stack device, stack member, or stack link.

For the stack device, the left mouse click includes the following:

- **Device label**: Contains the IMC name for the stack device, which, by default, is the name assigned to it by IMC in its device configuration. If the stack device is configured with a systemName, IMC uses this as the Device Label unless a Device Label has been manually configured. The stack device label serves as an active link for drilling down into the Device Details page, which offers you convenient access to device management features.
- **IP Address**: Contains the management IP address of the stack device.
- **Mask**: Contains the mask of the management IP address.
- **Device Status**: Contains the most current status of the stack device. Status is determined by the highest severity or alarm level for the stack device, when a stack device has more than one current alarm that has not been cleared or recovered.
- **Sysname**: Contains the name that is configured on the stack device.
- **Vendor**: Contains the stack device vendor’s name.

For the stack member and stack link, the left mouse click includes the following:

- **Device label**: Contains the device label of the stack member.
- **Stack Member ID**: Contains the stack member ID.
- **Stack Member Role**: Contains the role of the stack member, which can be Master or Slave.
- **Link Name**: Contains the name for the stack link.
- **Line Type**: Contains information about the stack link type.
- **Left Node**: Contains the device label for the stack member device that is located on the left of the link as represented in the stack topology map.
- **Left Physical Interface**: Contains the physical interface name for the device that connects on the left in the stack topology map.
- **Left Logical Interface**: Contains the logical interface name for the device that connects on the left in the stack topology map.
o **Right Node**: Contains the device label for the stack member device that is located on the right of the link as represented in the stack topology map.

o **Right Physical Interface**: Contains the physical interface name for the device that connects on the right in the stack topology map.

o **Right Logical Interface**: Contains the logical interface name for the device that connects on the right in the stack topology map.

o **Link Speed**: Contains the speed of the stack link in bits per second.

**Deleting invalid stack members from the stack topology**

To delete invalid stack members from the stack topology:

1. Click the **Resource** tab from the tabular navigation system on the top.
2. Click **View Management** on the navigation tree on the left.
3. Click **Network Topology** under **View Management** from the navigation system on the left.
4. Double click either **Custom Topology** or **IP Topology** under **Topology**.
   A new page for the **Custom Topology** or **IP Topology** displays in the main pane. Multiple pages in the main pane can be navigated using the tabs located at the top of the main pane.
5. To access the stack topology, do one of the following:
   - Right-click the stack device icon and select **Open Stack Topology** from the shortcut menu, or
   - Double click the stack device icon.
   A new page for the stack topology displays in the main pane.
6. Use the tabs located at the top of the page to navigate between topology maps.
7. Select the tab located at the top of the page for the stack topology you want to display.
   The stack device icon expands as a rectangle. From this rectangle you can view the internal topology of the stack device. A device marked with the icon is an invalid stack member.
8. To delete an invalid stack member, right-click the invalid stack member in the stack topology map and select **Delete Stack Member** from the shortcut menu.
9. Click **OK**.

**Viewing traffic with traffic topology**

The traffic topology enables you to view the traffic conditions of links of the specified type in the custom topology.

To view the traffic from the traffic topology:

1. Click the **Resource** tab from the tabular navigation system on the top.
2. Click **View Management** on the navigation tree on the left.
3. Click **Network Topology** under **View Management** from the navigation system on the left.
4. Double click any custom topology under **Custom Topology**.
   A new page for the **Custom Topology** displays in the main pane. Multiple pages in the main pane can be navigated using the tabs located at the top of the main pane.
5. Click the icon. The following menus appear:
   - **Traffic Topology Index**: Allows you to decide which index will denote the traffic of the link on a topology map.
   - **Link Type of Traffic Topology**: Allows you to decide which type of the link displays the traffic on a topology map. Options include All links, Core links, Links to servers, and Link to PCs. Core links refer to links connecting network devices. Links to servers refer to links connecting network devices to servers. Links to PCs refer to links connecting network devices to PCs.
   - **Show**: Identifies the link traffic load status by color. This option is available when No Index is not selected for Traffic Topology Index. The Show feature provides the Traffic Labels and Traffic load options.
   - **Traffic labels**: Displays the values of the indexes selected in Traffic Topology Index over links, and displays the values in different background colors according to the level-1 and level-2 thresholds set in the global indexes. If the traffic over a link is normal, the background color of the index values is the same as the background color of the traffic topology.
   - **Traffic load**: Displays links in different colors according to their traffic load conditions. The system has pre-defined traffic ranges for each index in the Traffic Topology Index. After you select an index in the Traffic Topology Index, the topology displays the links in different colors according to the traffic ranges of these links.

6. Customize the traffic range thresholds and their corresponding colors in the Traffic load parameters.

7. Add a file `userDefined.xml` in directory:
   ```plaintext
   IMC\client\conf\perf\trafficTop
   ```
   a. Configure the traffic range thresholds and their corresponding colors in the file `userDefined.xml`.

   For example, task id=1 corresponds to the index Interface Transmitting Rate. By setting the min and max parameters for the region parameter and setting rgb-r, rgb-g, and rgb-b values for the color_value parameter, you can set different colors for different threshold ranges.

   For more information, see the system-defined configuration file `systemDefined.xml`. IMC preferentially uses the configurations in the file `userDefined.xml`. At the same time, do not modify the configurations in the system-defined configuration file `systemDefined.xml`.

   The traffic topology feature applies only to the current topology.

   If you enable the traffic topology, the message box located at the bottom of the current topology will prompt you to start to monitor traffic on topology links.

**Viewing the virtual network with VNM topology maps**

You can view the virtual network with VNM topology maps. Options for VNM topology maps include displaying or hiding the storage devices, and viewing the physical servers managed by a specific vManager.

To display/hide the storage devices:
1. Click the Resource tab from the tabular navigation system on the top.
2. Click View Management on the navigation tree on the left.
3. Click **Network Topology** under **View Management** from the navigation system on the left.

4. Double click **VNM Topology** under **Topology**.
   A new page for the **VNM Topology** displays in the main pane. Multiple pages in the main pane can be navigated using the tabs located at the top of the main pane.

5. Right click with nothing selected on the VNM topology to display a menu containing the **Display/Hide Storage Devices** option.

6. Select this option, to display or hide the storage devices.

**Viewing the physical servers managed by a specific vManager**

You can select a vManager and view the physical servers it manages. When you use this feature, the physical servers managed by the vManager you select are highlighted, whereas all physical servers managed by other vManager are grayed out.

To view the physical servers managed by a specific vManager:

1. Click the **Resource** tab from the tabular navigation system on the top.

2. Click **View Management** on the navigation tree on the left.

3. Click **Network Topology** under **View Management** from the navigation system on the left.

4. Double click **VNM Topology** under **Topology**.
   A new page for the **VNM Topology** displays in the main pane. Multiple pages in the main pane can be navigated using the tabs located at the top of the main pane.

5. Click the **vManager Topology** icon and select the vManager you want to view in the popup menu.
   The vManagers are sorted by IP address and device label.

6. Click the **vManager Topology** icon and select the **Exit** option in the popup menu to cancel viewing the physical servers.

**Viewing devices with custom views**

Custom views offer you the ability to create their own views based on groups of devices they define. Like all IMC views, custom views offer you a real time snapshot of the status of devices in the network infrastructure through color-coded icons that match the highest severity or alarm level for devices in the view.

Unlike Device, IP, or custom views enable you to grant and revoke management rights for devices in custom views. First, you create custom views and add devices to them. Then, you grants access to the custom groups in the individual operator accounts.

When considering how to organize devices into custom groups and subviews, consider first the rights and privileges you want to grant to or restrict you from. Also, consider how the logical grouping of devices can support an effect rights management policy. For more information on the relationship of custom views and operator rights, see "Operator management: managing secure access to IMC" (page 103).

You can organize one or more views according to the IMC security needs and viewing requirements of their organization. Custom views can be organized by geography, or location, buildings, organizational groupings, just to name a few. Devices can belong to more than one custom view.
As all IMC views do, custom views offer drilldown to the device details for an individual device. From the Device Details page, you can access management features that offer you quick and easy access to network resources as well as the ability to manage them.

Accessing Custom Views

To access custom views

1. Navigate to Resource→Custom View.
   a. Click the Resource tab from the tabular navigation system on the top.
   b. Click View Management on the navigation tree on the left.
   c. Click Custom View on the navigation tree on the left. The list of custom views is displayed in the Custom View List. This list is empty if no custom views have been created.

2. Click the view name you want to access. The Device List/Topology for the custom view you choose appears.

Device List

- **Status**: Contains the most current status of the device. Device icons that are gray are not managed.
- **Device List**: Contains the name of a device in the view. The contents of this field serve as an active link for drilling down into the Device Details page, which offers you convenient access to device management features.
- **Category**: Contains the IMC device category for the associated device.
- **Model**: Contains device model information. If the device is managed for reachability using ICMP only no device model information is available and the field contains “ICMP.”
- **IP Address**: Contains the IP address of the device.
- **Interface List**: Contains a link to the list of interfaces for the selected device. This list provides access to the Interface Details page for each interface.
- **Operation**: Contains an icon 🚀 that displays links to operational tasks for the associated device.

You can sort the Device List by the Status, Device List, Category, Model, or IP Address fields by clicking the column label to sort the list by the selected field. The column label is a toggle switch that allows you to toggle between the various sort options specific to each field.

If the Device List contains multiple entries, following navigational aids may appear:

- Click ⏷️ to page forward in the Device List.
- Click ⏴️ to page forward to the end of the Device List.
- Click ⏪️ to page backward in the Device List.
- Click ⏬️ to page backward to the front of the Device List.

3. Click 8, 15, 50, 100, or 200 from the right side of the main pane to configure how many items per page you want to view.

You can only view the custom views and devices to which they have been granted management access.
The color of a device icon represents the severity or alarm level for the most severe alarm condition for that device.

IMC enables you to manage multiple devices via the custom view, including deleting, synchronizing, managing and unmanaging devices. For information on managing multiple devices through these views, see "Managing multiple devices from the device list" (page 299).

**Topology**

A topology map of the custom view is located on the **Topology** tab, from which you can view the network diagram and perform certain operations on the topology map of the custom view. For more information on operating the topology map, see "Viewing devices via the Network Topology" (page 181).

**Managing custom views**

Custom views offer administrators the ability to create views based on groups of devices you define. Unlike other IMC device views, custom views enable you to grant and revoke management rights to operators based on custom views. First, you must create the custom views, add devices to them, and then grant access to the custom groups in the individual operator accounts.

It is important to also consider the rights and privileges you want to grant or restrict to you and how the logical grouping of devices can support an effective rights management policy. For more information on the relationship of custom views and operator rights, see "Operator management: managing secure access to IMC" (page 103).

You can create one or more custom views based on the IMC security needs and viewing requirements of their organization.

**Creating custom views**

To create a custom view:

1. Navigate to **Resource → Custom View**.
   a. Click the **Resource** tab from the tabular navigation system on the top.
   b. Click **Custom View** on the navigation tree on the left. The list of custom views is displayed in the **Custom View List**. This list is empty if no custom views have been created.

2. Click **Add**.

3. Enter the name for the custom view you want to add in the **View Name** field.

4. Click the link to the right of the **Upper-Level View** field.
   The window for selecting a view appears.

5. Select an upper-level view for the new view, and click **OK**.
   The selected view appears at the right of the **Upper-Level View** field.

6. Select an option from the **Automatically Add New Devices** list.
   If you select the **From Network Segment** option, the following options appear:
   a. Enter the start IP address in the **Start IP** field.
   b. Enter the end IP address in the **End IP** field.
   c. Do one of the following:
− Click **Add** to add the network segment to the **Network Segment** field and the new devices on the network segment are automatically added to the view, or
− Click **Delete** to delete one or more IP address segments.

7. In the **Device List**, select whether to **Add all devices of the current system**.

8. If this option is selected, the **Device List** is hidden, all devices managed by IMC are added to the view, and you directly go to **Step 10**.

9. If the **Add all devices of the current system** option is not selected in **Step 5**, you can click **Add** in the **Device List** to select devices you want to add to the view.

10. Add devices using either **By View** or **Advanced** query option. See "Adding devices by View" (page 85) and "Adding devices by Advanced query" (page 85).

11. Click **OK** to create the custom view.

### Modifying Custom Views

To modify a custom view:

1. Navigate to **Resource**→**Custom View**.
   a. Click the **Resource** tab from the tabular navigation system on the top.
   b. Click **Custom View** on the navigation tree on the left. The list of custom views is displayed in the **Custom View List**.

2. Click the **Modify** icon associated with the custom view you want to modify.

3. Modify the name for the custom view in the **View Name** field.

4. Click the **link** to the right of the **Upper-Level View** field.
The window for selecting a view appears.

5. Select an upper-level view for the new view, and click **OK**.
The selected view appears at the right of the **Upper-Level View** field.

6. Reselect an option from the **Automatically Add New Devices** list.

7. If you select the **From Network Segment** option, the following options appear:
   a. Enter the start IP address in the **Start IP** field.
   b. Enter the end IP address in the **End IP** field.
   c. Do one of the following:
      − Click **Add** to add the network segment to the **Network Segment** field and the new devices on the network segment are automatically added to the view, or
      − Click **Delete** to delete one or more IP Address segments.

8. In the **Device List**, select whether to **Add all devices of the current system**.
   If this option is selected, the **Device List** is hidden, all devices managed by IMC are added to the view, and you directly go to **Step 10**.

9. If the **Add all devices of the current system** option is not selected in **Step 5**, you can click **Add** in the **Device List** to select devices you want to add to the view.

10. Add devices using either **By View** or **Advanced** query option. See "Adding devices by View" (page 85) and "Adding devices by Advanced query" (page 85).
11. Click OK to modify the custom view.

Deleting custom views
To delete a custom view:
1. Navigate to Resource→Custom View.
   a. Click the Resource tab from the tabular navigation system on the top.
   b. Click Custom View on the navigation tree on the left. The list of custom views is displayed in the Custom View List.
2. Click the Delete icon associated with the custom view you want to delete.
3. Click OK to confirm deletion of the custom view.

⚠️ WARNING:
All the devices in the view are removed from the deleted views but are deleted from IMC.

Adding Devices to Custom Views
Once you have created the custom views, you are ready to add devices.
To add devices to custom views:
1. Navigate to the Device List for a custom view.
   a. Click the Resource tab from the tabular navigation system on the top.
   b. Click Custom View on the navigation tree on the left.
   This displays the Custom View List in the main pane of the Custom View page.
2. To add devices to a Level 1 view, click the View Name link for the custom view you want to add devices to.
3. Click Add.
4. Add devices using either By View or Advanced query option. See "Adding devices by View" (page 85) and "Adding devices by Advanced query" (page 85).

Removing devices from custom views
To remove devices from custom views:
1. Navigate to the Device List for a custom view.
   a. Click the Resource tab from the tabular navigation system on the top.
   b. Click Custom View on the navigation tree on the left.
   c. This displays the Custom View List in the main pane of the Custom View page.
2. To remove devices from a view, click the View Name link for the custom view you want to delete devices from.
3. Click the Operation icon associated with the device you want to remove from the custom view.
4. Select Delete from the Operation menu to remove the device.
Removing a device removes it from the custom view but it does not remove or delete the device from IMC.
5. Do one of the following:
   - Confirm removal of the device from the custom view, or
   - Remove one or more devices from the Device List by clicking the checkboxes to the left of the devices you want to remove from the custom view and click Remove.

Now that you have created custom views and have added devices to them, the next step is to grant or restrict access to these views and the devices in them by configuring each operator account.

Operator accounts that are included in the Administrator Group have administrator privileges to all custom views. These privileges cannot be revoked. Therefore, to effectively use custom views to restrict access and management rights to devices in them, you must also configure the operators to have membership in an operator group that does not have ADMIN privileges. For more information on configuring operator groups and individual operator accounts, see “Operator management: managing secure access to IMC” (page 103).

**Viewing device interfaces with port groups**

IMC offers you a variety of options for viewing network resources and for drilling down into the features used to manage them. IMC provides you with the ability to manage port groups. To facilitate viewing interface status, administrators can group several concerned interfaces or important interfaces (such as the device interfaces that connect to a mail server, or core layer device interfaces) together as a port group.

The Port Group also offers drilldown capabilities to the device and interface details page. The Device Details page provides you with access to IMC’s network device management features. The Interface Details page provides you with access to IMC’s interface management features.

**Managing port groups**

The Port Group feature provides you with the ability to query, add, modify, and delete port groups and to grant and revoke management rights to operators. You can create one or more port groups based on the administrators’ jobs and port functions. In addition, port groups offer you the ability to drill down to port groups’ details.

**Querying port group list**

IMC enables you to filter port groups by a partial or complete port group name, by interface status, or by interface alias and then displays only those port groups that match the search or filter criteria.

To filter the Port Group List:

1. Navigate to Resource→Port Group List:
   a. Click the Resource tab from the tabular navigation system on the top.
   b. Click View Management on the navigation tree on the left.
   c. Click Port Group under View Management from the navigation system on the left. The Port Group List displays in the main pane of the Port Group List page.

   **Port group list**
   - **Expand/Collapse icon**: Contains the expand/collapse icon for the associated port group.

2. Click the icon to expand the associated port group to view the interface list.
3. Click icon to collapse the associated port group.
   o **Port Group Name**: Contains the port group name.
   o **Total Number**: Contains the number of the interfaces in the associated port group.
   o **Interface Status**: Contains the most current status statistic of the interfaces in the associated port group. The interface statuses include:
     - **Down**
     - **Up**
     - **Unknown**
     - **Blocked**
     - **Unmanaged**
   Each interface status icon is attached with the number of interfaces in the port group that are in that status.
   o **Created by**: Contains the name of the operator who created the associated port group.
   o **Actions**: Contains the Modify and Delete icons that link to modify and the delete port group. For more information on modifying and deleting port groups, see "Modifying a port" (page 209) and "Deleting a port group" (page 210).
   o **Description**: Contains the description for the associated port group.

4. Move the pointer over **Query Groups** at the upper right corner of the **Port Group List**, and a search criteria dialog box appears.
   a. Enter the following search criteria in the dialog box:
      - **Group Name**: Enter the port group name you want to search for. Select Fuzzy from the list located to the right of the **Group Name** if you want to enter a partial IP address. Select Exact from this list if you want IMC to search for an exact match for the port group name you have entered.
      - **Created by**: Enter the name of the operator who created the port group for which you want to search. IMC supports fuzzy matching for this field, allowing you to enter a partial or complete string for the operator name.
      - **Interface Status**: Select the status of the interfaces in the port group you want to search for from the **Interface Status** list.
      - **Interface Description**: Enter the description of the port group you want to search for in the **Interface Description** field. IMC supports fuzzy matching for this field, allowing you to enter a partial or complete string for the interface description.
      - **Interface Alias**: Enter the interface alias that is contained in the port group you want to search for in the **Interface Alias** field. IMC supports fuzzy matching for this field, allowing you to enter a partial or complete name for the interface alias.
   b. Click **Query**.

The results display in the main pane of the **Port Group List** page.

**Viewing the interface list of a port group**

To view the interface list of a port group:

1. Navigate to Resource→Port Group List:
a. Click the Resource tab from the tabular navigation system on the top.

b. Click View Management on the navigation tree on the left.

c. Click Port Group under View Management from the navigation system on the left.

The Port Group List displays in the main pane of the Port Group List page.

2. Click the expand icon located to the left of the name of the port group for which you want to view the interface list.

The interface list of the port group appears.

Interface list of the port group

- **Interface Status**: Contains the most current status of the interfaces in the associated port group. The interface statuses:
  - ![x] Down
  - ![circle green] Up
  - ![circle orange] Unknown
  - ![circle red] Blocked
  - ![circle blue] Unmanaged

- **Interface**: Contains the interface name, which serves as a link for navigating to the Interface Details page. For more information on the Interface Details page, see "Interface details page" (page 269).

- **Interface Index**: Contains a unique index of the associated interface.

- **Interface Type**: Contains the type of the associated interface.

- **Device Label**: Contains the name of the device where the interface is located, serving as a link for navigating to the Device Details page. For more information on the Device Details page, see "Managing one device via device details" (page 212).

- **Interface IP**: Contains the IP address of the associated interface.

- **Mac Address**: Contains the MAC address of the associated interface.

- **Speed (bps)**: Contains the speed of the associated interface, in bits per second.

- **Rx (bps)**: Contains the average receive rate of the day on the associated interface, in bits per second.

- **Tx (bps)**: Contains the average transmit rate of the day on the associated interface, in bits per second.

- **Rx Util (%)**: Contains the average receive bandwidth usage of the day on the associated interface, in percent.

- **Tx Util (%)**: Contains the average transmit bandwidth usage of the day on the associated interface, in percent.

- **Rx Dis (%)**: Contains the average inbound packet loss rate of the day on the associated interface, in percent.

- **Tx Dis (%)**: Contains the average outbound packet loss rate of the day on the associated interface, in percent.

You can sort the interface list by the **Interface Status**, **Interface**, **Interface Type**, **Device Label**, **Interface IP**, **Mac Address**, and **Speed (bps)** fields by clicking the column label to sort the list by
the selected field. The column label is a toggle switch that allows you to toggle between the various sort options specific to each field.

**Customizing Columns for the Interface List**

To customize columns for the interface list:

1. Click the **Customize Columns** link located in the upper right corner of the Port Group List, the **Customize Columns** dialog box appears.
2. Click the checkbox to the left of the **Columns Name** you want to display.
3. Click **OK**.

You cannot hide the following columns of the interface list: **Interface Status**, **Interface**, and **Device Label**.

4. Select the filter from the **Filter** list located in the upper left corner of the interface list to filter the interface list. The interface refreshes to display the interfaces that match the filter conditions.

**Adding a port**

To add a port group:

1. **Navigate to Resource→Port Group List:**
   a. Click the **Resource** tab from the tabular navigation system on the top.
   b. Click **View Management** on the navigation tree on the left.
   c. Click **Port Group** under **View Management** from the navigation system on the left.
   
   The Port Group List displays in the main pane of the Port Group List page.
2. Click **Add** to add a port group.

   The Add Port Group page appears.
3. Enter the port group name in the **Group Name** field.
4. Select the operator groups to access to the port group.
5. Click the checkbox to the left of the operator group name you want to select.
6. Enter a description for this port group in the **Description** field.
7. Click **Add** to select interfaces you want to add to the port group.
   
   The Select Interfaces dialog box appears.
8. Add interfaces using either the **View** or **Advanced** query option. Adding interfaces uses the same process as adding devices. See "Adding devices by View" (page 85) and "Adding devices by Advanced query" (page 85).
9. Click **OK** to create a port group.

**Modifying a port**

To modify a port group:

1. **Navigate to Resource→Port Group List.**
   a. Click the **Resource** tab from the tabular navigation system on the top.
   b. Click **View Management** on the navigation tree on the left.
   c. Click **Port Group** under **View Management** from the navigation system on the left.
   
   The Port Group List displays in the main pane of the Port Group List page.
2. Click **Modify** icon located at the right of the **Action** field for the port group you want to modify.
   The **Modify Port Group** page appears.
3. Modify the port group name in the **Group Name** field.
4. Do one of the following:
   o To change access to this port group, click the checkboxes to the left of the operator groups you want to grant access to, or
   o To remove operator groups, click the checked boxes to the left of the operator groups you want to revoke access for.
5. Modify the description for this port group in the **Description** field.
6. Click **Add** to select the device interfaces to a port group.
7. The **Select Interfaces** dialog box appears.
8. Add interfaces using either the **View** or **Advanced** query option. Adding interfaces uses the same process as adding devices. See "Adding devices by View" (page 85) and "Adding devices by Advanced query" (page 85).
9. Do one of the following;
   o To delete the selected interfaces from a port group lick **x** icon in the delete field of the **Select Interfaces** list, or
   o To delete all interfaces from a port group, click **Remove All** button in the upper of the **Select Interfaces** list.
10. Click **OK** to accept you change to this port group.

**Deleting a port group**

To delete a port group

1. Navigate to **Resource→Port Group List**.
   a. Click the **Resource** tab from the tabular navigation system on the top.
   b. Click **View Management** on the navigation tree on the left.
   c. Click **Port Group** under **View Management** from the navigation system on the left.
      The **Port Group List** displays in the main pane of the **Port Group List** page.
2. Click **Delete** icon located at the right of the **Action** field for the port group you want to delete.
3. Click **OK** to confirm the deletion of the port group.
   Deleting a port group does not remove the interfaces of this port group from IMC.

**Searching for devices in IMC**

You can use the **Basic** or the **Advanced** query feature to locate devices in IMC.
Searching for a device using the basic search feature

To perform a basic device search:

1. To search for a device, select the Query Devices icon , located in the upper right corner of most IMC pages to the left of the Advanced query link.
2. Enter your search criterion.
3. Click Go.

Searching for a device using the advanced search feature

To perform a search using the Advanced link

1. Navigate to Advanced Query.
   a. Click the Advanced link located in the upper right corner of the IMC page.
2. Click the radio button to the left of Query Devices to perform a device search.
3. Enter one or more of the following search criteria in the Advanced Query dialog box:
   a. Device Label: Enter the device name in the Device Label field.
   b. Device IP: Enter a partial or complete IP address for the device you want to search for in the Device IP field.
4. Do one of the following:
   a. Select Fuzzy from the list located to the right of the Device IP address if your IP address search criterion is not exact, or
   b. Select Exact from this list if you want IMC to search for an exact match for the IP address you have entered.
5. Continue making selections in the following fields:
   a. MAC: Enter the MAC address of the device you want to search for in the MAC field.
   b. Bridge MAC: Enter the MAC address for the bridge device that you want to query for in the Bridge Mac field.
   c. Device Category: Select the device category from the Device Category list.
   d. Device Status: Select the device status from the Device Status list.
   e. Device Series: Select the device series from the Device Series list.
   f. Contact: Enter the contact information for the devices you want to search for.
   g. Location: Enter the location of the device you want to search for in the Location field.
   h. Device Reachability: Select the reachability status of the device from the Device Reachability list.
6. Click Query.
Managing one device via device details

IMC offers you a rich set of monitoring and management features for network devices. You have the option to manage one device at a time or multiple devices. IMC’s feature set for managing one device includes the ability to synchronize and refresh views, manage, unmanage, and delete devices from IMC, launch Telnet, SSH, Device Panel and Web Manager sessions for the selected device, perform ping and Traceroute tests.

You can also configure the selected device from the Device Details page including configuring the device label, system group attributes, IMC’s SNMP, SSH, and Telnet settings for the selected device, modifying status and configuration polling intervals, ping parameters and ACL settings.

In addition, you can both monitor and manage switches for PoE, RMON, VLAN and Spanning Tree configurations. You can configure and view performance information for a selected device as well as launch configuration management functions including backing up device configurations. You can also view protocol management information for OSPF, IGMP, and IPv6.

All of these options are available through the Device Details page of a selected device.

Accessing the device details page

There are many ways to access the Device Details page, the most common of which is through the Device List. The Device List is displayed in each of the following views – Device View, IP View, and the Custom View. The Device Label column in the Device List contains a link that navigates you to the Device Details page for the selected device. For information on accessing the Device List displayed in these views, see “Viewing devices with Device, IP, and Topology Views” (page 176) and “Viewing devices with custom views” (page 201).

In addition, the Device Details page can be accessed by using a right mouse click on a selected device in the Network Topology. For information on viewing Device Details from the Network Topology view, see “Viewing devices via the Network Topology” (page 181).

Navigation instructions for accessing the Device Details page from the Device View for all devices are provided below.

1. Navigate to Resource→Devices View:
   a. Click the Resource tab from the tabular navigation system on the top.
   b. Click View Management on the navigation tree on the left.
   c. Click Device View under View Management from the navigation system on the left.

   The Device List – All displays all devices in IMC.

2. Locate the device you want to view the details for.

3. Click the link in the Device Label column in the Device List for the device.

   The Device Details page appears.

Device details page

The Device Details page has features and resources that provide you with quick and easy access to important device information as well as links to device configuration options.

The Device Details section of the Device Details page presents basic device information as well as several options for device configuration.
Device details section contents & configuration options

- **Device Label**: Contains the IMC name for the device. By default, IMC uses the system name or sysName of the device if it has been configured.

4. To modify the device label, click the Modify link located to the right of the Device Label field.
5. Delete the existing Device Label value and enter the new device label.
6. Click OK.

Modifying the device label changes IMC's name or label for the device in IMC only. It does not change the name of the device on the device itself.

- **Device Status**: Contains the most current status for the device. Status is determined by the highest severity or alarm level for the device, when a device has more than one current alarm that has not been cleared or recovered. Device icons with the color gray denote that the device is unmanaged.

- **IP Address**: Contains the IP address of the device.
- **Mask**: Contains the IP address subnet mask for the associated device.
- **sysOID**: Contains the system Object ID for this device.
- **Device Model**: Contains information on the model of the device.
- **Device Category**: Contains IMC's category of the device.

7. To modify the Device Category, click the Modify link located to the right of the Device Category field.
8. Reselect a device category.
9. Click OK.

- **System Name**: Contains the name of the device as configured on the device.

10. To modify the System Name, click the Modify link located to the right of the System Name field.
11. Delete the existing system name value and enter the new system name.
12. Click OK.

- **Contact**: Contains contact information for this device.

13. To modify the contact information, click the Modify link located to the right of the Contact field.
14. Delete the existing contact information and enter the new contact information.
15. Click OK.

- **Location**: Contains the location of the device.

16. To modify the location information, Click the Modify link located to the right of the Location field.
17. Delete the existing Location value and enter the new location.
18. Click OK.
- **Runtime**: Contains the SysUpTime or system up time for this device.
- **Last Poll**: Contains the date and time stamp for IMC’s last status poll for the associated device.
- **Login Type**: Contains the access method for the device.

19. To modify the login type, click on the **Modify** link located to the right of the **Login Type** field.
20. Select the new login type or access method from the **Login Type** list. The device must also be configured to support this login type.
21. Click **OK**.

- **Interfaces**: This field contains the number of interfaces and a link that displays a list of all interfaces on the device. This list includes interface status as well as a link to view and take action on specific interfaces. For more information on the **Interface Details** page, see "Interface details" (page 268). This list contains all of the fields displayed, including those fields that IMC is unable to gather information for. In these cases, the field is blank or contains the value "unknown."

- **System Description**: Contains the system description as defined by the vendor.

**Service monitoring**

From the **Device Details** page, you can configure IMC to perform TCP and UDP port checks to validate that a service on the selected device is listening and responding to queries on that port. This form of monitoring validates basic service availability. By default, Telnet, FTP, SMTP, DNS, HTTP, and TFTP are configured but not enabled at installation. In addition to these standard service monitors, user defined service monitors can be added. Once configured, you can view real time status of services running on a selected device, also from the **Device Details** page.

You configure service monitors from the **Device Details** page of a selected device. In addition, IMC displays the results of this service monitoring in the **Service Monitoring** tab found in the lower portion of the **Device Details** page.

**Viewing monitored services**

To view real time service monitoring for an individual device navigate to the **Device Details** page for the selected device:

1. From the **Device Details** page, click the **Service Monitoring** tab located below the **Device Details** section.

2. To view all of the monitored services, click the **Monitoring Service** link located just below the **Service Monitoring** tab.

   IMC displays all service monitoring entries in a table located under the **Service Monitoring** tab.

**Monitoring service list fields and explanations**

- **Service Name**: Contains the name of the service being monitored.
- **Service Port**: Contains the TCP or UDP port number that is being monitored.
- **Service Type**: Identifies which IP transmission protocol is being monitored, TCP or UDP.
- **Service Status**: Contains the last known status of this service, based on IMC’s last poll. Status of a service can be running, stopped, or unknown.
Configuring monitored services

To configure IMC to perform service monitoring:

1. From the Device Details page, click on the Service Monitoring tab located below the Device Details section.

2. Click the Customize link located to the right of Monitoring Information.

3. Click the checkbox to the left of the Service Name you want to enable service monitoring for.

4. Do one of the following:
   - If you have selected a system defined service (Telnet, FTP, SMTP, DNS, HTTP, or TFTP), skip to Step 6, or
   - If you want to monitor a service that is not one of the system-defined services displayed in the Service Name field, click one of the checkboxes to the left of one of the fields that contains "CustomService_1-5", or
   - If you are monitoring a custom or user defined service, first delete the CustomService_# value in the field associated with the checkbox you checked in Step 3.

5. Enter the service name for the service you want to monitor.

6. Enter the TCP or UDP port number for the service that is being used by the monitored service on the selected device in the Service Port field.

7. Select the transmission protocol that is being used by this service on the managed device from the Service Type list.

8. Click OK.

It may take a few minutes for IMC to execute the service monitoring poll and update the Monitor Information field with the status of this service. Use your browser’s refresh or reload option to refresh the Service Monitoring table. The Service Port number and Service Type or transmission protocol must match what is configured on and being used by the service being monitored on the managed device.

Alarms

From the Device Details page, you can view the 10 most recent alarms that have not been cleared or recovered along with a graph that summarizes alarms that have not been cleared or recovered. The alarms list also provides you with drilldown capabilities to alarm details.

Scroll down to the section of the Device Details page titled Recent 10 unrecovered alarms to view the most recent unrecovered alarms from the Device Details page.

IMC displays the 10 most recent, unrecovered alarms in a table that contains the fields listed below.

- **Level**: Contains the current severity or alarm level status for the associated alarm.
- **Description**: Contains a description of the event or condition that is being alarmed on. The Description field contains a hyperlink for drilling down into the Alarm Details for the selected alarm. For more information on the Alarm Details page and actions that you can take from this page, see "Alarm actions in the alarm details page" (page 569).
- **Alarm At**: Contains the date and time stamp for the associated alarm.
1. For a view of all alarms for the selected device, click the **More** link located in the right corner of the table.

   The **All Alarms** table appears, filtered by the selected device’s IP address. For more information on the **All Alarms** page, see “Browsing all alarms” (page 580).

**Alarm summary graph**

The **Device Details** page also includes a graph that summarizes all alarms except the **Info** alarms for the selected device. This graph contains active links on the graph itself for drilling down into alarms by severity or alarm level.

**Performance monitor**

From the **Device Details** page, you can access the **Performance Monitor**. This feature provides you with a quick snapshot of the performance metrics for the selected device from which can view the most current performance statistics as well as generate historical reports for the same metrics.

Scroll down to the section of the **Device Details** page titled **Performance Monitor** to view the most recent performance metrics.

IMC displays performance metrics in a table that contains the fields listed below.

- **Monitor Index**: Contains the performance metric that the device is being monitored for.
- **Monitor Value**: Contains the most recent polled value for the performance metric.
- **Operation**: This field contains the **Start/Stop Monitor** option.

To view historical data for the performance monitors listed in the **Performance Monitor** table:

1. From the **Device Details** page, click the **Details** link located to the far right of the **Performance Monitor**.
   
   IMC displays reports for the current day for all performance metrics listed in the **Performance Monitor** table.

2. Use the scroll bar to view all displayed reports.

**Right navigation tree**

The **Device Details** page contains many options for configuring one device. The navigation tree located on the right side of the **Device Details** page contains configuration options for the selected device. The sections of the right navigation tree include **Action**, **Configure**, **Performance Monitor**, **Configuration Center**, **VLAN Management**, **Device Management**, **RMON Management**, and **Protocol Management**.

The right navigation tree is context sensitive and configuration options on this tree vary as the device type changes.

**Actions – For all devices**

The **Action** menu options enable you to apply management and configuration options to the selected device from the convenience of the navigation tree located on the right of the **Device Details** section, including the ability to synchronize and refresh the current **Device Details** page, to manage and unmanage the selected device, and delete the device from IMC.

In addition, you can establish a remote session with the selected device using Telnet or SSH from the **Device Details** page, launch the **Web Manager** or **Device Panel** for remote management of the selected device, and execute Ping and Traceroute tests from the IMC server to the selected device.
Synchronize

Synchronize allows you to update IMC views with current data for the selected device update the current page with any updated information. Information in the device details section of the page as well as changes to Telnet or SNMP parameters are updated.

To synchronize the selected device from the Device Details page:

1. Click the Synchronize link located under the Action section of the right navigation tree on the selected device’s Device Details page. For information on navigating to a device’s Device Details page, see “Viewing devices with Device, IP, and Topology Views” (page 176).
   The top of the Device Details page updates to reflect the initiation of the synchronization process.
2. Refresh this page using the Refresh option on the right navigation tree to view any updates to device data.
   To synchronize more than one device, see "Managing multiple devices from the device list" (page 299).

Refresh

Refresh allows you to reload the current Device Details page and capture any updates to the device details or other dynamic data found on this page. This feature is particularly useful when you use the Synchronize option to query the selected device for updated information.

To refresh the selected device from the Device Details page:

1. Click the Refresh link located under the Action section of right navigation tree on the selected device’s Device Details page. For information on navigating to a device’s Device Details page, see “Viewing devices with Device, IP, and Topology Views” (page 176).
2. To refresh more than one device, see "Managing multiple devices from the device list" (page 299).

Manage/Unmanage

The process of discovering devices in IMC is separate and distinct from the process of managing them. During discovery, IMC add all discovered devices to the IMC database. You should determine which devices should be actively managed. Managing devices means that IMC features for monitoring and managing the device are available for the managed device. Managed devices consume node licenses.

From the Action menu, you can manage or unmanage the selected device. The Manage/Unmanage link is a toggle switch between these two states. If the right navigation tree menu option displays the Manage option, this means that the device is currently unmanaged. Conversely, if the right navigation tree menu option displays the Unmanage option, this means that the device is currently managed.

To manage or unmanage the selected device from the Device Details page:

1. Click the Unmanage link located under the Action section of the right navigation tree on the selected device’s Device Details page to unmanage a device.
2. Click the Manage link located under the Action section of the right navigation tree on the selected device’s Device Details page to manage a device. For information on navigating to a device’s Device Details page, see "Viewing devices with Device, IP, and Topology Views" (page 176).

The top of the Device Details page updates to reflect the completion status of the Manage or Unmanage task.

3. Refresh this page using the Refresh option on the right navigation tree to view any updates to device data.

To manage or unmanage more than one device, see "Managing multiple devices from the device list" (page 299).

Delete

With the Delete option, you can permanently delete the selected device from IMC along with all associated data for this device. When you delete a device all associated data is purged from IMC immediately.

To delete the selected device from the Device Details page:

1. Click the Delete link located under the Action section of the selected device’s Device Details page. For information on navigating to a device’s Device Details page, see "Viewing devices with Device, IP, and Topology Views" (page 176).

2. Click OK to confirm deletion of the selected device.

To delete more than one device, see, "Managing multiple devices from the device list" (page 299).

⚠️ WARNING:

Once a device has been deleted, it cannot be restored. Proceed with caution.

Telnet

Operators can launch a Telnet session to the selected device from the Device Details page, offering them quick and centralized access to managed devices.

To telnet to the selected device from the Device Details page:

1. Click the Telnet link located under the Action section of the selected device’s Device Details page. For information on navigating to a device’s Device Details page, see "Viewing devices with Device, IP, and Topology Views" (page 176).

2. Follow your operating system instructions for loading the appropriate Telnet application to be used to establish a Telnet session with the selected device.

⚠️ WARNING:

To use this feature, you must have an operating system or application that supports Telnet on the computer you use to access IMC.

Open web manager
Operators can open a Web Manager session to manage the selected device from the **Device Details** page, providing you quick web access to managed devices.

To use Web Manager to access and manage the selected device from the **Device Details** page:

1. Click the **Open Web Manager** link located under the **Action** section of the right navigation tree on the selected device’s **Device Details** page.
   For information on navigating to a device’s **Device Details** page, see "Viewing devices with Device, IP, and Topology Views" (page 176).
   The **Web Manager** interface appears.
2. Enter your Web Manager User Name and Password.
3. Click **OK**.
   Web Service must be supported and enabled on the device for this feature to function properly.

**Ping**

Operators can execute a Ping test from the IMC server to the selected device from the **Device Details** page, providing them with the ability to test the reachability of a managed device from the IMC server.

To ping the selected device from the **Device Details** page:

1. Click the **Ping** link located under the **Action** section of the selected device’s **Device Details** page. For information on navigating to a device’s **Device Details** page, see "Viewing devices with Device, IP, and Topology Views" (page 176).
   The **Ping** dialog box appears.
2. Select the Ping packet size in bytes from the **Buffer Size** list.
3. Select the number of Ping packets you want IMC to send to the selected device from the **Number** list.
4. Click **OK** to accept your changes and begin the Ping test.
5. View the results of your Ping test in the **Ping** dialog box.
6. Click **OK** to close the Ping test dialog box.

**Traceroute**

You can perform a Traceroute from the IMC server to the selected device from the **Device Details** page, which provides you the ability test the reachability of a managed device from the IMC server and to troubleshoot if and where connectivity problems might be.

To perform a Traceroute to the selected device from the **Device Details** page:

1. Click the **TraceRoute** link located under the **Action** section of the right navigation tree on the selected device’s **Device Details** page. For information on navigating to a device’s **Device Details** page, see "Viewing devices with Device, IP, and Topology Views" (page 176).
   The **Traceroute** dialog box appears.
2. View the results of your Traceroute in the **Traceroute** dialog box.
3. Click **OK** to close the **Traceroute** dialog box.
View topology
You can view the position of the device in a topology and the network structure.

To view the topology of a device:

1. Click the **View Topology** link located under the **Action** section of the right navigation tree on the selected device’s **Device Details** page.
   For information on navigating to a device’s **Device Details** page, see "Viewing devices with Device, IP, and Topology Views" (page 176).
   The **Select Topology** dialog box appears.
2. Select a topology from the **Topology List**.
3. Click **OK**.

MIB management
The **MIB Management** option offers operators with the ability to view, edit, and manage the MIB file of the device.

To launch MIB Management for the selected device from the **Device Details** page:

1. Click the **MIB Management** link located under the **Action** section of the selected device’s **Device Details** page. For information on navigating to a device’s **Device Details** page, see "Viewing devices with Device, IP, and Topology Views" (page 176).
2. Load the MIB file and view MIB information.
   For more information on MIB Management, see "MIB management" (page 138).

Telnet/SSH proxy
With the Telnet/SSH proxy feature, you can use a browser to remotely access and manage devices through SSH or Telnet on any client without installing a Telnet/SSH tool. This feature uses the IMC server as a proxy, and uses a browser on a client to access devices, sends configuration commands, and displays output through Telnet/SSH.

To use the Telnet/SSH proxy to access and manage a device:

1. Click the **Telnet/SSH** link located under the **Action** section of the selected device’s **Device Details** page.
   For information on navigating to a device’s **Device Details** page, see "Viewing devices with Device, IP, and Topology Views" (page 176).
   The **Telnet/SSH Proxy** window appears.
2. Do one of the following:
   - Click the **button on the upper part of the window to connect to the selected device and the client displays the connection status information, or
   - Click the **button to disconnect from the device, or
   - Click the **button to set the connection protocol parameters, or
     If you use the Telnet protocol, you can modify the Telnet listening port, which is 23 by default. If you use the SSH protocol, you can modify the login information, including **User**
**Name, Password, and Port.** The Telnet/SSH proxy automatically selects Telnet or SSH for login according to the login method configured on the device. By default, Telnet is used.

- Click the button to clear all output displayed on the client.
  When you use the SSH protocol for connecting to a device, the username+password authentication is supported, and the key file authentication is not supported.

3. **Enter commands in the field on the lower part of the Telnet/SSH Proxy window to interact with the device.**

4. **After you type the commands, click the button to the right of the field or press Enter to send the commands to the device.**

**Open device panel**

The **Device Panel** provides you with a graphical view of HP, 3Com and H3C devices with the ability to monitor and manage the device from the graphical view.

To access the graphical device panel for the selected device from the **Device Details** page:

1. **Click the Open Device Panel link located under the Action section of the selected device’s Device Details page.**

   For information on navigating to a device’s Device Details page, see "Viewing devices with Device, IP, and Topology Views" (page 176).

The **Device Panel** for the selected device displays in a new browser window, providing you with a real time graphical rendering of the selected device. From the **Device Panel**, you can configure the selected device as well as view configuration and other information.

**Device panel navigation aids**

- Pointing to a component of the device displays component information.
- A left click a port to select the port.
- A right-click the chassis to display the **Chassis Menu** for viewing device information or configuration options. Information on the Chassis Menu can be found in the following section titled **Device Panel Chassis Menu**.
- A right-click a port from the device panel to display the **Port Menu** for viewing port information or configuration options. Information on the Port Menu can be found in the following section titled **Device Panel Port Menu**.

**Device panel chassis menu**

The Device Panel Chassis menu can be accessed by right-clicking the chassis itself from the **Device Panel**. This section provides an overview of the information and configuration options of the Chassis Menu.

- **Device Information:**

  From this menu option, you can:
  - View some or all of information in the following areas depending on the device type selected.
  - Configure the selected device.
- Perform Port Mode Switch, Port Aggregation, Reset Device, Save Device Configuration, Mpu Switch, Port Mirror, Address Binding, Environment Monitor, RMON, Config Interface 802.1X Status and RADIUS Server Configuration.

- **Protocol Management:** From this menu option, you can view information in the following areas (the areas vary with the device model):
  - **OSPF:** OSPF Attribute, Area Information, Stub Area Information, LSDB Information, Extended LSDB Information, OSPF Interface, Interface ToS Metric, Peer Information, Virtual Link Interface and Virtual Link Peer.
  - **MSTP:** Global MSTP, MSTI, and Port MSTP.
  - **IGMP Snooping:** IGMP Snooping Status, Aging Time of Router Port (second), Maximum Response Time of Query (second), and Aging Time of multicast Port (second).

- **Real-time Performance Monitor:** From this menu option, you can view performance information and configure the selected device in the **Device Realtime Monitor** area.

**Device panel port menu**

The **Device Panel Port Menu** can be accessed by right-clicking a port from the **Device Panel**, providing an overview of the information and configuration options of the Port Menu.

- **Port Management:** From this menu option, you can view information and configure Port Information, Loopback Test, and Add Port to VLAN.
  
  - **Realtime Performance Monitor:** From this menu option, you can view performance information and configure the selected device in the **Port Realtime Monitor** area.

**SSH**

You can launch an SSH session to the selected device from the **Device Details** page, providing quick and centralized access to managed devices.

To SSH to the selected device from the **Device Details** page:

1. Click the **SSH** link located under the **Action** section of the selected device’s **Device Details** page. For information on navigating to a device’s **Device Details** page, see "Viewing devices with Device, IP, and Topology Views" (page 176).
2. Follow the **Tools Configuration** dialog box for instructions on downloading and installing an SSH application used to establish an SSH session with the selected device, or browse your local machine for an application that supports SSH.
3. Follow the applications instructions for configuring and establishing an SSH sessions to the selected device. To use this feature, you must have an operating system or application that supports SSH on the computer you use to access IMC.

**Actions - For switches**

IMC offers the **IP/MAC Learning Query** service under the **Actions** section of the right navigation tree of the **Device Details** page which provides you with quick query the IP/MAC Learned information.

1. Click the **IP/MAC Learning Query** link located under the **Action** section of the selected device’s **Device Details** page.
For information on navigating to a device’s Device Details page, see "Viewing devices with Device, IP, and Topology Views" (page 176).

2. Enter the Learned IP address in the Learned IP Address field.
3. Enter the Learned MAC address in the Learned MAC Address field.
4. Click Query.

The results of your query display in the IP/MAC Learning List.

### IP/MAC learning list
- **Switch IP**: Contains the IP address of the selected switch which serves as a link for drilling down to the associated device’s Device Details page.
- **Interface Description**: Contains the interface description of the associated interface on the selected switch which serves as a link for drilling down to the associated interface’s Interface Details page.
- **VLAN ID**: Contains the VLAN ID to which the associated interface belongs.
- **Learned IP Address**: Contains the learned IP address associated with the interface listed in the Interface Description field.
- **Learned MAC Address**: Contains the learned MAC address associated with interface listed in the Interface Description field.

If the IP/MAC Learning List contains multiple entries, the following navigational aids may appear:

- Click ➔ to page forward in the IP/MAC Learning List.
- Click ➔ to page forward to the end of the IP/MAC Learning List.
- Click ➔ to page backward in the IP/MAC Learning List.
- Click ➔ to page backward to the front of the IP/MAC Learning List.

5. Click 8, 15, 50, 100, and 200 from the right side of the main pane to configure how many items per page you want to view.

6. For IP/MAC Learning lists that have more than one page, click 1, 2, 3, 4, 5, 6, 7, 8, 9, 10… from the bottom right side of the main pane to jump to a particular page of the IP/MAC Learning list.

You can sort the IP/MAC Learning List by most fields by clicking on the column label to sort the list by the selected field. The column label is a toggle switch that allows you to toggle between the various sort options specific to each field.

7. Click Reset when you have finished your query to clear the IP/MAC Learning List.

### Configure - For all devices

Using the Configure features found in the Device Details right navigation tree, you can modify a device label and system group attributes including system name, location, and contact, modify SNMP, Telnet, and SSH settings and modify status and configuration polling intervals as well as ping and Web Manager parameters.

**Modify device label**

The Device Label is the IMC name for the selected device. By default, IMC takes the system name or sysName of a device if the system name has been configured on it. However, you can change the name of the device in IMC for the device without changing the name on the device itself.
To modify the device label of the selected device from the Device Details page:

1. Click the Modify Device Label link located under the Configure section of the right navigation tree on the selected device’s Device Details page.
   
   For information on navigating to a device’s Device Details page, see "Viewing devices with Device, IP, and Topology Views" (page 176).
   
   The Modify device label dialog box appears.

2. Delete the existing device label name from the Device Label field and enter the new device name.

3. Click OK.

Modify system group attributes

You can also change other attributes of a device including its system name or sysName, its contact information, and the device’s location. This option is not available for desktop devices.

To modify the system group attributes of the selected device from the Device Details page:

1. Click the Modify System Group Attributes link located under the Configure section of the right navigation tree on the selected device’s Device Details page. For information on navigating to a device’s Device Details page, see "Viewing devices with Device, IP, and Topology Views" (page 176).
   
   The modify System Group Attributes dialog box appears.

2. Delete the existing system name in the System Name field and enter the new system name.

3. Delete the existing contact information in the Contact field and enter the new system name.

4. Delete the existing location information in the Location field and enter the new system name.

5. Click OK.

In addition to numbers, letters, and spaces, the characters in Table 4 (page 224) are valid entries for the System Name, Contact, and Location fields.

Table 4 Valid Characters for Naming

<table>
<thead>
<tr>
<th>Character</th>
<th>Name</th>
<th>Character</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>~</td>
<td>Tilde</td>
<td>'</td>
<td>Apostrophe or single quotation</td>
</tr>
<tr>
<td>!</td>
<td>Exclamation mark</td>
<td>@</td>
<td>At sign</td>
</tr>
<tr>
<td>#</td>
<td>Pound sign</td>
<td>$</td>
<td>Dollar sign</td>
</tr>
<tr>
<td>%</td>
<td>Percent sign</td>
<td>^</td>
<td>Caret</td>
</tr>
<tr>
<td>&amp;</td>
<td>Ampersand</td>
<td>*</td>
<td>Asterisk</td>
</tr>
<tr>
<td>( )</td>
<td>Parenthesis</td>
<td>=</td>
<td>Equal sign</td>
</tr>
<tr>
<td>+</td>
<td>Plus sign</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-</td>
<td>Hyphen</td>
<td>_</td>
<td>Underscore</td>
</tr>
<tr>
<td>[ ]</td>
<td>Square brackets</td>
<td>{ }</td>
<td>Braces</td>
</tr>
<tr>
<td>:</td>
<td>Colon</td>
<td>;</td>
<td>Semicolon</td>
</tr>
</tbody>
</table>
Modify SNMP settings

You can also modify IMC’s SNMP settings for the selected device. Modifying the SNMP settings changes the device’s SNMP settings but does not change the SNMP settings on the managed device.

To modify IMC’s SNMP settings for the selected device from the Device Details page:

1. Click the Modify SNMP Settings link located under the Configure section of the right navigation tree on the selected device’s Device Details page.

   For information on navigating to a device’s Device Details page, see “Viewing devices with Device, IP, and Topology Views” (page 176).

   The modify SNMP Parameters dialog box appears.

2. Do one of the following:
   o To edit IMC’s configuration of the device’s SNMP parameters, verify that the radio button to the left of Edit SNMP Parameters is selected, or
   o To edit IMC’s configuration using templates, skip down to "Using existing SNMP template" (page 156).

3. Select the version of SNMP (v1 or v2c) that is configured on the device to be added from the Parameter Type list:
   o Enter the read-only community string in the Read-Only Community String field, or
   o Enter the read-write community string in the Read-Write Community String field.

4. Enter the SNMP timeout value (1–60 seconds) in the Timeout field.
   This parameter determines how long IMC waits for an SNMP reply from the managed device before declaring that the request has timed out. The default is 4.

5. Enter the number of SNMP retries (1–20) in the Retries field.
   The retries parameter defines how many times the management system (IMC) sends SNMP retries in an attempt to communicate with the managed device before reporting a failure. The default is 3.

6. Click OK.

Using existing SNMP templates

To use existing SNMP templates:

1. To apply the SNMP settings of an existing SNMP template to this device, do one of the following:
   o Click the radio button to the left of Select an Existing Template, or
   o Click the radio button to the left of the SNMP template you want to use.
2. Click OK. For more information on creating SNMP templates, see "SNMP templates" (page 74).

Modify Telnet settings

To modify Telnet settings for the selected device from the Device Details page:

1. Click the Modify Telnet Settings link located under the Configure section of the right navigation tree on the selected device’s Device Details page.

   For information on navigating to a device’s Device Details page, see "Viewing devices with Device, IP, and Topology Views" (page 176).

   The modify Telnet Parameters dialog box appears.

2. Do one of the following:
   - To edit IMC’s configuration using templates, skip down to "Using an existing Telnet template" (page 156), or
   - To edit the Telnet parameters manually, verify that the radio button to the left of Edit Telnet Parameters is selected.

3. Select the Telnet authentication mode from the Authentication Mode list.

4. Enter the username in the Username field, if prompted.

5. Enter the password in the Password field, if prompted.

6. Enter the super password in the Super Password field, if prompted.

7. Enter the Telnet timeout value (1–60 seconds) in the Timeout field.

   The timeout parameter defines how long the system waits for the device to respond in seconds. The authentication mode selected must match what is configured on the device.

8. Click OK.

Using existing Telnet templates

To configure the Telnet settings for this device using an existing Telnet template:

1. Click the radio button to the left of Select an Existing Template.

2. Click the radio button to the left of the Telnet template you want to use.

3. Click OK. For more information on creating Telnet templates, see "Telnet templates" (page 77).

Modify SSH Settings

To modify SSH settings for the selected device from the Device Details page:

1. Click the Modify SSH Settings link located under the Configure section of the right navigation tree on the selected device’s Device Details page.

   For information on navigating to a device’s Device Details page, see "Viewing devices with Device, IP, and Topology Views" (page 176).

   The modify SSH Parameters dialog box appears.

2. Do one of the following:

   To edit IMC’s configuration using templates, skip down to "Using existing SSH templates" (page 165), or
To edit the SSH parameters, verify that the radio button to the left of Edit SSH Parameters is selected.

3. Select the authentication mode from the Authentication Mode list.
   The authentication mode selected must match what is configured on the device.

4. Enter username in the User Name field.

5. Enter the password in the Password field, if prompted.

6. Enter the path and filename of the private key file that contains the key that enables login, if prompted.

7. Enter the private key password for the private key file, if prompted.

8. Enter the TCP port for SSH in the Port field. The default TCP port is 22.

9. Enter the SSH timeout value (1–120 seconds).
   The timeout parameter defines how long the system waits for the device to respond in seconds before declaring that the response has timed out. The default setting is 10 seconds.

10. Enter the number of SSH retries (1–5).
    The retries parameter defines how many times the management system (IMC) sends SSH retries in an attempt to communicate with the managed device before reporting a failure. The default setting is 3.

11. Click OK to accept the SSH configuration.

Using existing SSH templates

To configure the SSH settings for this device using SSH templates:

1. Click the radio button to the left of Select SSH Parameters.

2. Click the radio button to the left of the SSH template you want to use.

3. Click OK to accept the SSH configuration. For more information on creating SSH templates, see “SSH templates” (page 80).

Modify SOAP Settings

When IMC’s add-on Virtual Network Manger (VNM) module is installed and in use, you can modify the SOAP settings IMC uses to remotely access the selected device.

To modify SOAP settings for the selected device from the Device Details page:

1. Click the Modify SOAP Settings link located under the Configure section of the right navigation tree on the selected device’s Device Details page.

   For information on navigating to a device’s Device Details page, see “Viewing devices with Device, IP, and Topology Views” (page 176).

   The modify SOAP Parameters dialog box appears.

2. Do one of the following:
   o To edit IMC’s configuration using templates, skip down to "Using existing SOAP Templates" (page 228), or
   o To edit the SOAP parameters, verify that the radio button to the left of Edit SOAP Parameters is selected.
3. Select the access URL protocol from the protocol list.
4. Enter the port number in the Port field.
5. Enter access URL root path in the Root Path field.
6. Enter the user name in the Username field.
7. Enter the password in the Password field.
8. Click the checkbox to the left of the Test connection to vManager/physical server, if you want to do the testing.
9. Click OK to accept the SOAP configuration.

Using existing SOAP Templates

To configure the SOAP settings for this device using SOAP templates:
1. Click the radio button to the left of Select an Existing Template.
2. Click the radio button to the left of the SOAP template you want to use.
3. Click OK to accept the SOAP configuration. For more information on creating SOAP templates, see "SOAP templates" (page 83).

Modify poll interval

You can also modify the polling interval settings for status and configuration polling for the selected device. Modifying the status or configuration polling interval influences directly how quickly IMC detects problems with status or configuration; setting long polling intervals delays the amount of time it takes IMC to detect a problem in the infrastructure and settings short polling intervals increases the resource demand on IMC.

To modify polling interval settings for the selected device from the Device Details page:
1. Click the Modify Poll Interval link located under the Configure section of the right navigation tree on the selected device’s Device Details page.
   For information on navigating to a device’s Device Details page, see "Viewing devices with Device, IP, and Topology Views" (page 176).
   The modify Poll Interval dialog box appears. The Configuration Poll Interval is the parameter that determines how long IMC waits before polling managed devices for any configuration changes.
2. Enter the configuration polling interval in minutes in the Configuration Poll Interval field.
   The range is 5–1500 minutes and the default is 120 minutes. Like most management systems, IMC uses ping to query devices for their status or reachability. The Status Poll Interval is the parameter that determines how long IMC waits before sending ping requests to the managed device to determine its reachability status.
3. Enter the status-polling interval in minutes in the Status Poll Interval field.
   The range is 30–600 seconds and the default is 60 seconds.
4. Click OK to accept the polling interval configuration.

Modify ping parameters
You can disable the status polling for devices and therefore eliminate alarms and reporting for those devices that are configured not to respond to ping requests.

To disable status polling using ping for the selected device from the Device Details page:

1. Click the Modify Ping Parameters link located under the Configure section of the right navigation tree on the selected device’s Device Details page.
   
   For information on navigating to a device’s Device Details page, see “Viewing devices with Device, IP, and Topology Views” (page 176).

   The modify Ping Parameters dialog box appears.

2. Uncheck the check marked box to the left of Support Ping Operation if you want to disable status polling for the selected device.

3. Click OK.

Modify web manager parameters

To modify the communication parameters for Web Manager

1. Click the Modify Web Manager Parameters link located under the Configure section of the right navigation tree on the selected device’s Device Details page.
   
   For information on navigating to a device’s Device Details page, see “Viewing devices with Device, IP, and Topology Views” (page 176).

   The modify Web Manager Parameters dialog box appears.

2. Select the protocol that is used by Web Manager from the Protocol list.

3. Enter the port number for Web Manager in the Port field.

4. Click OK.

   If you do not make a selection from the Protocol list and therefore the selection for Protocol is blank, IMC uses the global setting found under the System tab and the port value assigned is ignored.

Configure – For specific device types

IMC offers quick access to the ACL Management service module from the Device Details page. The ACL Configure link, which can be found under Configure on the right navigation tree for routers, redirects you to the ACL Management service module found under the Service tab. For more information on the ACL management features of IMC, see "10 Access control list management" (page 645).

Performance monitoring

In the Performance Monitor section of the right navigation tree of the Device Details page, you can quickly access performance reports for the selected device. In addition, you can refresh monitor instances as well as delete performance data and cancel configured monitor instances.

By default, IMC provides two monitors for all devices: Average Unreachability and Average Response Time as measured by ping requests and responses for devices that support ping monitoring. By default, four monitors are created for managed network devices, such as routers, switches, and wireless devices, which support these metrics. These four monitors are: Average CPU Utilization, Average Memory Utilization, Average Unreachability, and Average Response Time.
For devices that support neither, the Add Monitor link appears when there is no performance monitor instance configured for the selected device.

**Add Monitor**

The Add Monitor link appears under Performance Monitor on the right navigation tree only if there are no performance monitors already configured for the selected device. The Add Monitor link is a shortcut to the Performance Management → Monitoring Settings → Add Monitor menu option located on the left navigation tree under the Resource tab. For more information on adding monitors, see “9 Performance management” (page 607).

**Cancel Monitor**

Once monitors have been created for the selected device, the Cancel Monitor option appears on the right navigation tree. From this menu option, you can remove or cancel all monitoring instances for the selected device.

To cancel all monitor instances from the Device Details page:

1. Click the Cancel Monitor link located under the Performance Monitor section of the right navigation tree on the selected device’s Device Details page. For information on navigating to a device’s Device Details page, see “Viewing devices with Device, IP, and Topology Views” (page 176).

   All monitors are removed and the Results page appears.

2. Refer to the Result field of the Results table for details on the results of the monitoring operation. In addition, all links under the Performance Monitor section of the right navigation tree are replaced with the Add Monitor link.

   **WARNING:**
   
   Clicking the Cancel Monitors removes all monitoring instances for the selected device without warning; use this feature with caution.

**Performance at a glance**

To view the most current and historical data for the performance monitor instances configured for this device from the Device Details page:

1. Click the Performance at a Glance link located under the Performance Monitor section of the right navigation tree on the selected device’s Device Details page.

   For information on navigating to a device’s Device Details page, see “Viewing devices with Device, IP, and Topology Views” (page 176).

   IMC displays reports for the current day for all monitors instances for the selected device. Use the scroll bar on the right to view all reports.

**Refresh monitor instance**

To refresh the data for the monitor instances for this device from the Device Details page:
1. Click the **Refresh Monitor Instance** link located under the **Performance Monitor** section of the right navigation tree on the selected device’s **Device Details** page.

For information on navigating to a device’s **Device Details** page, see “Viewing devices with Device, IP, and Topology Views” (page 176).

2. Click **OK** to perform your operation.

**Delete performance data**

To delete performance data for the monitor instances for this device without deleting the monitoring instances from the **Device Details** page:

1. Click the **Delete Performance Data** link located under the **Performance Monitor** section of the right navigation tree on the selected device’s **Device Details** page.

For information on navigating to a device’s **Device Details** page, see “Viewing devices with Device, IP, and Topology Views” (page 176).

2. Click **OK** to confirm deletion of the performance data.

**Device real-time monitor**

To add a **Realtime Monitor** for this device:

1. Click the **Device Realtime Monitor** link located under the **Performance Monitor** section of the right navigation tree on the selected device’s **Device Details** page.

For information on navigating to a device’s **Device Details** page, see “Viewing devices with Device, IP, and Topology Views” (page 176).

2. Click **Select Index** to select one or more monitor indexes.

3. Click **OK**.

**Configuration center**

IMC provides you with the ability to launch configuration management tasks for the selected device directly from the **Device Details** page. From the **Device Details** page, you can, with one click, back up the configuration of the selected device and configure the automated backup attributes for the selected device.

**Backup configuration files**

To backup device configuration from the **Device Details** page:

1. Click the **Backup Configuration File** link located under the **Configuration Center** section of the right navigation tree on the selected device’s **Device Details** page.

2. View the results of the backup task in the **Configuration File Backup Result** page that display upon completion of the backup request.

**Set auto backup attribute**
The Set Auto Backup Attribute link is a shortcut to the Auto Backup Plan feature of the Configuration Center service module. For more information on adding monitors, see "Automatic device configuration backups" (page 475).

Device default startup configuration

You can specify the default startup software, primary configuration file, and secondary configuration file for a device.

1. Click the Device Default Startup Configuration link located under the Configuration Center section of the right navigation tree on the selected device’s Device Details page. The Device Default Startup Configuration window appears.

2. Set the default startup software. Select Image. Valid options include Primary and Secondary.

3. Do one of the following:
   o To configure the device to start with the primary startup software, select Primary, or
   o To configure the device to start with the secondary startup software, select Secondary.

The Startup Configuration File list shows all configurations files on the device:
   o File Name: Contains the name of the configuration file.
   o Active: Identifies the configuration file that is currently in use with an icon ✓.
   o Primary: Identifies the primary configuration file with an icon ✓. If the file is not the primary configuration file of the device, this field contains a ✓ Configure link. You can click the link to configure the file as the primary configuration file. Note that the process takes some time.
   o Secondary: Identifies the secondary configuration file with an icon ✓. If the file is not the secondary configuration file of the device, this field contains a ✓ Configure link. You can click the link to configure the file as the secondary configuration file. The process takes some time.
   o Copy: Contains an icon ☐ that copies the configuration file. After you rename the copied configuration file, it appears on the Startup Configuration File list.
   o Delete: Contains an icon ✗ for deleting the configuration file.

4. Click Close.

Device Management

The options displayed in this section of the right navigation tree vary based upon the selected device being viewed in the Device Details page.

Basic options under Device Management include the ability to reset a device and save device configuration.

From the Device Management menu option, you can also view system information including the IP Address Table, the Address Translation Table, the IP Routing Table and the TCP Connection Table.
You can also view address binding including **MAC-Port Binding Management**, **Global MAC Address Learning Configuration** and **Port MAC Address Learning Management**.

You can also view device hardware information including module, port, power, and fan information.

IPv6 information is also available from the **Device Management** menu. This option enables you to view the following: **IPv6 Address Translation Table**, **IPv6 Interface Table**, **IPv6 Address Table**, **IPv6 Routing Table**, **IPv6 Address Prefix Table**, **IPv6 UDP Table**, and **IPv6 TCP Table**.

Finally, port aggregation information is also available from the **Device Management** menu. From this menu, you can configure or remove port aggregation for the selected device.

### Resetting a device

You can reset routers, switches, and wireless devices by using the **Reset Device** option located in the **Device Management** section of the right navigation tree of the **Device Details** page.

To reset the selected device from the **Device Details** page:

1. Click the **Reset Device** link located under the **Device Management** section of the right navigation tree on the selected device’s **Device Details** page.
   
   For information on navigating to a device’s **Device Details** page, see "Viewing devices with Device, IP, and Topology Views" (page 176) and "Viewing devices with custom views" (page 201).

   The **Reset Device** dialog box appears.

2. Do one of the following:
   
   a. Click the check marked box to the left of **Save device’s current configuration** if you want to reboot the device without saving its current configuration, or
   
   b. Leave the checkbox checked if you want to save the device’s current configuration.

3. Click **Reset**.

4. Verify that the device reset was successful by checking the **Reset Device** dialog box for reset results.

5. Click **Close** to close the **Reset Device** dialog box.

### Saving configuration

You can save the configuration of routers, switches, and wireless devices by using the **Save Configuration** option located in the **Device Management** section of the right navigation tree of the **Device Details** page.

To save the configuration of the selected device from the **Device Details** page:

1. Click the **Save Configuration** link located under the **Device Management** section of the right navigation tree on the selected device’s **Device Details** page.
   
   For information on navigating to a device’s **Device Details** page, see "Viewing devices with Device, IP, and Topology Views" (page 176) and "Viewing devices with custom views" (page 201).

2. Click **OK** to confirm your request to save the configuration for the selected device.
Environment monitor

To view or modify the environment information for the selected card, or reset the card:

1. Click the Environment Monitor link located under the Device Management section of the right navigation tree on the selected device’s Device Details page.

   For information on navigating to a device’s Device Details page, see “Viewing devices with Device, IP, and Topology Views” (page 176) and “Viewing devices with custom views” (page 201).

   The Environment Monitor page appears.

   Environment monitor list

   - Frame No.: Contains the frame No.
   - Slot No.: Contains the slot No. that specifies the slot where the board resides.
   - Type: Contains the type of the board.
   - Status: Indicates the state is normal, upper indicates that the temperature exceeds the upper threshold, and lower indicates the temperature is under the lower threshold.
   - Value(cent.): Contains the temperature of the board.
   - Upper Limit(cent.): Contains the upper threshold for the board temperature.
   - Lower Limit(cent.): Contains the lower threshold for the board temperature.
   - Modify: Contains the link for modifying the environment parameters, including upper limit, lower limit and critical limit.
   - Reset: Contains a link to reset the card and the Save device’s current configuration option.

   If the Environment lists multiple entries, the following navigational aids may appear:

   - Click ▶️ to page forward in the Environment list.
   - Click ▶️ to page forward to the end of the Environment list.
   - Click ◀️ to page backward in the Environment list.
   - Click ◀️ to page backward to the front of the Environment list.

2. Click 8, 15, 50, 100, and 200 from the right side of the main pane to configure how many items per page you want to view.

Switch MPU

To switch the active/standby MPUs for the selected device and view MPU information:

1. Click the Switch MPU link located under the Device Management section of the right navigation tree on the selected device’s Device Details page.

   For information on navigating to a device’s Device Details page, see “Viewing devices with Device, IP, and Topology Views” (page 176) and “Viewing devices with custom views” (page 201).

   The MPU Switch page appears, including the Last MPU Switch Date, Last MPU Switch Time, and MPU Switch Times options.

2. Click Switch to switch the active/standby MPUs.
System information

To view the system information for the selected device from the Device Details page:

1. Click the **System Information** link located under the Device Management section of the right navigation tree on the selected device’s Device Details page.

2. For information on navigating to a device’s Device Details page, see “Viewing devices with Device, IP, and Topology Views” (page 176) and “Viewing devices with custom views” (page 201).

   The IP Address Table page appears. Four tables of system information are displayed: IP Address Table, Address Translation Table, IP Routing Table, and TCP Connection Table.

3. To access any one of these tables, click the tabs located at the top of the page.

4. Click **Close** to close the page.

Mirror group

You can add, edit, and delete mirror groups for devices.

Displaying mirror group information

1. Click the **Mirror Group** link located under the Device Management section of the right navigation tree on the selected device’s Device Details page.

   For information on navigating to a device’s Device Details page, see “Viewing devices with Device, IP, and Topology Views” (page 176) and “Viewing devices with custom views” (page 201).

   The Mirror Group (MG) page appears.

   **Mirror Group (MG) list**
   - **MG ID**: Contains the MG ID.
   - **MG Type**: Contains the MG type.
   - **MG Status**: Contains the MG status.
   - **MG Mirror**: Contains a link to edit the MG mirror.
   - **MG Reflector**: Contains a link to edit the MG reflector.
   - **MG VLAN ID**: Contains a link to edit the MG VLAN ID.

   If the Mirror Group (MG) List contains multiple entries, the following navigational aids may appear:
   - Click to page forward in the Mirror Group (MG) List.
   - Click to page forward to the end of the Mirror Group (MG) List.
   - Click to page backward in the Mirror Group (MG) List.
   - Click to page backward to the front of the Mirror Group (MG) List.

2. Click 8, 15, 50, 100, and 200 from the right side of the main pane to configure how many items per page you want to view.
Adding a mirror group

1. Click the Mirror Group link located under the Device Management section of the right navigation tree on the selected device’s Device Details page.

For information on navigating to a device’s Device Details page, see “Viewing devices with Device, IP, and Topology Views” (page 176) and “Viewing devices with custom views” (page 201).

The Mirror Group (MG) page appears.

2. Click Add to add a mirror group.

3. Enter the MG ID in the MG ID field.

4. Select the MG type from the MG Type list.

5. Click OK to add the mirror group.

Editing a mirror group

After you add a mirror group, you need to configure the MG mirrors, MG reflectors, or MG VLAN IDs for the mirror group.

Configuring MG mirrors

1. Click the Mirror Group link located under the Device Management section of the right navigation tree on the selected device’s Device Details page.

For information on navigating to a device’s Device Details page, see “Viewing devices with Device, IP, and Topology Views” (page 176) and “Viewing devices with custom views” (page 201).

The Mirror Group (MG) page appears.

2. Click the MG Mirror icon you want to configure.

The MG Mirror page appears.

MG mirror list

- **MG ID**: Contains the MG ID.
- **MG Mirror**: Contains the MG mirror.
- **MG Mirror Direction**: Contains the MG mirror direction.

If the **MG Mirror** List contains multiple entries, the following navigational aids may appear:

- Click to page forward in the **MG Mirror** List.
- Click to page forward to the end of the **MG Mirror** List.
- Click to page backward in the **MG Mirror** List.
- Click to page backward to the front of the **MG Mirror** List.

3. Click 8, 15, 50, 100, and 200 from the right side of the main pane to configure how many items per page you want to view.

4. Click Add to add an MG mirror.

5. Select the MG ID in the **MG ID** list.

6. Select the MG mirror in the **MG Mirror** list.
7. Select the MG mirror direction in the **MG Direction** list.

8. Do one of the following:
   - Click **OK** to add the MG mirror, or
   - Select one or more MG mirrors you want to delete and click **Delete**.

9. Click **Return** to return to the **Mirror Group (MG)** page.

### Configuring MG monitors

1. Click the **Mirror Group** link located under the **Device Management** section of the right navigation tree on the selected device’s **Device Details** page.

   For information on navigating to a device’s **Device Details** page, see “Viewing devices with Device, IP, and Topology Views” (page 176) and “Viewing devices with custom views” (page 201).

   The **Mirror Group (MG)** page appears.

2. Click the **MG Monitor** icon you want to configure.

   The **MG Monitor** page appears.

   **MG monitor list**
   - **MG ID**: Contains the MG ID.
   - **MG Monitor**: Contains the MG monitor.

   If the **MG Monitor** List contains multiple entries, the following navigational aids may appear:
   - Click **to page forward in the **MG Monitor** List.
   - Click **to page forward to the end of the **MG Monitor** List.
   - Click **to page backward in the **MG Monitor** List.
   - Click **to page backward to the front of the **MG Monitor** List.

3. Click 8, 15, 50, 100, or 200 from the right side of the main pane to configure how many items per page you want to view.

4. Click **Add** to add an MG monitor.

5. Select the MG ID in the **MG ID** list.

6. Select the MG monitor in the **MG Monitor** list.

7. Do one of the following:
   - Click **OK** to add the MG monitor, or
   - Select one or more MG monitors you want to delete and click **Delete**.

8. Click **Return** to return to the **Mirror Group (MG)** page.

### Configuring MG reflectors

You can configure this option only when the **remoteSource** option is selected as the MG type. To configure the MG reflector:

1. Click the **Mirror Group** link located under the **Device Management** section of the right navigation tree on the selected device’s **Device Details** page.
For information on navigating to a device’s Device Details page, see "Viewing devices with Device, IP, and Topology Views" (page 176) and "Viewing devices with custom views" (page 201).

The Mirror Group (MG) page appears.

2. Click the MG Reflector icon you want to configure.

The MG Reflector page appears.

**MG reflector list fields and explanations**

- **MG ID**: Contains the MG ID.
- **MG Reflector**: Contains the MG reflector.

If the MG Monitor List contains multiple entries, the following navigational aids may appear:

- Click to page forward in the MG Reflector List.
- Click to page forward to the end of the MG Reflector List.
- Click to page backward in the MG Reflector List.
- Click to page backward to the front of the MG Reflector List.

3. Click 8, 15, 50, 100, or 200 from the right side of the main pane to configure how many items per page you want to view.

4. Click Add to add an MG reflector.

5. Select the MG ID in the MG ID list.

6. Select the MG reflector in the MG Reflector list.

7. Do one of the following:
   - Click OK to add the MG reflector, or
   - Select one or more MG reflectors you want to delete and click Delete.

8. Click Return to return to the Mirror Group (MG) page.

**Setting the MG VLAN ID**

You can configure this option only when the remoteSource or remoteDestination option is selected as the MG type. To set the MG VLAN ID:

1. Click the Mirror Group link located under the Device Management section of the right navigation tree on the selected device’s Device Details page.

   For information on navigating to a device’s Device Details page, see "Viewing devices with Device, IP, and Topology Views" (page 176) and "Viewing devices with custom views" (page 201).

   The Mirror Group (MG) page appears.

2. Click the MG VLAN ID icon you want to set.

   The MG VLAN ID page appears.

**MG VLAN ID list**

- **MG ID**: Contains the MG ID.
- **MG VLAN ID**: Contains the MG VLAN ID.
If the **MG VLAN ID** list contains multiple entries, the following navigational aids may appear:

- Click to page forward in the **MG VLAN ID** list.
- Click to page forward to the end of the **MG VLAN ID** list.
- Click to page backward in the **MG VLAN ID** list.
- Click to page backward to the front of the **MG VLAN ID** list.

3. Click 8, 15, 50, 100, or 200 from the right side of the main pane to configure how many items per page you want to view.

4. Click **Add** to add an **MG VLAN ID**.

5. Select the **MG ID** in the **MG ID** list.

6. Select the **MG VLAN ID** in the **MG VLAN ID** list.

7. Do one of the following:
   - Click **OK** to add the **MG VLAN ID**, or
   - Select one or more **MG VLAN IDs** you want to delete and click **Delete**.

8. Click **Return** to return to the **Mirror Group (MG)** page.

### Deleting mirror groups

1. Click the **Mirror Group** link located under the **Device Management** section of the right navigation tree on the selected device’s **Device Details** page.

   For information on navigating to a device’s **Device Details** page, see "Viewing devices with Device, IP, and Topology Views" (page 176) and "Viewing devices with custom views" (page 201).

   The **Mirror Group (MG)** page appears.

2. Click the checkboxes  to the left of the **MG ID** you want to delete.

3. Click **Delete**.

4. Click **OK** to confirm deletion of the selected items.

### Address binding

You can both view and configure port to MAC address binding for devices by using the **Address Binding** option located in the **Device Management** section of the right navigation tree of the **Device Details** page.

To view and configure MAC address binding for the selected device from the **Device Details** page:

1. Click the **Address Binding** link located under the **Device Management** section of the right navigation tree on the selected device’s **Device Details** page. For information on navigating to a device’s **Device Details** page, see "Viewing devices with Device, IP, and Topology Views" (page 176) and "Viewing devices with custom views" (page 201).

   The **MAC-Port Binding Management** page appears. Three types of MAC address information tables and configuration options are displayed: **MAC-Port Binding Management**, **Global MAC Address Learning Configuration**, and **Port MAC Address Learning Management**.

2. To access any one of these configuration windows, click the tabs located at the top of the page.
The title bar of the window changes to reflect the tab’s title and IMC displays all MAC-Port Binding Management entries in the list displayed under the MAC-Port Binding Management tab.

**MAC-Port Binding Management Table**
- **VLAN ID**: Contains the VLAN ID to which the associated MAC address belongs.
- **MAC Address**: Contains the MAC address.
- **Port**: Contains the interface description.
- **MAC Address Entry Type**: Contains information on how the address was acquired.
- **Modify**: Contains a link for modifying the associated MAC address.

**To bind a MAC address-port**
1. Click the **Address Binding** link located under the Device Management section of the right navigation tree on the selected device’s Device Details page.
   For information on navigating to a device’s Device Details page, see "Viewing devices with Device, IP, and Topology Views" (page 176) and "Viewing devices with custom views" (page 201).
   The MAC-Port Binding Management page appears.
2. Click **Add** from the MAC-Port Binding Management table.
3. Select the VLAN to which this port belongs from the **VLAN ID** list.
4. Enter the MAC address you want to bind to this port in the **MAC Address** field.
   The format IMC accepts for MAC addresses is ####-####-#### where # is the hexadecimal value of the MAC address.
5. Select the port you want to bind to the MAC address to in the **Port** field.
6. Select the type of MAC address from the **MAC Address Entry Type** field.
7. Click **OK** to accept your configuration.
8. Click **Close**.

**To modify a MAC address-port binding configuration**
1. Click the **Address Binding** link located under the Device Management section of the right navigation tree on the selected device’s Device Details page.
   For information on navigating to a device’s Device Details page, see "Viewing devices with Device, IP, and Topology Views" (page 176) and "Viewing devices with custom views" (page 201).
   The MAC-Port Binding Management page appears.
2. Click the **Modify** icon associated with the MAC-Port binding configuration you want to modify.
3. Select the type of MAC address from the **MAC Address Entry Type** field.
4. Click **OK** to accept your configuration.
5. Click **Close**.
To delete a MAC-port binding

1. Click the Address Binding link located under the Device Management section of the right navigation tree on the selected device’s Device Details page.

   For information on navigating to a device’s Device Details page, see “Viewing devices with Device, IP, and Topology Views” (page 176) and “Viewing devices with custom views” (page 201).

   The MAC-Port Binding Management page appears.

2. From the MAC-Port Binding Management table, click on the checkboxes ☐ to the left of the MAC-Port binding configuration you want to delete.

3. Click Delete.

4. Click OK to confirm deletion of the selected items.

To configure the global MAC address learning configuration

1. Click the Address Binding link located under the Device Management section of the right navigation tree on the selected device’s Device Details page.

   For information on navigating to a device’s Device Details page, see “Viewing devices with Device, IP, and Topology Views” (page 176) and “Viewing devices with custom views” (page 201).

   The MAC-Port Binding Management page appears.

2. Click the Global MAC Address Learning Configuration tab.

3. Enter the MAC address aging time in seconds in the MAC Address Aging Time field.

   Valid range is 10–1000000. The value -1 entered in this field indicates no limit to MAC address aging.

4. Click OK.

To modify a port MAC address learning management

1. Click the Address Binding link located under the Device Management section of the right navigation tree on the selected device’s Device Details page.

   For information on navigating to a device’s Device Details page, see “Viewing devices with Device, IP, and Topology Views” (page 176) and “Viewing devices with custom views” (page 201).

   The MAC-Port Binding Management page appears.

2. Click the Port MAC Address Learning Management tab.

3. Click the Modify icon ☑ associated with interface you want to modify.

4. Enter the maximum learnable MAC address in the Max Learnable MAC Addresses field.

   Valid range is 1–262144. The value –1 entered in this field denotes no limit.

5. Click OK to accept your configuration.

Hardware information
From the **Hardware Information** link under **Device Management**, you can view information about selected routers, switches, and wireless devices. The information provided in this view may vary by device type but most network device types provide **Device Information**, **Module Information**, **Port Information**, **Power Information**, and **Fan Information**.

To view hardware information for the selected device from the **Device Details** page:

1. Click the **Hardware Information** link located under the **Device Management** section of the right navigation tree on the selected device’s **Device Details** page.

   For information on navigating to a device’s **Device Details** page, see "Viewing devices with Device, IP, and Topology Views" (page 176) and "Viewing devices with custom views" (page 201).

   The **Hardware Information** page appears.

2. Use the **Device Information**, **Module Information**, **Port Information**, **Power Information**, and **Fan Information** tabs located at the top of the **Device Information** page to navigate to the information page you wish you view.

3. Click **Close** when you have finished viewing the hardware information for the selected device.

**IPv6 information**

From the **IPv6 Information** link under **Device Management**, you can view IPv6 information for selected routers, switches, and wireless devices. The information provided in this view includes **IPv6 Address Translation Table**, **IPv6 Interface Table**, **IPv6 Address Table**, **IPv6 Routing Table**, **IPv6 Address Prefix Table**, **IPv6 UDP Table**, and **IPv6 TCP Table**.

To view IPv6 information for the selected device from the **Device Details** page:

1. Click the **IPv6 Information** link located under the **Device Management** section of the right navigation tree on the selected device’s **Device Details** page.

   For information on navigating to a device’s **Device Details** page, see "Viewing devices with Device, IP, and Topology Views" (page 176) and "Viewing devices with custom views" (page 201).

   The **IPv6 Information** page appears.

2. Use the **IPv6 Address Translation Table**, **IPv6 Interface Table**, **IPv6 Address Table**, **IPv6 Routing Table**, **IPv6 Address Prefix Table**, **IPv6 UDP Table**, and **IPv6 TCP Table** tabs located at the top of the **IPv6 Information** page to navigate to the information page you wish you view.

3. Click **Close** when you have finished viewing the IPv6 information for the selected device.

**Port mode switch**

This feature enables you to switch the port mode. The options include **Bridge Mode** and **Route mode**.

To switch the port mode:

1. Click the **Port Mode Switch** link located under the **Device Management** section of the right navigation tree on the selected device’s **Device Details** page.

   For information on navigating to a device’s **Device Details** page, see "Viewing devices with Device, IP, and Topology Views" (page 176) and "Viewing devices with custom views" (page 201).

   The Port Mode Switch page appears.
Port mode switch list
- **Port Description**: Contains the port description.
- **Port Mode**: Contains the port mode.
- **Is Support**: Contains support for switching the port mode.
- **Switch**: Contains a link to switch the port mode.

If the **Port Mode Switch List** contains multiple entries, the following navigational aids may appear:
- Click ![Next](image) to page forward in the **Port Mode Switch List**.
- Click ![End](image) to page forward to the end of the **Port Mode Switch List**.
- Click ![Back](image) to page backward in the **Port Mode Switch List**.
- Click ![First](image) to page backward to the front of the **Port Mode Switch List**.

2. Click 8, 15, 50, 100, or 200 from the right side of the main pane to configure how many items per page you want to view.

3. Click the ![Switch](image) link next to the port whose port mode you want to switch in the **Port Mode Switch List**.

4. Confirm your operation to switch the port mode.

Port aggregation
You can add, modify, and delete port aggregation information for devices.

Viewing port aggregation information

1. Click the ![Aggregation](image) link located under the **Device Management** section of the right navigation tree on the selected device’s **Device Details** page.

   For information on navigating to a device’s **Device Details** page, see “Viewing devices with Device, IP, and Topology Views” (page 176) and “Viewing devices with custom views” (page 201).

   The **Port Aggregation Management** page appears.

Port aggregation list
- **Aggregation ID**: Contains the aggregation ID.
- **Aggregation Mode**: Contains the aggregation mode.
- **Edit**: Contains a link to edit port aggregation information.

If the **Port Aggregation Management List** contains multiple entries, the following navigational aids may appear:
- Click ![Next](image) to page forward in the **Port Aggregation Management List**.
- Click ![End](image) to page forward to the end of the **Port Aggregation Management List**.
- Click ![Back](image) to page backward in the **Port Aggregation Management List**.
- Click ![First](image) to page backward to the front of the **Port Aggregation Management List**.

2. Click 8, 15, 50, 100, or 200 from the right side of the main pane to configure how many items per page you want to view.
Adding a port aggregation entry

1. Click the Port Aggregation link located under the Device Management section of the right navigation tree on the selected device’s Device Details page.

For information on navigating to a device’s Device Details page, see "Viewing devices with Device, IP, and Topology Views" (page 176) and "Viewing devices with custom views" (page 201).

The Port Aggregation Management page appears.

2. Click Add to add a port aggregation entry.

3. Enter the aggregation ID in the Aggregation ID field.

4. Select aggregation mode from the Aggregation Mode list.

5. Click OK to add the port aggregation entry.

Modifying port aggregation information

1. Click the Port Aggregation link located under the Device Management section of the right navigation tree on the selected device’s Device Details page.

For information on navigating to a device’s Device Details page, see "Viewing devices with Device, IP, and Topology Views" (page 176) and "Viewing devices with custom views" (page 201).

The Port Aggregation Management page appears.

2. Click the Edit link on the Port Aggregation Management list.

The Port List page appears.

Port list

- Aggregation ID: Contains the aggregation ID in the Aggregation ID field.
- Port Index: Contains the port index in the Port Index field.
- Port Description: Contains the port description in the Port Description field.

If the Port List contains multiple entries, the following navigational aids may appear:

- Click to page forward in the Port List.
- Click to page forward to the end of the Port List.
- Click to page backward in the Port List.
- Click to page backward to the front of the Port List.

3. Click 8, 15, 50, 100, or 200 from the right side of the main pane to configure how many items per page you want to view.

4. Click Add Port above the Port List.

5. Select one or more ports in the Please Select Port dialog box.

6. Do one of the following:
   - Click OK to add the ports, or
   - Select one or more ports you want to delete and click Delete.

7. Click Return to return to the Port Aggregation Management page.
Deleting port aggregation information

1. Click the Port Aggregation link located under the Device Management section of the right navigation tree on the selected device’s Device Details page.

   For information on navigating to a device’s Device Details page, see “Viewing devices with Device, IP, and Topology Views” (page 176) and “Viewing devices with custom views” (page 201).

   The Port Aggregation Management page appears.

2. Click the checkboxes □ to the left of the aggregation ID n you want to delete.

3. Click Delete.

4. Click OK to confirm deletion of the selected items.

PoE management for switches

IMC offers you a portal for configuring Power over Ethernet for switches.

From the PoE Energy Management link under Device Management, you can view and configure the PoE settings for the selected switch. The information provided in this view includes PoE Power Units information and PoE Port Power Consumption information and configuration options.

To view and configure PoE management settings for the selected device from the Device Details page:

1. Click the PoE Energy Management link located under the Device Management section of the right navigation tree on the selected device’s Device Details page.

   For information on navigating to a device’s Device Details page, see “Viewing devices with Device, IP, and Topology Views” (page 176) and “Viewing devices with custom views” (page 201).

   The PoE Energy Management page appears.

2. Use the PoE Power Units and PoE Port Power Consumption tabs located at the top of the PoE Energy Management page to navigate to the information page you wish you view:

   • Use the PoE Power Units tab to view PoE power units for the selected switch.
   • Use the PoE Port Power Consumption tab to configure PoE port power allocations on a per port basis.

Modifying PoE port power consumption

1. Click the Modify icon associated with the port you want to modify.

2. To enable PoE port power consumption on the selected port, select Enable from the Status list.

3. Select the priority of the selected port for power allocation from the Port Priority list.

4. Enter the maximum amount of power, in mill watts (mW), to be allocated to the selected port from the Max Power field.

   The valid range is 0–100000.

5. Click OK to accept your changes.

   For more information on PoE configurations for the selected switch, see the vendor’s switch documentation.
RADIUS server configuration

This feature enables you to configure the RADIUS server for access devices.

1. Click the **RADIUS Server Configuration** link located under the Device Management section of the right navigation tree on the selected device’s Device Details page.

2. For information on navigating to a device’s Device Details page, see "Viewing devices with Device, IP, and Topology Views" (page 176) and "Viewing devices with custom views" (page 201).

   The RADIUS Server Configuration page appears. The configuration page contains RADIUS Authentication Server Configuration, RADIUS Accounting Server Configuration, and 802.1X Configuration.

3. **RADIUS Authentication Server Configuration:**
   a. Enter the scheme name in the Scheme Name field.
   b. Enter the primary server IP address in the Primary Server IP field.
   c. Enter the primary server UDP port number in the Primary Server UDP Port field. By default, the UDP port number is 1812.
   d. Enter the second server IP address in the Secondary Server IP field.
   e. Enter the second server UDP port number in the Secondary Server UDP Port(1-65535) field.
   f. Enter the shared secret in the Shared Secret field.
   g. Select the service type from the Service Type list.
   h. Select the username format from the Username Format list.
   i. Enter the domain name in the Domain Name field.

4. **RADIUS Accounting Server Configuration:**
   a. Enter the primary server IP address in the Primary Server IP field.
   b. Enter the primary server UDP port number in the Primary Server UDP Port(1-65535) field. By default, the primary server UDP port number is 1813.
   c. Enter the secondary server IP address in the Secondary Server IP field.
   d. Enter the secondary server UDP port number in the Secondary Server UDP Port(1-65535) field. By default, the secondary server UDP port number is 1813.

5. **802.1X Configuration:**
   a. Select the global 802.1X status from the Global 802.1X Status list.
   b. Select the authentication mode from the Authentication Mode list.

6. Click **Config** to complete the configuration.

Interface 802.1X configuration

This function allows you to enable or disable 802.1X on interfaces, and remove interfaces for which you do not need to change the 802.1X status from the interface list.

1. Click the **Interface 802.1X Configuration** link located under the Device Management section of the right navigation tree on the selected device’s Device Details page.
For information on navigating to a device’s Device Details page, see "Viewing devices with Device, IP, and Topology Views" (page 176) and "Viewing devices with custom views" (page 201).

The Interface 802.1X configuration page appears.

**Configure interface 802.1X status list**

- **Device IP**: Contains the device IP address of the interface.
- **Interface Description**: Contains the interface description.
- **802.1X Status**: Contains the current 802.1X status of the interface.
- **Delete**: Contains the link to delete the interface that you do not need to change the 802.1X status.

If the **Configure Interface 802.1X Status** list contains multiple entries, the following navigational aids may appear:

- Click ⬅️ to page backward in the **Configure Interface 802.1X Status** list.
- Click ➔ to page forward in the **Configure Interface 802.1X Status** list.
- Click ➔ to page forward to the end of the **Configure Interface 802.1X Status** list.
- Click ⬅️ to page backward to the front of the **Configure Interface 802.1X Status** list.

2. Click 8, 15, 50, 100, or 200 from the right side of the main pane to configure how many items per page you want to view.
3. Click **Enable 802.1X** or **Disable 802.1X** to enable or disable 802.1X from all interfaces on the list.

**Virtual connect**

VC is a network interconnected technology to replace traditional switch connections and management. VC reduces network costs in various aspects. For example, it reduces cabling cost and complexity, and allows pre-provision of network assignments. VC also simplifies blade server connectivity to production LANs, SANs and converged networks. The VC technology uses an abstraction layer between servers and their external networks to virtualize I/O connections, and displays network interface (NIC) and host bus adapter (HBA) addresses on LANs and SANs, instead of the default physical interface addresses.

IMC offers virtual connect management, allowing you to configure Ethernet network, FC, FCoE, and iSCSI connections and server downlink port mappings.

1. Click the 🌐 Virtual Connect link located under the Device Management section of the right navigation tree on the selected device’s Device Details page.
   The Virtual Connect window appears.
2. Click a tab on top of the window to enter the corresponding configuration page. The tabs include **Ethernet Network Connections**, **FC SAN Connections**, **FCoE Connections**, **iSCSI Connections**, and **Server Port Mappings**.
3. Click **Add**.
   On the window that appears, you can configure the following parameters:

   - **Ethernet Network Connections**
- **Profile Name**
- **Network**
- **PXE**
- **Address Type**
- **Ethernet MAC**
- **iSCSI MAC**
- **Speed Type**
- **Speed**

- **FC SAN** Connections
  - **Profile Name**
  - **Fabric**
  - **Speed**
  - **Address Type**
  - **Port WWN**
  - **Node WWN**

- **FCoE** Connections
  - **Profile Name**
  - **Fabric**
  - **Speed**
  - **Custom Speed**
  - **WWN Type**
  - **Port WWN**
  - **Node WWN**
  - **MAC Address Type**
  - **Ethernet MAC**

- **iSCSI** Connections
  - **Profile Name**
  - **Network**
  - **Address Type**
  - **iSCSI MAC**
  - **Speed Type**
  - **Speed**

- **Server Port Mappings**
  - **Profile Name**
  - **Port Name**
  - **Network**
  - **Uplink Set Name**
  - **VLAN ID**
4. Click OK.
5. Do one of the following:
   - To remove an entry, click the checkbox □ to the left of the entry, and click Delete, or
   - To refresh the page, click Refresh.

RMON

IMC supports the ability to configure RMON for network devices that support RMON. From the right navigation tree of the Device Details page, you can configure the following RMON groups: Statistics, History, Alarm, Event, Extension Alarm and Log.

Managing the RMON statistics group

The RMON Statistics group provides real-time statistics on LAN traffic.

Viewing RMON statistics group details

To view RMON Statistics Group details for the selected device from the Device Details page:

1. Click the RMON link located under the Device Management section of the right navigation tree on the selected device’s Device Details page.
2. Click the Statistics Group tab located at the top of the RMON Stat Group page.
   IMC displays all RMON Stat Group entries in the Stat Group list displayed in the main pane of the RMON Stat Group page.

Stat group list

- **Index**: Contains unique index values for the associated Statistics Group instance. If a MIB object contains more than one entry, indexes are used to uniquely identify each entry.
- **Port**: Contains port name/description for the associated interface.
- **Received Bytes**: Contains the number of received bytes for the associated interface for the most recent polling cycle.
- **Received Packets**: Contains the number of received packets for the associated interface for the most recent polling cycle.
- **Owner**: Contains the name of the owner of the RMON statistics collection that is configured when you add the interface to Statistics group collection.
- **Status**: Indicates whether or not the Stat Group collection is active for this interface.
- **Monitor Status**: Indicates the status of monitor for this interface.
- **At a Glance**: Shows the RMON statistics in the RMON diagram. You can select a time range to query the RMON statistics within the specified time range.

If the RMON Stat Group List contains multiple entries, the following navigational aids may appear:

- Click ▶ to page forward in the Stat Group List.
- Click ▶ to page forward to the end of the Stat Group List.
- Click ◀ to page backward in the Stat Group List.
3. Click 8, 15, 50, 100, or 200 from the right side of the main pane to configure how many items per page you want to view.
   You can only view devices that they have been granted management access to.

**Adding RMON statistics group entries**

To add interfaces to the RMON Statistics Group to enable data collection for the selected interfaces from the Device Details page:

1. Click the RMON link located under the Device Management section of the right navigation tree on the selected device’s Device Details page.
2. Click the Statistics Group tab located at the top of the RMON Stat Group page.
   IMC displays all RMON stat group entries in the Stat Group List displayed in the main pane of the RMON Stat Group page.
3. Click Add.
4. Select the port or interface you want to collect RMON statistics for from the Port list.
5. Enter the name of the person who owns this RMON Statistics Group collection in the Owner field.
6. Click OK.

Deleting RMON statistics group entries

To delete interfaces from RMON statistics group collection for the selected device:

1. Click the RMON link located under the Device Management section of the right navigation tree on the selected device’s Device Details page.
2. Click the Statistics Group tab located at the top of the RMON Stat Group page.
   IMC displays all RMON stat group entries in the Stat Group List displayed in the main pane of the RMON Stat Group page.
3. Click the checkbox associated with the ports or interfaces you want to remove from RMON Statistics Group collection.
4. Click Delete.
5. Click OK to confirm deletion of the selected interfaces.

**Managing the RMON history group**

The RMON History group defines the sampling configuration for one or more monitored interfaces.
From the RMON History group configuration window, you can configure the sampling rate for selected interfaces.

**Viewing RMON history group details**

To view RMON History Group details for the selected device from the Device Details page:

1. Click the RMON link located under the Device Management section of the right navigation tree on the selected device’s Device Details page.
2. Click the History Group tab located at the top of the RMON Stat Group page.
IMC displays all RMON history group entries in the History Group List displayed in the main pane of the RMON History Group page.

History group list fields and explanations

- **Index**: Contains unique index values for the associated history collection instance. If a MIB object contains more than one entry, indexes are used to uniquely identify each entry.
- **Port**: Contains port name/description for the associated interface.
- **Configured Max Samples**: Contains the maximum number of samples that are collected and retained for viewing for the given metrics.
- **Actual Max Samples**: When the Configured Max Samples is less than the max samples supported by the device, the Actual Max Samples are the same as the Configured Max Samples. When the Configured Max Samples is greater than the max samples supported by the device, the Actual Max Samples is the max number supported by the device.
- **Sampling Interval (second)**: Contains the amount, in seconds, of time between polls.
- **Owner**: Contains the name of the owner of the RMON statistics collection that is configured when you add the interface to History Group collection.
- **Status**: Indicates whether or not the history collection is active for this interface.

If the RMON History Group List contains multiple entries, the following navigational aids may appear:

- Click to page forward in the History Group list.
- Click to page forward to the end of the History Group list.
- Click to page backward in the History Group list.
- Click to page backward to the front of the History Group list.

3. Click 8, 15, 50, 100, or 200 from the right side of the main pane to configure how many items per page you want to view.
   You can only view devices that they have been granted management access to.

Adding RMON history group entries

To add interfaces to the RMON History Group to enable data collection for the selected interfaces from the Device Details page:

1. Click the RMON link located under the Device Management section of the right navigation tree on the selected device’s Device Details page.
2. Click the History Group tab located at the top of the RMON Stat Group page.
IMC displays all RMON history group entries in the History Group List displayed in the main pane of the RMON History Group page.
3. Click Add.
4. Select the port or interface you want to collect RMON statistics for from the Port list.
5. Enter the maximum number of samples IMC retains for this interface in the Configured Max Samples field. Valid range is 1–65535.
6. Enter the sampling interval in the Sampling Interval (second) field. Valid range is 1–3600.
7. Enter the name of the person who owns this RMON History Group collection in the Owner field.
8. Click OK.

Deleting RMON history group entries

To delete one or more entries from the RMON History group for the selected device from the Device Details page:

1. Click the RMON History Group link located under the Device Management section of the right navigation tree on the selected device’s Device Details page.
2. Click the History Group tab located at the top of the RMON Stat Group page.
   IMC displays all RMON history group entries in the History Group list displayed in the main pane of the RMON History Group page.
3. Click the checkbox associated with the ports or interfaces you want to remove from RMON History Group collection.
4. Click Delete.
5. Click OK to confirm deletion of the selected interfaces.

Managing the RMON alarm group

The RMON Alarm Group defines when SNMP traps are sent based on collection samples that exceed defined thresholds. From the RMON Alarm Group configuration window, you can configure sampling types and rates as well as rising and falling thresholds for selected interfaces.

Once a condition is met to generate an SNMP trap, the device forwards the trap to the trap destination configured in the SNMP settings on it. For information on configuring the SNMP trap destination, refer to the device vendor’s documentation.

Viewing RMON alarm group details

To view RMON Alarm Group details for the selected device from the Device Details page:

1. Click the RMON link located under the Device Management section of the right navigation tree on the selected device’s Device Details page.
2. Click the Alarm Group tab located at the top of the RMON Stat Group page.
   IMC displays all RMON alarm group entries in the Alarm Group list displayed in the main pane of the RMON Alarm Group page.

Alarm group list

- **Index**: Contains unique index values for the associated alarm. If a MIB object contains more than one entry, indexes are used to uniquely identify each entry.
- **Item**: Contains the metric that is measured by this alarm instance.
- **Port**: Contains a port name/description for the associated interface.
- **Sampling Type**: Identifies whether or not the value of the sample to be measured should be evaluated in an absolute sense or in a comparative sense. Absolute sampling measures the current sampling value accumulated since the system started up. Comparative sampling, also referred to as delta sampling, measures the value by subtracting the last absolute sampling value from the current absolute sampling value. The sampling interval is also a factor in comparative or delta sampling. Generally, delta or comparative sampling is selected.
- **Interval (second)**: Contains the amount, in seconds, of time between polls.
- **Current Sampling Value**: Contains the value for the most recent sample.
- **Startup Type**: Contains the type of threshold being used by the alarm instance. Three alarm startup types are available: allowing rising and falling alarms, allowing rising alarms and allowing falling alarms.
- **Rising Threshold**: Contains the rising threshold value. A rising threshold defines the value that the sampled value must exceed in order to generate an alarm.
- **Falling Threshold**: Contains the falling threshold value. A falling threshold defines the value that the sampled value must fall below in order to generate an alarm.
- **Rising Event Index**: Contains the index for a rising event.
- **Falling Event Index**: Contains the index for a falling event.
- **Owner**: Contains the name of the owner of the RMON statistics collection that is configured when you add the interface to **Alarm Group** collection.
- **Status**: Indicates whether or not the alarm instance is active.

If the **RMON Alarm Group** list contains multiple entries, the following navigational aids may appear:
- Click **»** to page forward in the **Alarm Group** list.
- Click **»** to page forward to the end of the **Alarm Group** list.
- Click **»** to page backward in the **Alarm Group** list.
- Click **»** to page backward to the front of the **Alarm Group** list.

3. Click 8, 15, 50, 100, or 200 from the right side of the main pane to configure how many items per page you want to view.
   You can only view devices that they have been granted management access to.

### Adding RMON alarm group entries

To add an alarm instance to the RMON Alarm Group for the selected interfaces on the device from the **Device Details** page:

1. Click the **RMON Alarm** link located under the **Device Management** section of the right navigation tree on the selected device’s **Device Details** page.
2. Click the **Alarm Group** tab located at the top of the **RMON Stat Group** page.
   IMC displays all RMON alarm group entries in the **Alarm Group** list displayed in the main pane of the **RMON Alarm Group** page.
3. Click **Add**.
4. Select the metric you want to alarm for from the **Item** list.
5. Select the port or interface you want to collect RMON statistics for from the **Port** list.
   To enable alarming on an interface, you must have configured statistics collection for it. For information on configuring an interface for RMON Statistics Group collection, see "Managing the RMON statistics group" (page 249).
6. Select the sampling type you want to use from the **Sampling Type** list.
   There are two sampling type options: **Absolute Value** and **Comparative Value**. Absolute sampling measures the current sampling value accumulated since the system started up.
Comparative sampling also referred to as delta sampling, measures the value by subtracting the last absolute sampling value from the current absolute sampling value. The sampling interval is also a factor in relative or delta sampling. Typically, delta or comparative sampling is selected.

7. Enter the sampling interval in the **Interval (second)** field. Valid range is 5-65535.

8. Do one of the following:
   - Select **Yes** from the **Create Default Event** list if you want to create a default event to generate an alarm, or
   - Select **No** from the **Create Default Event** list if you do not want to create a default event to generate an alarm.

9. Enter the rising threshold value in the **Rising Threshold** field.
   A rising threshold defines the value that the sampled value must exceed in order to generate an alarm.

10. Enter the falling threshold value in the **Falling Threshold** field.
    A falling threshold defines the value that the sampled value must fall below in order to generate an alarm.

11. Select the rising event index from the **Rising Event Index** list.

12. Select the falling event index from the **Falling Event Index** list.
    You must select **No** from the **Create Default Event** list to configure the Rising and Falling Event Index settings.

13. Enter the name of the person who owns this RMON Alarm Group collection in the **Owner** field.

14. Click **OK**.

### Deleting RMON alarm group entries

To delete alarm instances from the RMON Alarm Group for the selected device from the **Device Details** page:

1. Click the ![RMON](image) link located under the **Device Management** section of the right navigation tree on the selected device’s **Device Details** page.

2. Click the **Alarm Group** tab located at the top of the **RMON Stat Group** page.
   IMC displays all RMON alarm group entries in the **Alarm Group** list displayed in the main pane of the **RMON Alarm Group** page.

3. Click the checkbox □ associated with the alarm instance you want to remove from RMON Alarm Group collection.

4. Click **Delete**.

5. Click **OK** to confirm deletion of the instances.

### Viewing invalid RMON alarm details

IMC displays all alarms that returned a null value in the **Invalid RMON Alarm** table.

To view RMON invalid alarm details for the selected device from the **Device Details** page:
1. Click the RMON link located under the Device Management section of the right navigation tree on the selected device’s Device Details page.

2. Click the Alarm Group tab located at the top of the RMON Alarm Group page.

3. Click Invalid Item located at the top of the Alarm Group table.

   IMC displays all RMON invalid alarm entries in the Invalid RMON Alarm list on the RMON Alarm Group page.

Alarm group list

- **Index**: Contains unique index values for the associated alarm.
- **Item**: Contains the metric that is measured by this alarm instance.
- **Port**: Contains the port name/description for the associated interface.
- **Sampling Type**: Identifies whether or not the value of the sample to be measured should be evaluated in an absolute sense or in a comparative sense. Absolute sampling measures the current sampling value accumulated since the system started up. Comparative sampling, also referred to as delta sampling, measures the value by subtracting the last absolute sampling value from the current absolute sampling value. The sampling interval is also a factor in comparative or delta sampling. Generally, delta or comparative sampling is selected.
- **Interval (second)**: Contains the amount, in seconds, of time between polls.
- **Current Sampling Value**: Contains the value for the most recent sample.
- **Startup Type**: Contains the type of threshold being used by the alarm instance. Three alarm startup types are available: allowing rising and falling alarms, allowing rising alarms and allowing falling alarms.
- **Rising Threshold**: Contains the rising threshold value. A rising threshold defines the value that the sampled value must exceed in order to generate an alarm.
- **Falling Threshold**: Contains the falling threshold value. A falling threshold defines the value that the sampled value must fall below in order to generate an alarm.
- **Rising Event Index**: Contains the index for a rising event.
- **Falling Event Index**: Contains the index for a falling event.
- **Owner**: Contains the name of the owner of the RMON statistics collection that is configured when you add the interface to Alarm Group collection.
- **Status**: Indicates whether or not the alarm instance is active.
- **Reason for Null**: Contains the cause for the null value for the associated alarm group entry.

If the Invalid RMON Alarm list contains multiple entries, the following navigational aids may appear:

- Click to page forward in the Invalid RMON Alarm list.
- Click to page forward to the end of the Invalid RMON Alarm list.
- Click to page backward in the Invalid RMON Alarm list.
- Click to page backward to the front of the Invalid RMON Alarm list.

4. Click 8, 15, 50, 100, or 200 from the right side of the main pane to configure how many items per page you want to view.

   You can only view devices that they have been granted management access to.
Managing the RMON event group

The RMON Event Group provides you with the ability to define the events that generate event log entries and send SNMP traps to a management workstation. Events can originate from a crossed threshold on any RMON variable.

Viewing RMON event group details

To view RMON Event Group details for the selected device from the Device Details page:

1. Click the RMON link located under the Device Management section of the right navigation tree on the selected device’s Device Details page.
2. Click the Event Group tab located at the top of the RMON Stat Group page.

IMC displays all RMON event group entries in the Event Group list displayed in the main pane of the RMON Event Group page.

RMON event group list

- **Event Index**: Contains a unique index for the associated event instance.
- **Description**: Contains a description for the event.
- **Type**: Identifies the action that is taken by the RMON agent when an event has occurred: Log to an event log, send an SNMP trap or both.
- **Trap Community**: Contains the community string of the trap destination device. This value is included in the trap that is sent to the management station receiving the trap. Therefore, this value must match the Trap community string setting on the management station.
- **Last Trigger Time**: Contains the date and time stamp for the last occurrence of an event.
- **Owner**: Contains the name of the owner of the RMON statistics collection that is configured when you add the interface to Event Group collection.
- **Status**: Indicates whether or not the event instance is active.

If the RMON Event Group list contains multiple entries, the following navigational aids may appear:

- Click to page forward in the RMON Event Group list.
- Click to page forward to the end of the RMON Event Group list.
- Click to page backward in the RMON Event Group list.
- Click to page backward to the front of the RMON Event Group list.

3. Click 8, 15, 50, 100, or 200 from the right side of the main pane to configure how many items per page you want to view.

You can only view devices that they have been granted management access to.

Adding RMON event group entries

To add event instances for the RMON Event Group for the selected device from the Device Details page:

1. Click the RMON link located under the Device Management section of the right navigation tree on the selected device’s Device Details page.
2. Click the Event Group tab located at the top of the RMON Stat Group page.
IMC displays all RMON event group entries in the **RMON Event Group** list displayed in the main pane of the **RMON Event Group** page.

3. Click **Add**.

4. Enter a description for this event in the **Description** field.

5. Select the action to be taken for this event from the **Type** list. Options include sending a **None, Log, SNMP Trap, and Both**.

6. Enter the community string for the management station that receives the traps in the **Trap Community** field.
   The value entered in the **Trap Community** field must match what is configured on the management station that receives the traps.

7. Enter the name of the person who owns this RMON Event Group collection in the **Owner** field.

8. Click **OK**.

**Deleting RMON event group entries**

To delete event instances from RMON Event Group collection for the selected device:

1. Click the 📱 **RMON** link located under the **Device Management** section of the right navigation tree on the selected wireless device’s **Device Details** page.

2. Click the **Event Group** tab located at the top of the **RMON Stat Group** page.
   IMC displays all RMON Event Group entries in the **Event Group** list displayed in the main pane of the **RMON Event Group** page.

3. Click the checkbox ☐ associated with the alarm instance you want to remove from RMON Event Group collection.

4. Click **Delete**.

5. Click **OK** to confirm deletion of the selected events.

**Viewing the invalid event list details**

IMC provides you with a list of invalid RMON events and the cause for the invalidation. To view RMON Invalid Event List details for the selected device from the **Device Details** page:

1. Click the 📱 **RMON** link located under the **Device Management** section of the right navigation tree on the selected device’s **Device Details** page.

2. Click the **Event Group** tab located at the top of the **RMON Stat Group** page.

3. Click the **Invalid Item** button located at the top of the **Event Group** list.
   IMC displays all RMON invalid event entries in the **Invalid Event Item** list on the RMON Event Group page.

**Invalid event list**

- **Event Index**: Contains a unique index for the associated event instance.
- **Description**: Contains a description for the event.
- **Type**: Identifies the action that is taken by the RMON agent when an event has occurred: Log to an event log, send an SNMP trap or both.
- **Trap Community**: Contains the community string of the trap destination device. This value is included in the trap that is sent to the management station receiving the trap. Therefore, this value must match the Trap community string setting on the management station.

- **Last Trigger Time**: Contains the date and time stamp for the last occurrence of an event.

- **Owner**: Contains the name of the owner of the RMON statistics collection that is configured when you add the interface to Event Group collection.

- **Status**: Indicates whether or not the event instance is active.

- **Reason for Null**: Indicates the cause for the invalidation of the entry in the Invalid Event List.

If the **Invalid Event Item** list contains multiple entries, the following navigational aids may appear:

- Click ➔ to page forward in the **Invalid Event Item** list.
- Click ➔ to page forward to the end of the **Invalid Event Item** list.
- Click ➔ to page backward in the **Invalid Event Item** list.
- Click ➔ to page backward to the front of the **Invalid Event Item** list.

4. Click 8, 15, 50, 100, or 200 from the right side of the main pane to configure how many items per page you want to view.

You can only view devices that they have been granted management access to.

**Managing the RMON extension alarm group**

The RMON Extension Alarm Group is an extension to the RMON Alarm Group developed by HP, designed to support alarm configuration for a single object as well as for the object expression. This group also supports interface configuration and configurations for any valid index instance value. With the extension alarm group management, you can add or delete an RMON extension alarm group, refresh the data for the current group’s view and view invalid RMON extension alarm groups.

**Viewing RMON extension alarm group details**

To view RMON Extension Alarm Group details for the selected device from the **Device Details** page:

1. Click the 🔄 RMON link located under the **Device Management** section of the right navigation tree on the selected device’s **Device Details** page.

2. Click the **Extension Alarm Group** tab located at the top of the RMON Stat Group page.

IMC displays all RMON extension alarm group entries in the **Extension Alarm Group** list in the main pane of the **RMON Extension Alarm Group** page.

**Extension alarm group list**

- **Index**: Contains unique index values for the associated alarm. If a MIB object contains more than one entry, indexes are used to uniquely identify each entry.

- **Item**: Contains the metric that is measured by this alarm instance.

- **Sampling Object Expression**: Several formulas composed of OIDs and arithmetic expressions are provided in the Extension Alarm Group. Alarms are generated based on the results of the operation.

- **Port**: Contains port name/description for the associated interface.
- **Alarm Sampling Type**: Identifies how the value of the sample to be measured. There are three sampling types: absolute, delta, and speed sampling. Absolute sampling measures the current sampling value accumulated since the system started up. Delta sampling, also referred to as comparative or relative sampling, measures the value by subtracting the last absolute sampling value from the current absolute sampling value. Speed sampling refers to the delta sampling value per unit of time, that is, the delta sampling value divided by the sampling interval.

- **Interval (second)**: Contains the amount, in seconds, of time between polls.

- **Alarm Value**: Contains the value for the most recent sample.

- **Alarm Startup Type**: Contains the type of threshold being used by the alarm instance. Three alarm startup types are available: allowing rising and falling alarms, allowing rising alarms and allowing falling alarms.

- **Rising Threshold**: Contains the rising threshold value. A rising threshold defines the value that the sampled value must exceed in order to generate an alarm.

- **Falling Threshold**: Contains the falling threshold value. A falling threshold defines the value that the sampled value must fall below in order to generate an alarm.

- **Rising Event Index**: Contains the index for a rising event.

- **Falling Event Index**: Contains the index for a falling event.

- **Stat. Type**: Contains two statistics period types in the Extension Alarm Group: **Permanent** and **Periodic**.

  - Selecting a **Permanent Stat. Type** creates a permanent group with a sampling interval that is based on the configured interval.

  - Selecting a **Periodic Stat. Type** creates a temporary statistical collection group. Therefore, if **Periodic** is selected, the **Stat. Period** must be specified (> Interval). The collection group disappears after the **Stat. Period** has expired.

- **Stat. Period**: Contains the number of samples IMC must collect for a **Periodic Stat. Group** for the group expires.

- **Owner**: Contains the name of the owner of the RMON statistics collection that is configured when you add the interface to Extension Alarm Group collection.

- **Status**: Indicates whether or not the alarm instance is active.

If the **RMON Extension Alarm Group** list contains multiple entries, the following navigational aids may appear:

- Click to page forward in the **Extension Alarm Group** list.

- Click to page forward to the end of the **Extension Alarm Group** list.

- Click to page backward in the **Extension Alarm Group** list.

- Click to page backward to the front of the **Extension Alarm Group** list.

3. Click 8, 15, 50, 100, or 200 from the right side of the main pane to configure how many items per page you want to view.

   You can only view devices that they have been granted management access to.
Adding RMON extension alarm group entries

To add an alarm instance for the RMON Extension Alarm Group for the selected interfaces on the device:

1. Click the RMON link located under the Device Management section of the right navigation tree on the selected device’s Device Details page.
2. Click the Extension Alarm Group tab located at the top of the RMON Stat Group page.
   IMC displays all RMON extension alarm group entries in the Extension Alarm Group list displayed in the main pane of the RMON Extension Alarm Group page.
3. Click Add.
4. Select the metric you want to alarm for from the Item list.
5. Select the port or interface you want to collect RMON statistics for from the Port list.
6. Select the sampling type you want to use from the Alarm Sampling Type list.
   There are three sampling types: absolute, delta, and speed sampling. Absolute sampling measures the current sampling value accumulated since the system started up. Delta sampling, also referred to as comparative or relative sampling, measures the value by subtracting the last absolute sampling value from the current absolute sampling value. Speed sampling refers to the delta sampling value per unit of time, that is, the delta sampling value divided by the sampling interval.
7. Enter the sampling interval in the Interval (second) field.
   The valid range is 10-65535.
8. Do one of the following:
   o Select Yes from the Create Default Event list if you want to create a default event, or
   o Select No from the Create Default Event list if you do not want to create a default event.
9. Enter the rising threshold value in the Rising Threshold field.
   A rising threshold defines the value that the sampled value must exceed in order to generate an alarm.
10. Enter the falling threshold value in the Falling Threshold field.
    A falling threshold defines the value that the sampled value must fall below in order to generate an alarm.
11. Select the rising event index from the Rising Event Index list.
12. Select the falling event index from the Falling Event Index list.
    You must select No from the Create Default Event list to configure the Rising and Falling Event Index settings.
    When a value greater than 0 is entered as the Rising Event Index value and 0 is entered as the Falling Event Index value, the Alarm Startup Type is a rising alarm. When 0 is entered as the Rising Event Index and a value greater than 0 is entered as the Falling Event Index, the Alarm Startup Type is a falling alarm.
14. Do one of the following:
o Select **Permanent** if you want to create a permanent group with a sampling interval that is based on the configured interval, or

o Select **Periodic** if you want to create a temporary statistical collection group. The collection group disappears after the **Stat. Period** interval has expired.

15. If you selected **Permanent** in the **Stat. Type** field, enter the **Stat. Period** value in the **Stat. Period** field.

   The valid range is 0-2147483647.

16. Enter the name of the person who owns this RMON Extension Alarm Group collection in the **Owner** field.

17. Click **OK**.

**Deleting RMON extension alarm group entries**

To delete alarm instances from the RMON Extension Alarm Group for the selected device:

1. Click the ![RMON](#) link located under the **Device Management** section of the right navigation tree on the selected device’s **Device Details** page.

2. Click the **Extension Alarm Group** tab located at the top of the **RMON Stat Group** page.

   IMC displays all RMON extension alarm group entries in the **Extension Alarm Group** list in the main pane of the **RMON Extension Alarm Group** page.

3. Click the checkbox ![ ] associated with the alarm instance you want to remove from RMON Extension Alarm Group collection.

4. Click **Delete**.

5. Click **OK** to confirm deletion of the selected interfaces.

**Managing the RMON log**

The RMON Log enables you to view log entries that are triggered by events configured in the RMON MIB in the Alarm Group and the Extension Alarm Group.

**Viewing RMON log details**

To view the RMON Log details for the selected device:

1. Click the ![RMON](#) link located under the **Device Management** section of the right navigation tree on the selected device’s **Device Details** page.

2. Click the **Log** tab located at the top of the RMON Stat page.

   IMC displays all RMON log entries in the **Log** list in the main pane of the **RMON Log** page.

**Log list fields and explanations**

- **Event Index**: Contains a unique index value for the event associated with the log entry.
- **Log Index**: Contains a unique index value for the log entry.
- **Log Time**: Contains a date and time stamp for the log entry.
- **Log Description**: Contains information about the event.

If the **RMON Log Group** list contains multiple entries, the following navigational aids may appear:
Click to page forward in the Log list.
Click to page forward to the end of the Log list.
Click to page backward in the Log list.
Click to page backward to the front of the Log list.

3. Click 8, 15, 50, 100, or 200 from the right side of the main pane to configure how many items per page you want to view.
You can only view devices and their components that they have been granted management access to.

Protocol Management
IMC provides you with visibility into various protocol information and configuration settings. Note that the menu varies with the protocols supported by the device.

RIP browsing for routers
From the RIP link under Protocol Management, you can view RIP information for the selected router. The information provided in this view includes RIP Interface Configuration, RIP Interface Statistics and RIP Peer Information.
To access RIP browsing from the Device Details page:
1. Click the RIP link located under the Protocol Management section of the right navigation tree on the selected device’s Device Details page.
2. Use the RIP Interface Configuration, RIP Interface Statistics and RIP Peer Information tabs located at the top of the RIP page to navigate to the information page you wish you view.

BGP browsing for routers
From the BGP link under Protocol Management, you can view BGP information for the selected router. The information provided in this view includes BGP Attribute, Basic Information, Statistic Information, Time Attribute, BGP4 Path Information.
To access BGP browsing from the Device Details page:
1. Click the BGP link located under the Protocol Management section of the right navigation tree on the selected device’s Device Details page.
2. Use the BGP Attribute, Basic Information, Statistic Information, Time Attribute, BGP4 Path Information tabs located at the top of the BGP page to navigate to the information page you wish you view.

OSPF browsing for routers
From the OSPF link under Protocol Management, you can view OSPF information for the selected router. The information provided in this view includes OSPF Attribute, Area Information, Stub Area Information, LSDB Information, Extended LSDB Information, OSPF Interface, Interface TOS Metric, Peer Information, Virtual Link Interface and Virtual Link Peer information.
To access OSPF browsing from the Device Details page:
1. Click the OSPF link located under the Protocol Management section of the right navigation tree on the selected device’s Device Details page.

2. Use the OSPF Attribute, Area Information, Stub Area Information, LSDB Information, Extended LSDB Information, OSPF Interface, Interface TOS Metric, Peer Information, Virtual Link Interface and Virtual Link Peer tabs located at the top of the OSPF page to navigate to the information page you wish you view.

### Managing MSTP options for routers and switches

IMC provides you with the ability to configure Multiple Spanning Tree Protocol (MSTP) options for both routers and switches. From the MSTP link under Protocol Management, you can configure the MSTP options for the selected router or switch.

#### Configuring global MSTP settings

To configure Global MSTP settings from the Device Details page:

1. Click the MSTP link located under the Protocol Management section of the right navigation tree on the selected router or switch’s Device Details page.

2. Click the Global MSTP tab located at the top of the page to navigate to the Global MSTP page.

3. To enable MSTP on the selected switch or router, select Enable from the MSTP Status list.

4. Select the Spanning Tree Protocol version you want to apply to this device from the MSTP Type list. Options include STP, RSTP, and MSTP.

   STP BPDUs and RSTP BPDUs can be recognized and used for spanning tree calculation on MSTP-enabled switches.

5. Enter the Spanning Tree diameter in the Diameter field. A valid range for diameter is 2-7.

   This option configures the network diameter of a switched network. The network diameter parameter indicates the size of a network. The bigger the network diameter is, the larger the network size is.

6. Enter the maximum number of hops in the Max Hops field.

   The value of maximum hops limits the size of the MST region. The maximum hop count configured on the region root also acts as the maximum hop count of the MST region. The larger the maximum hop count of an MST region is, the larger the scale of the MST region is.

   The scale of an MST region can be limited only when the maximum hop count is configured for the root switch of the MST region. Other switches in the MST region adopt the configuration on the region root, even if the switch configuration is different.

7. If you want to enable BPDU protection, select Enable from the BPDU Protection list.

   For access layer devices, the access port is usually connected to the user terminal (such as PC) or the file server. In this case, the access port is configured as an edge port to implement fast migration. When these ports receive BPDU, the system automatically configures these ports as non-edge ports and re-calculates the spanning tree, causing network topology instability.

   Under normal conditions, these ports should not receive STP BPDU. If someone forges BPDU maliciously to attack the switch, network topology instability occurs. You can prevent this type of attacks by utilizing the BPDU guard function. This configuration item can be Enable or Disable. By default, BPDU guard is disabled on a switch.

8. If needed, modify the name for the STP admin region in the Admin Region Name field.
By default, the MST region name is the first MAC address of the MST region switch.

9. If needed, modify the admin revision level in the **Admin Revision Level** field. The valid range is 0-65535. All VLANs in the MST region belong to spanning tree instance 0, and the revision level of the MST region is 0.

10. Click **Config** to accept any changes you have made to the Global MSTP settings.
   a. Click **Apply** to apply the existing global MSTP settings.
   b. Click **Default VLAN** to reset the VLANs to their default settings, which configures all VLANs to spanning tree instance 0.
   c. Click **Default Region** to reset the region parameters to their default settings. This restores the MST region name to its default.
     When you configure the parameters related to the MST region, especially the VLAN-to-instance mapping table, network topology instability can result. To reduce such instability caused by configuration changes, MSTP does not immediately trigger the re-calculation of the spanning tree upon processing the region-related configurations. The region-related configurations take effect only when MSTP is enabled.
   d. Click **Close** when you have finished configuring the Global MSTP settings.

   For more information on configuring **Spanning Tree**, refer to your switch vendor’s documentation.

### Modifying MSTI settings

To modify the configuration of **Multiple Spanning Tree Instance (MSTI)** settings:

1. Click the **MSTP** link located under the **Protocol Management** section of the right navigation tree on the selected router or switch’s **Device Details** page.
2. Click the **MSTI** tab located at the top of the page to navigate to the **MSTI** page.
3. Locate the MSTI instance you want to modify from the list provided.
4. Click the **Modify** icon associated with the instance you want to modify.
5. Select the bridge priority for this instance from the **Priority** list.
   The priority of a bridge determines whether or not the bridge can be elected as the root of the spanning tree. You can force a specific switch serve as the root bridge by setting a low value for the bridge priority for the switch. An MSTP-enabled switch may have different bridge priorities in different spanning tree instances. The bridge priority of a switch is 32768 by default.
6. Select the root type for this instance from the **Root Type** list.
   Configuring the network bridge root type assigns priority to the switch for the purposes of determining the root bridge. The root type can be **Normal**, **Secondary**, or **Primary**. **Normal** sets the priority to 32768, **Primary** sets the priority to 0, and **Secondary** sets the priority to 4096. A bridge with a lower priority value is more likely to be elected as the root bridge. By default, the role of a bridge is **Normal**.
   When the **Root Type** is set to **Primary** or **Secondary**, the bridge **Priority** cannot be set.
7. Enter the Admin VLAN ID for this instance in the **Admin VLAN ID** field. You can enter more than one VLAN ID. Separate each VLAN ID with a comma (,). You can also enter VLAN IDs by range, using a dash (-) between the beginning and ending of the VLAN ID range.
Admin VLAN ID is used to tie an MSTI to a specific VLAN. The configured VLAN-to-instance mapping does not take effect until MSTP is enabled.

8. Click OK to accept your changes.
9. Click Close to close the MSTI window.

For more information on configuring the Spanning Tree feature, refer to your switch vendor’s documentation.

Modifying port MSTP settings

To modify port configuration of the Multiple Spanning Tree Protocol (MSTP) settings:

1. Click the MSTP link located under the Protocol Management section of the right navigation tree on the selected router or switch’s Device Details page.
2. Click the Port MSTP tab located at the top of the page to navigate to the Port MSTP page.
3. Locate the port you want to modify the MSTP settings for from the list provided.
4. Click the Modify icon associated with the instance you want to modify.
5. Select the port priority for the selected port from the Priority list.
   The priority of a port is an important factor in determining whether the port can be elected as the root port of a device during the spanning tree calculation process. If all other conditions are equal, the port with the highest priority is elected as the root port. On an MSTP-enabled device, a port can have different priorities in different MSTIs, and the same port can play different roles in different MSTIs, so that data of different VLANs can be propagated along different physical paths, thus implementing per-VLAN load balancing. When the priority of a port is changed, MSTP re-computes the role of the port and initiate a state transition. Generally, a configured lower priority value indicates a higher priority of the port. If all the ports of a switch have the same port priority value, the port priorities are determined by the port indexes. You can set port priority values based on the actual networking requirements. The default port priority is 128.
6. Enter the path cost to the root bridge in the Path Cost to Root Bridge field.
   The Path Cost to Root Bridge parameter is related to the rate of port-connected links. On a switch supporting MSTP, the port may have varying path costs in different spanning tree instances so that traffic from different VLANs can be forwarded along different physical links to implement per-VLAN load sharing. By default, MSTP calculates the path cost of each port.
7. To enable CIST Edge Port, select Enable from the CIST Edge Port field.
   The CIST Edge Port option is only applicable when the MSTI is a CIST. Edge port indicates that the port is neither directly connected to any switch nor indirectly connected to any switch through the port-connected network. When the operator specifies one port as the edge port and when the port migrates from the congestion state to the forwarding state, fast migration can be implemented without any delay. The user can only configure the port connecting the terminal as the edge port. If BPDUs from other ports are received on the edge port, the port becomes a non-edge port again. This parameter is valid for all spanning tree instances. In other words, when the port is configured as an edge port or non-edge port, the port is configured as an edge port or non-edge port on the CIST and all MSTIs. When the port receives BPDUs, the port actually operates as a non-edge port even if it is configured as the edge port by the operator. By default, all Ethernet ports of a switch are non-edge ports.
8. Select the CIST Port Point-to-Point configuration from the CIST Port Point-to-Point list.
Point-to-Point link generally refers to the link between switches. The two ports in a point-to-point link can be quickly migrated to the forwarding state by transmitting synchronous packets, thus reducing forwarding delay. If this option is configured for automatic mode, MSTP can automatically detect whether the current Ethernet port is connected to a point-to-point link. Note that for an aggregation port, only the link type of the aggregation group can be configured as point-to-point. If a port operates in the auto-negotiation mode and the negotiated operation mode is the full duplex mode, the link type of the port can be configured as point-to-point. The configuration is valid for the CIST and all MSTIs. If the actual physical link of a port is not a point-to-point link and you forcibly configure the link as a point-to-point link, temporary loops may occur. By default, this parameter is auto.

9. Enter the value for transmission limit for this port in the Trans Limit field.

The Trans Limit option is related to the physical state and the network structure of the port. You can configure the maximum transmitting rate as needed. Note that the larger the Trans Limit setting, the more packets are sent per unit time, consequently consuming more network bandwidth and resources. HP recommends retaining the default setting. By default, the maximum transmission rate for all Ethernet ports on a switch is 10.

10. To disable a port’s participation in Spanning Tree calculations, select Disable from the Port MSTP Status field to reduce CPU utilization on the switch.

11. To enable root bridge protection, select Enable from the Root Protection list.

The root switch and backup switch of the spanning tree should be located in the same region, especially the root switch and backup switch of the CIST. Generally, the root switch and backup switch of the CIST is placed in the core region of high bandwidth upon network design. Sometimes, due to device configuration errors or malicious attacks by users, the current valid root switch may receive configuration messages with a higher priority. When this occurs, the current root switch loses its status as the root switch. This causes an invalid change of the network topology structure. Such invalid changes may cause traffic, which should be transmitted over the high-speed link, to be transmitted over the low-speed link, resulting in network congestion. You can avoid this problem by enabling the root guard function. For a port configured with the root guard function, it can only be the designated port. Once this port receives BPDUs with a higher priority, it is selected as a non-designated port and enters the discarding state and no longer forwards packets. When the priority of the received BPDUs is lower than that of the local BPDUs, the port automatically migrates from the listening state, via the intermediate state, to the normal forwarding state. The root guard function is disabled by default.

12. Click OK.

For more information on configuring Spanning Tree, refer to your switch vendor’s documentation.

Forcing port migration to MSTP mode

From the Port MSTP window, you can force a switch port to operate in MSTP mode. Ports on an MSTP-enabled switch can operate in STP-compatible mode or MSTP mode. In a switched network, if a port on the device running MSTP connects to a device running STP, this port automatically migrates to the STP-compatible mode. However, if the device running STP is removed, this cannot migrate automatically to the MSTP mode, but remains working in the STP-compatible mode.

To force a port to migrate to MSTP mode:
1. Click the MSTP link located under the Protocol Management section of the right navigation tree on the selected router or switch’s Device Details page.

2. Click the Port MSTP tab located at the top of the page to navigate to the Port MSTP page.

3. Locate the port you want to modify the MSTP settings for from the list provided.

4. Click the icon in the Mcheck field associated with the instance you want to modify.

5. Click OK to confirm this configuration change.

Clearing MSTP statistics entries
To clear the MSTP statistics entries:

1. Click the MSTP link located under the Protocol Management section of the right navigation tree on the selected router or switch’s Device Details page.

2. Click the Port MSTP tab located at the top of the page to navigate to the Port MSTP page.

3. Locate the port you want to clear statistics for from the list provided.

4. Click the icon in the Clear Statistics field associated with the instance you want to clear statistics for.

5. Click OK to confirm clearing the statistics for the selected port.

Restoring default settings for path cost
From the Port MSTP window, you can also restore the default settings for path cost of each port.

1. Click the MSTP link located under the Protocol Management section of the right navigation tree on the selected router or switch’s Device Details page.

2. Click the Port MSTP tab located at the top of the page to navigate to the Port MSTP page.

3. Locate the port you want to modify the MSTP settings for from the list provided.

4. Click the Configure icon in the Default Port Cost field associated with the instance you want to restore default settings to.

5. Click OK to confirm this configuration change.

IGMP snooping
IMC provides you with the ability to configure IGMP snooping options for devices. To configure IGMP Snooping settings from the Device Details page:

1. Click the IGMP Snooping configuration link located under the Protocol Management section of the right navigation tree on the selected wireless device’s Device Details page.

   The IGMP Snooping Configuration page appears.

2. To enable IGMP Snooping on the selected wireless device, select Enable from the IGMP Snooping Status list.

3. Enter the aging time of the router port in seconds in the Aging Time of Router Port field.

   The routing port should be deleted from all port members of the MAC multicast group if IGMP general queries are not received within the aging time of routing port. By default, the aging time of a routing port is 105 seconds.

4. Enter the maximum response time for queries in the Maximum Response Time of Query field.
If no IGMP reports are received within the query response time, the port is removed from the multicast member ports. By default, the maximum response time to IGMP queries is 10 seconds.

5. Enter the aging time for the multicast port in the Aging Time of multicast Port field.
   If no multicast report is received on a port within the aging time of the port, group-specific queries are sent to the port. By default, the aging time of a multicast port is 260 seconds.

6. Click OK to confirm the IGMP settings.
   IGMP snooping and GMRP are mutually exclusive. You cannot enable IGMP snooping while GMRP is enabled.

**VLAN management**

IMC provides you with the ability to configure VLAN on managed devices. The VLAN Management menu options are the shortcuts to the VLAN Management→VLAN Devices menu options located on the left navigation tree under the Service tab. For more information on configuring VLAN for a specific device, see "VLAN device management" (page 830).

**Interface details**

From the Device Details page, you can navigate to the Interface Details page. From the Interface Details page, you can view interface information including status and speed as well as perform interface related actions.

**Accessing the interface list and interface details page**

There are many ways to access the Interface List. The most straightforward way to access the Interface Details page is through the individual device’s Device Details page.

To access the Interface List and Interface Details page:

1. Navigate to Resources→Device Name→Interface List.
   a. Click the Resource tab from the tabular navigation system on the top.
   b. Click View Management on the navigation tree on the left.
   c. Click Device View under View Management from the navigation system on the left.
   The Device List – All appears, listing all devices in IMC.

2. Locate the device you want to view interface details for and click the link in the Device Label column in the Device List for the device you want to view interface details for.
   The Device Details page appears.

3. Click the Interface List link in the Interfaces field of the Device Details section for the selected device.
   The Interface List appears, with all interfaces for the selected device shown in the main pane of the page.

**Interface list**

- **Interface Status:** Contains an active icon indicating the current up/down status for the associated interface.
- **Interface Index:** Contains a unique index for the associated interface.
- **Interface Description:** Contains a description of the associated interface. The entry in the description field serves as a link to the Interface Details page.
- **Interface Alias**: Contains the name of the interface that has been configured on the device. For information on configuring interface alias, refer to the vendor’s documentation.

- **Interface IP**: Contains the IP address for the associated interface.

- **Speed (bps)**: Contains the speed, in bits per second of the associated interface.

If the **Interface Group** list contains multiple entries, the following navigational aids may appear:

- Click ← to page forward in the **Interface List**.
- Click → to page forward to the end of the **Interface List**.
- Click ← to page backward in the **Interface List**.
- Click → to page backward to the front of the **Interface List**.

4. Click 8, 15, 50, 100, or 200 from the right side of the main pane to configure how many items per page you want to view.

You can only view devices that they have been granted management access to.

5. To access, the **Interface Details** page, click the link in the **Interface Description** field for the interface you want to view details for.

The **Interface Details** page appears.

### Interface details page

The **Interface Details** page is a rich resource that provides you and you with quick and easy access to important interface information as well as links to interface configuration options.

The **Interface Details** section provides the following information on the selected interface.

### Interface details page

- **Interface Index**: Contains the unique index value for the associated interface.
- **Interface Type**: Identifies the type of interface as defined by its physical/link protocol.
- **Interface Description**: Provides a description for the interface.
- **Management Status**: Contains an active icon denoting the current management status for the interface.
- **Operational Status**: Contains an active icon denoting the current operational status for the associated interface.
- **Speed (bps)**: Contains the speed, in bits per second of the associated interface.
- **User-Defined Speed (bps)**: Contains the user-defined speed, in bits per second of the interface.
- **Interface Alias**: Contains the name of the interface that has been configured on the device. For information on configuring interface alias, refer to the vendor’s documentation.
- **MAC Address**: Contains the MAC address for the associated interface.
- **MTU**: Contains the maximum size of IP packets processed by this interface.
- **Last Change**: Contains the time when the interface status was last changed (for example, plug/unplug the network cable).
- **Interface Up/Down Alarm Filter**: Identifies whether or not there are system defined or user defined filters in place for filtering out Interface up and down traps for the selected interface.
IP Address/Mask: Contains the IP address and subnet mask for the interface.

Interface details right navigation tree

Like the right navigation tree for the Device Details page, the Interface Details page provides quick and easy access to configuration and management tasks for the selected interface. Actions

The Action menu options enable you to apply management and configuration options to the selected interface from the convenience of the navigation tree located on the right of the Interface Details section.

Synchronize

With the Synchronize option, you can update IMC’s data on the selected interface. When an operator uses the Synchronize option, IMC queries the selected device for information on the selected interface and then updates the Interface Details page with any updated information.

To synchronize the selected interface from the Interface Details page:

1. Navigate to the Device Details page for the device you want to manage interfaces for.
   For information on navigating to a device’s Device Details page, see "Viewing devices with Device, IP, and Topology Views" (page 176) and "Viewing devices with custom views" (page 201).

2. Click the Interface List link in the Interfaces field for the interface you want to manage.
   The Interface List appears. For more information on the Interface List, see "Accessing the interface list and interface details page" (page 268).

3. From the Interface List, click the Interface Description field for the interface you want to manage.
   The Interface Details page appears.

4. Click the Synchronize link located under the Action section of the right navigation tree on the selected interface’s Interface Details page.
   The top of the Interface Details page updates to reflect the initiation of the synchronization process. Refresh this page using the Refresh option on the right navigation tree to view any updates to device data.

Refresh

With the Refresh option, you can reload the current Interface Details page and capture any updates to the interface details or other dynamic data found on this page. This feature is particularly useful when you use the Synchronize option to query the selected interface for updated information.

To refresh the selected device:

1. Navigate to the Device Details page for the device you want to manage interfaces for.
   For information on navigating to a device’s Device Details page, see "Viewing devices with Device, IP, and Topology Views" (page 176) and "Viewing devices with custom views" (page 201).

2. Click the Interface List link in the Interfaces field for the interface you want to manage.
   The Interface List appears. For more information on the Interface List, see "Accessing the interface list and interface details page" (page 268).

3. From the Interface List, click the Interface Description field for the interface you want to manage.
   The Interface Details page appears.
4. Click the ✪ Refresh link located under the Action section of right navigation tree on the selected interface’s Interface Details page.

Unmanage

You can choose to unmanage an interface. This feature is particularly useful for those interfaces that are either not in use or significant enough to warrant monitoring them.

To unmanage the selected interface from the Interface Details page:

1. Navigate to the Device Details page for the device you want to manage interfaces for.
   For information on navigating to a device’s Device Details page, see "Viewing devices with Device, IP, and Topology Views" (page 176) and "Viewing devices with custom views" (page 201).

2. Click the Interface List link in the Interfaces field for the interface you want to manage.
   The Interface List appears. For more information on the Interface List, see "Accessing the interface list and interface details page" (page 268).

3. From the Interface List, click the Interface Description field for the interface you want to manage.
   The Interface Details page appears.

4. Click the ✪ Unmanage link located under the Action section of the right navigation tree on the selected interface’s Interface Details page.
   The top of the Interface Details page updates to reflect the completion status of the unmanage task. Refresh this page using the Refresh option on the right navigation tree to view any updates to interface data.

The Manage/Unmanage link is a toggle switch between these two states:

- ✪ Manage means that the interface is currently unmanaged.
- ✪ Unmanage means that the interface is currently managed.

UP

From the Interface Details page, you can change the management status of the selected interface to UP.

1. Navigate to the Device Details page for the device you want to manage interfaces for.
   For information on navigating to a device’s Device Details page, see "Viewing devices with Device, IP, and Topology Views" (page 176) and "Viewing devices with custom views" (page 201).

2. Click the Interface List link in the Interfaces field for the interface you want to manage.
   The Interface List appears. For more information on the Interface list, see "Accessing the interface list and interface details page" (page 268).

3. From the Interface List, click the Interface Description field for the interface you want to manage.
   The Interface Details page appears.

4. Click the ✪ UP link located under the Action section of the right navigation tree on the selected interface’s Interface Details page.
   The top of the Interface Details page updates to reflect the completion status of the task.

DOWN
From the Interface Details page, you can change the management status of the selected interface to DOWN.

1. Navigate to the Device Details page for the device you want to manage interfaces for.
   For information on navigating to a device’s Device Details page, see "Viewing devices with Device, IP, and Topology Views" (page 176) and "Viewing devices with custom views" (page 201).

2. Click the Interface List link in the Interfaces field for the interface you want to manage.
   The Interface List appears. For more information on the Interface list, see "Accessing the interface list and interface details page" (page 268).

3. From the Interface List, click the Interface Description field for the interface you want to manage.
   The Interface Details page appears.

4. Click the DOWN link located under the Action section of the right navigation tree on the selected interface’s Interface Details page.
   The top of the Interface Details page updates to reflect the completion status of the task.

User-Defined Speed

From the Interface Details page, you can change the user-defined speed setting for the selected interface.

1. Navigate to the Device Details page for the device you want to manage interfaces for.
   For information on navigating to a device’s Device Details page, see "Viewing devices with Device, IP, and Topology Views" (page 176) and "Viewing devices with custom views" (page 201).

2. Click the Interface List link in the Interfaces field for the interface you want to manage.
   The Interface List appears. For more information on the Interface list, see "Accessing the interface list and interface details page" (page 268).

3. From the Interface List, click the Interface Description field for the interface you want to manage.
   The Interface Details page appears.

4. Click the User-Defined Speed link located under the Action section of the right navigation tree on the selected interface’s Interface Details page.

5. Enter the speed you want to assign to this interface in the User-Defined Speed field.

6. Select the unit of speed measurement from the list located to the right User-Defined Speed field.

7. Click OK.
   If you leave the User-defined Speed field blank, the value of N/A is applied.
   The top of the Interface Details page updates to reflect the completion status of the task. In addition, the User-Defined Speed field updates to include the configuration change.

Up/Down Alarm Filter

From the Interface Details page, you can change the Up/Down Alarm Filter status of the selected interface.

1. Navigate to the Device Details page for the device you want to manage interfaces for.
For information on navigating to a device’s Device Details page, see "Viewing devices with Device, IP, and Topology Views" (page 176) and "Viewing devices with custom views" (page 201).

2. Click the Interface List link in the Interfaces field for the interface you want to manage.

The Interface List appears. For more information on the Interface list, see "Accessing the interface list and interface details page" (page 268).

3. From the Interface List, click the Interface Description field for the interface you want to manage.

The Interface Details page appears.

4. Click the Up/Down Alarm Filter link located under the Action section of the right navigation tree on the selected interface’s Interface Details page.

The Interface Up/Down Alarm Filter page appears.

5. Select the status of up/down alarm filter you want to perform from the Interface Up/Down Alarm Filter list.

For more information on the System Settings, see "System settings" (page 144).

6. Click OK.

IP/MAC Learning Query

From the Interface Details page, you can query the IP/MAC learning for the selected interface.

For information on IP/MAC Learning Query, see "Actions - For switches" (page 222).

Interface management

The Interface Management menu options enable you to apply management and configuration options to the selected interface from the convenience of the navigation tree located on the right of the Interface Details section. Options under Interface Management include loopback testing, Interface IP Management, viewing port information and configuring ports, and adding ports to VLANs. However, the menu options available for Interface Management vary by device and interface type.

Loopback testing

From the Interface Details page, you can test the loopback interface for the selected device.

1. Navigate to the Device Details page for the device you want to manage interfaces for.

For information on navigating to a device’s Device Details page, see "Viewing devices with Device, IP, and Topology Views" (page 176) and "Viewing devices with custom views" (page 201).

2. Click the Interface List link in the Interfaces field for the interface you want to manage.

The Interface List appears. For more information on the Interface list, see "Accessing the interface list and interface details page" (page 268).

3. From the Interface List, click the Interface Description field for the interface you want to manage.

The Interface Details page appears.

4. Click the Loopback Testing link located under the Interface Management section of the right navigation tree on the selected interface’s Interface Details page.

5. Click the Port Loopback Test tab located at the top of the Loopback Test window.

6. Select the type of loopback test you want to perform from the Test Type list:
An internal test tests the reachability of the Loopback interface from an interface on the device itself, or
An external test tests the reachability of the Loopback interface from the IMC server.

7. Click OK.

The Loopback Test window updates with the results of the Loopback test.

Interface IP management

From the Interface Details page, you can configure the IP address for the selected interface.

1. Navigate to the Device Details page for the device you want to manage interfaces for.

For information on navigating to a device’s Device Details page, see "Viewing devices with Device, IP, and Topology Views" (page 176) and "Viewing devices with custom views" (page 201).

2. Click the Interface List link in the Interfaces field for the interface you want to manage.

The Interface List appears. For more information on the Interface list, see "Accessing the interface list and interface details page" (page 268).

3. From the Interface List, click the Interface Description field for the interface you want to manage.

The Interface Details page appears.

4. Click the Interface IP link located under the Interface Management section of the right navigation tree on the selected interface’s Interface Details page.

5. Click Add.

6. Enter the IP address in the IP Address field.

7. Enter the mask in the Mask field.

8. Select the type of the IP address in the Type field.

9. Click OK.

Adding ports to VLANs

From the Interface Details page, you can add the selected port to an existing VLAN.

1. Navigate to the Device Details page for the device you want to manage interfaces for.

For information on navigating to a device’s Device Details page, see "Viewing devices with Device, IP, and Topology Views" (page 176) and "Viewing devices with custom views" (page 201).

2. Click the Interface List link in the Interfaces field for the interface you want to manage.

The Interface List appears. For more information on the Interface list, see "Accessing the interface list and interface details page" (page 268).

3. From the Interface List, click the Interface Description field for the interface you want to manage.

The Interface Details page appears.

4. Click the Add to VLAN link located under the Interface Management section of the right navigation tree on the selected interface’s Interface Details page.

The Add Port to VLAN page appears.

5. Select the VLAN ID from the VLAN ID list.
The VLAN must already exist before ports can be added to it. For information on creating a VLAN in IMC, see "Creating a VLAN" (page 833).

6. Click OK.
   The Add to VLAN window updates with the results of the VLAN interface configuration.

Port properties

From the Interface Details page, you can view information for the selected interface. In addition, you can configure the selected interface from the Port Properties page. Menu options for Port Properties change based upon the device as well as the interface.

To view port information and to configure an Ethernet or Gigabit Ethernet port:

1. Navigate to the Device Details page for the device you want to manage interfaces for.
   For information on navigating to a device’s Device Details page, see "Viewing devices with Device, IP, and Topology Views" (page 176) and "Viewing devices with custom views" (page 201).

2. Click the Interface List link in the Interfaces field for the interface you want to manage.
   The Interface List appears. For more information on the Interface list, see "Accessing the interface list and interface details page" (page 268).

3. From the Interface List, click the Interface Description field for the interface you want to manage.
   The Interface Details page appears.

4. Click the Port Properties link located under the Interface Management section of the right navigation tree on the selected interface’s Interface Details page and do the following:
   a. Enter a name for the interface in the Port Alias field. Valid entry is 1-64 characters.
   b. Select the administrative status for this port from the Administrative Status list.
   c. Select the port priority from the Port Priority list.
   d. Select the speed of the port from the Configured Rate list.
   e. Select the broadcast suppression type from the Broadcast Suppression Type list.
   f. Enter the broadcast suppression value from the Broadcast Suppression field.
   g. Select the duplex mode for this interface from the Configured Duplex Mode list.
   h. Enable or disable flow control from the Flow Control Status list. To enable flow control, select True. To disable flow control, select False.
   i. Select the link type from the Link Type list. Options include Trunk, Access, Hybrid, and Fabric.
   j. Select the MDI mode from the MDI Mode list. Options include Normal, Across, and Auto.

5. Click Config to accept your changes.
   The Port Information window updates with the results of the VLAN interface configuration.
   When configuring a virtual interface, you only need to configure Port Alias and Administrative Status.

For more information on the configuration options available on the switch Port Information page, refer to your switch vendor’s documentation.
Performance Monitor

From the Interface Details page, you can monitor the performance indexes for the interface in real time. To do that,

1. Navigate to the Device Details page for the device you want to manage interfaces for.
   For information on navigating to a device’s Device Details page, see “Viewing devices with Device, IP, and Topology Views” (page 176) and “Viewing devices with custom views” (page 201).

2. Click the Interface List link in the Interfaces field for the interface you want to manage.
   The Interface List appears. For more information on the Interface list, see "Accessing the interface list and interface details page" (page 268).

3. From the Interface List, click the Interface Description field for the interface you want to manage.
   The Interface Details page appears.

4. Click the Interface Realtime Monitor link located under the Performance Monitor section of the right navigation tree on the selected interface’s Interface Details page.

5. Select an item from the Select Index list:
   a. Click the checkbox ☑ to the left of the monitor items you want to monitor, or
   b. Click the checkbox ☑ to the left of the instances you want to monitor.

6. Click OK to add the interface real-time monitor.

Managing multiple devices using batch operations

Batch Operations allow you to streamline repetitive administrative tasks by applying a single configuration to one or more devices. Configuring devices using batch operations reduces the amount of time and effort involved in managing network resources.

IMC provides batch mode support for administrative tasks including configuring SNMP, Telnet, and SSH settings, configuring status and configuration of polling intervals, and changing login types. Using batch mode, you can also check Telnet and SSH settings and perform network device configuration tasks including saving device configuration, rebooting devices, applying energy saving policies, configuring trap destinations, configuring STP, and LACP.

Using batch mode to configure SNMP settings

You can use the IMC batch mode feature to update IMC’s SNMP configuration for one or more devices within IMC but it does not modify the SNMP settings on the device itself.

To add or modify IMC’s SNMP settings for one or more devices in batch mode:

1. Navigate to Resource→Batch Operation→SNMP Settings:
   a. Click the Resource tab from the tabular navigation system on the top.
   b. Click Resource Management on the navigation tree on the left.
   c. Click 🌐 Batch Operation under Resource Management from the navigation system on the left.
d. Click the **SNMP Settings** link from the **NMS Parameter Configuration** section of the **Resource→Batch Operation** page.

2. Click the expand icon ✆ to the left of **NMS Parameter Configuration** to expand the batch operations in **NMS Parameter Configuration** section to access the **SNMP Settings** option.

3. Click **Add** to select the devices to which you want to apply the SNMP settings in the **SNMP Settings** window.
   
   You can add devices by using either the **View** or **Advanced** query option. See "Adding devices by View" (page 85) and "Adding devices by Advanced query" (page 85).

4. To configure the SNMP settings for selected devices, click the **Configuration** icon 🔗.
   
   The **SNMP Parameters** dialog box appears.
   
   You can either enter the SNMP settings in this dialog box or you can select an existing SNMP template that contains the SNMP settings for this device. SNMP templates are particularly useful when SNMP configurations are standardized. For more information on creating SNMP templates, see "SNMP templates" (page 74).

**Editing SNMP settings manually**

1. To edit the SNMP parameters, verify that the radio button ☐ to the left of **Edit SNMP Parameters** is selected.

2. Select the version of SNMP (v1 or v2c) that is configured on the device to be added from the **Parameter Type** list.
   
   You can only add devices that are configured with SNMPv3 using SNMP templates. Therefore, you must create an SNMP template with the SNMPv3 parameters for this device before adding this device. For more information on creating SNMP templates, see "SNMP templates" (page 74).

3. Enter the read-only community string in the **Read-Only Community String** field.

4. Enter the read-write community string in the **Read-Write Community String** field.

5. Enter the SNMP timeout value (1–60 seconds) in the **Timeout** field.
   
   This parameter determines how long IMC waits for an SNMP reply from the managed device before declaring that the request has timed out. The default is 4.

6. Enter the number of SNMP retries (1–20) in the **Retries** field.
   
   The retries parameter defines how many times the management system (IMC) sends SNMP retries in an attempt to communicate with the managed device before reporting a failure. The default is 3.

**Using existing SNMP templates**

1. To configure the SNMP settings for this device using an SNMP template, click the radio button ☐ to the left of **Select an Existing Template**.

2. Click the radio button ☐ to the left of the SNMP template you want to use.

3. Click **OK**.

4. Click **Configure** to apply the SNMP configuration settings to the selected devices.
   
   The **Batch Operation Result** page displays once IMC has completed the batch operation.
5. Review the Operation Result field to verify that the requested changes have been made for all devices.

Using batch mode to configure Telnet settings

You can use the IMC batch mode feature to update IMC’s Telnet configuration for one or more devices.

To add or modify IMC’s Telnet settings for one or more devices in batch mode:

1. Navigate to Resource→Batch Operation→Telnet Settings:
   a. Click the Resource tab from the tabular navigation system on the top.
   b. Click Resource Management on the navigation tree on the left.
   c. Click Batch Operation under Resource Management from the navigation system on the left.

2. Click the Telnet Settings link from the NMS Parameter Configuration section of the Resource→Batch Operation page.

3. Click the expand icon to the left of NMS Parameter Configuration to expand the batch operations in NMS Parameter Configuration section to access the Telnet Settings option.

4. Click Add to select the devices to which you want to apply the Telnet settings in the Telnet Settings window.
   You can add devices by using either the View or Advanced query option. See "Adding devices by View" (page 85) and "Adding devices by Advanced query" (page 85).

5. To configure the Telnet settings for selected devices, click on the Configuration icon .
   The Telnet Parameters dialog box appears.

6. You can either enter the Telnet settings in this dialog box or you can select an existing Telnet template that contains the Telnet settings for this device.
   Telnet templates are particularly useful when Telnet configurations are standardized. For more information on creating Telnet templates, see "Telnet templates" (page 77).

Editing Telnet settings manually

1. To edit the Telnet parameters manually, verify that the radio button to the left of Edit Telnet Parameters is selected.

2. Select the Telnet authentication mode from the Authentication Mode list:
   a. Username: Enter the Telnet username in the Username field, if prompted.
   b. Password: Enter the Telnet password in the Password field, if prompted.
   c. Super Password: Enter the Telnet super password in the Super Password field, if prompted.
   d. Timeout: Enter the Telnet timeout value configured on the managed device in the Timeout field.
      Valid range is 1–60 seconds.
Using existing Telnet templates

1. To configure the Telnet settings for this device using Telnet templates, click the radio button to the left of **Select an Existing Template**.
2. Click the radio button to the left of the Telnet template you want to use.
3. Click **OK**.
4. Click **Configure** to apply the Telnet configuration settings to the selected devices.
   The **Batch Operation Result** page displays once IMC has completed the batch operation.
5. Review the **Operation Result** field to verify that the requested changes have been made for all devices.
6. If you want to check the Telnet settings for the devices configured in this batch mode operation, click **Check**.
   The **Check Telnet Settings** pane appears.
7. Click **OK** to check the **Telnet settings** for all devices in the displayed list.
8. Review the **Operation Result** field in the **Check Telnet Settings** List to verify whether or not the Telnet settings you applied were successful.

Using batch mode to configure SSH settings

You and you can use the IMC batch mode feature to update IMC’s SSH configuration for one or more devices.

To add or modify IMC’s SSH settings for one or more devices in batch mode:

1. Navigate to **Resource→Batch Operation→SSH Settings**:
   a. Click the **Resource** tab from the tabular navigation system on the top.
   b. Click **Resource Management** on the navigation tree on the left.
   c. Click **Batch Operation** under **Resource Management** from the navigation system on the left.
2. Click **SSH Settings** link from the **NMS Parameter Configuration** section of the **Resource→Batch Operation** page.
3. Click the expand icon to the left of **NMS Parameter Configuration** to expand the batch operations in **NMS Parameter Configuration** section to access the **SSH Settings** option.
4. Click **Add** to select the devices to which you want to apply the SSH settings in the **SSH Settings** window.
   You can add devices by using either the **View** or **Advanced** query option. See “Adding devices by View” (page 85) and “Adding devices by Advanced query” (page 85).
5. To configure the SSH settings for selected devices, click on the **Configuration** icon .
   The **SSH Parameters** dialog box appears.
   You can either enter the SSH settings in this dialog box or you can select an existing SSH template that contains the SSH settings for this device. SSH templates are particularly useful when SSH configurations are standardized. For more information on creating SSH templates, see “SSH templates” (page 80).
Editing SSH settings manually

1. To edit the SSH parameters, verify that the radio button ☑️ to the left of Edit SSH Parameters is selected.

2. Select the authentication mode from the Authentication Mode list.

   The authentication mode selected must match the configuration on the managed devices.

3. Enter data in the following fields, as required:

   a. **User Name**: Enter username in the User Name field.
   b. **Password**: Enter the password in the Password field.
   c. **Private Key File**: Enter the path and filename of the private key file that contains the key that enables login, if prompted.
   d. **Private Key Password**: Enter the private key password for the private key file, if prompted.
   e. **Super Password**: Enter the super password in the Super Password field.
   f. **Port**: Enter the TCP port for SSH in the Port field. The default TCP port is 22.
   g. **Timeout**: Enter the SSH timeout value (1–120 seconds).
      The timeout parameter defines how long the system waits for the device to respond in seconds before declaring that the response has timed out. The default setting is 10 seconds.
   h. **Retries**: Enter the number of SSH retries (1–5).
      The retries parameter defines how many times the management system (IMC) sends SSH retries in an attempt to communicate with the managed device before reporting a failure. The default setting is 3.

Using existing SSH templates

1. To configure the SSH settings for this device using SSH templates, click the radio button ☑️ to the left of Select an Existing Template.

2. Click the radio button ☑️ to the left of the SSH template you want to use.

3. Click OK to accept the SSH configuration.

4. Click Configure to apply the SSH configuration settings to the selected devices.

   The Batch Operation Result page displays once IMC has completed the batch operation.

5. Review the Operation Result field to verify that the requested changes have been made for all devices.

6. If you want to check the SSH settings for the devices configured in this batch mode operation, click Check.

   The Check SSH Settings window appears.

7. Click OK to check the SSH settings for all devices in the displayed list.

8. Review the Operation Result field in the Check SSH Settings List to verify whether or not the SSH settings you applied were successful.

Using batch mode to configure polling intervals

To add or modify the polling interval for device configuration polls and device status to one or more devices in batch mode:
1. Navigate to **Resource→Batch Operation→Poll Interval Settings**:
   a. Click the **Resource** tab from the tabular navigation system on the top.
   b. Click **Resource Management** on the navigation tree on the left.
   c. Click 🔄 **Batch Operation** under **Resource Management** from the navigation system on the left.
2. Click the **Poll Interval** link from the **NMS Parameter Configuration** section of the **Resource→Batch Operation** page.
3. Click the expand icon 📨 to the left of **NMS Parameter Configuration** to expand the batch operations in **NMS Parameter Configuration** section to access the **Poll Interval** option.
4. Click **Add** to select the devices to which you want to apply the polling configuration settings in the **Poll Interval Settings** window.
   You can add devices by using either the **View** or **Advanced** query option. See "Adding devices by View" (page 85) and "Adding devices by Advanced query" (page 85).
   The **Configuration Poll Interval** is the parameter that determines how long IMC waits before polling managed devices for any configuration changes.
5. Enter the configuration polling interval in minutes in the **Configuration Poll Interval** field.
   The **Configuration Poll Interval** is the parameter that determines how long IMC waits before polling managed devices for any configuration changes. The range is 5–1500 minutes and the default is 120 minutes.
6. Enter the status polling interval in minutes in the **Status Poll Interval** field.
   The **Status Poll Interval** is the parameter that determines how long IMC waits before sending ping requests to managed devices to determine their reachability status. The range is 30–600 seconds and the default is 60 seconds.
7. Click **OK** to apply the configuration settings to the selected devices.
   The **Batch Operation Result** page display once IMC has completed the batch operation.
8. Review the **Operation Result** field to verify that the requested changes have been made for all devices.

**Using batch mode to modify login types**

To add or modify the login type for network devices using batch mode:
1. Navigate to **Resource→Batch Operation→Login Type Settings**:
   a. Click the **Resource** tab from the tabular navigation system on the top.
   b. Click **Resource Management** on the navigation tree on the left.
   c. Click 🔄 **Batch Operation** under **Resource Management** from the navigation system on the left.
2. Click the **Login Type Settings** link from the **NMS Parameter Configuration** section of the **Resource→Batch Operation** page.
3. Click the expand icon 📨 to the left of **NMS Parameter Configuration** to expand the batch operations in **NMS Parameter Configuration** section to access the **Login Type Settings** option.
4. Click **Add** to select the devices to which you want to apply the polling configuration settings in the **Login Type Settings** pane.
You can add devices by using either the View or Advanced query option. See "Adding devices by View" (page 85) and "Adding devices by Advanced query" (page 85).

5. Click the radio button to the left of the access type you want to use to the right of Login Type.
6. Click OK to apply the configuration settings to the selected devices.

The Batch Operation Result page display once IMC has completed the batch operation.

7. Review the Operation Result field to verify that the requested changes have been made for all devices.

Using batch mode to modify ping settings

To add or modify the Ping settings for network devices using batch mode:

1. Navigate to Resource→Batch Operation→Ping Settings:
   a. Click the Resource tab from the tabular navigation system on the top.
   b. Click Resource Management on the navigation tree on the left.
   c. Click 📊 Batch Operation under Resource Management from the navigation system on the left.

2. Click the Ping Settings link from the NMS Parameter Configuration section of the Resource→Batch Operation page.

3. Click the expand icon to the left of NMS Parameter Configuration to expand the batch operations in NMS Parameter Configuration section to access the Ping Settings option.

4. Click Add to select the devices to which you want to apply the polling configuration settings in the Ping Settings pane.

   You can add devices by using either the View or Advanced query option. See "Adding devices by View" (page 85) and "Adding devices by Advanced query" (page 85).

5. Click the Support Ping Operation checkbox.

6. Click OK to apply the configuration settings to the selected devices.

   The Batch Operation Result page displays once IMC has completed the batch operation.

7. Review the Operation Result field to verify that the requested changes have been made for all devices.

Using batch mode to modify interface up/down alarm filter

To modify the interface Up/Down alarm filter for network devices using batch mode:

1. Navigate to Resource→Batch Operation→Interface Up/Down Alarm Filter:
   a. Click the Resource tab from the tabular navigation system on the top.
   b. Click Resource Management on the navigation tree on the left.
   c. Click 📊 Batch Operation under Resource Management from the navigation system on the left.

2. Click the Interface Up/Down Alarm Filter link from the NMS Parameter Configuration section of the Resource→Batch Operation page.
3. Click the expand icon to the left of NMS Parameter Configuration to expand the batch operations in NMS Parameter Configuration section to access the Interface Up/Down Alarm Filter option.

4. Click Add to select the devices to which you want to apply the interface alarm filter settings in the Interface Alarm Filter pane.
   You can add devices by using either the View or Advanced query option. See "Adding devices by View" (page 85) and "Adding devices by Advanced query" (page 85).

5. Set the filter to permit or deny the Up/Down alarm of the interface settings from the Interface Up/Down Alarm Filter list.

6. Click OK to apply the configuration settings to the selected devices.
   The Batch Operation Result page displayed once IMC has completed the batch operation.

7. Review the Operation Result field to verify that the requested changes have been made for all devices.

Checking device configurations in batch mode

Using IMC’s batch mode operation feature, you can also check Telnet and SSH settings and determine quickly whether Telnet or SSH is enabled and functioning on managed devices.

Using batch mode to check Telnet settings

To verify the Telnet settings for network devices using batch mode:

1. Navigate to Resource → Batch Operation → Check Telnet Settings:
   a. Click the Resource tab from the tabular navigation system on the top.
   b. Click Resource Management on the navigation tree on the left.
   c. Click Batch Operation under Resource Management from the navigation system on the left.

2. Click the Check Telnet Settings link from the Check Configuration section of the Resource → Batch Operation page.

3. Click the expand icon to the left of Check Configuration to expand the batch operations in Check Configuration section to access the Check Telnet Settings option.

4. Click Add to select the devices to which you want to apply the Telnet settings in the Check Telnet Settings pane.
   You can add devices using either the View or Advanced query option. See "Adding devices by View" (page 85) and "Adding devices by Advanced query" (page 85).

5. Click OK to begin checking the Telnet settings for the selected devices.
   The Check Telnet Settings results page displays once IMC has completed the batch operation.

6. Review the Operation Result field for individual device results for the Telnet settings check.

Using batch mode to check SSH settings

To verify the SSH settings for network devices using batch mode:

1. Navigate to Resource → Batch Operation → Check SSH Settings:
   a. Click the Resource tab from the tabular navigation system on the top.
b. Click Resource Management on the navigation tree on the left.

c. Click Batch Operation under Resource Management from the navigation system on the left.

2. Click the Check SSH Settings link from the Check Configuration section of the Resource → Batch Operation page.

3. Click the expand icon on the left of Check Configuration to expand the batch operations in Check Configuration section to access the Check SSH Settings option.

4. Click Add to select the devices to which you want to apply the SSH settings in the Check SSH Settings window.

   You can add devices using either the View or Advanced query option. See "Adding devices by View" (page 85) and "Adding devices by Advanced query" (page 85).

5. Click OK to begin checking the SSH settings for the selected devices.

   The Check SSH Settings results page displays once IMC has completed the batch operation.

6. Review the Operation Result field for individual device results for the SSH settings check.

Modifying device configurations in batch mode

IMC also simplifies administrative tasks for saving device configurations, rebooting devices, configuring device interfaces, applying energy saving policies, configuring trap destinations, Spanning Tree Protocol and Spanning Tree Protocol interfaces, LACP, Device Configuration Wizard, and Interface Configuration.

Using batch mode to save device configurations

Using batch mode, you can save device configurations for one or more devices. You can also schedule IMC to run the save configuration batch mode operation once.

To save device configurations using batch mode:

1. Navigate to Resource→Batch Operation→Save Configuration:

   a. Click the Resource tab from the tabular navigation system on the top.

   b. Click Resource Management on the navigation tree on the left.

   c. Click Batch Operation under Resource Management from the navigation system on the left.

2. Click the Save Configuration link from the Device Configuration section of the Resource → Batch Operation page.

3. Click the expand icon on the left of Device Configuration to expand the batch operations in Device Configuration section to access the Save Configuration option.

4. Click Add to select the devices to apply this batch mode operation to.

   You can add devices using either the View or Advanced query option. "Adding devices by View" (page 85) and "Adding devices by Advanced query" (page 85).

5. Run the batch mode save configuration task now or schedule it to run once at a later date by selecting from the following:

   o To run the batch mode save configuration task now, select Immediately from the Schedule Information list, or
To schedule to run once in the future, select **Once**.

If you selected **Once**:

a. Enter a date and time in the field next to the **Schedule Information**.

b. Enter the date and time manually or enter it by clicking on the calendar icon located to the right of the field.

A popup calendar appears.

c. Select the date from the calendar. To enter it manually, the valid date format is YYYY-MM-DD HH:MM:SS where YYYY refers to the four-digit year, MM refers two-digit month, DD refers to the two-digit day, HH refers to the two-digit hour, MM refers to the two-digit minute, and SS refers to the two-digit second values.

6. Click **OK**.

The **Plan List** displays along with the status of the batch mode operation task in the **Status** field.

7. Click **Refresh** to update the **Plan List** and the **Status** field.

When the task is complete, the **Status** field updates to **Finished**.

8. Click the **Details** icon associated with the task to view detailed results of the batch mode task.

If you opted to run the batch mode operation at a later date, you can review the results of this batch operation task by clicking on **Edit Plan** to the right of **Save Configuration**.

**Using batch mode to reboot devices**

Using batch mode, you can reboot one or more devices. You can also schedule IMC to run the reboot device batch operation once.

To reboot devices using batch mode:

1. Navigate to **Resource→Batch Operation→Reboot Device**:
   a. Click the **Resource** tab from the tabular navigation system on the top.
   b. Click **Resource Management** on the navigation tree on the left.
   c. Click **Batch Operation** under **Resource Management** from the navigation system on the left.

2. Click the **Reboot Device** link from the **Device Configuration** section of the **Resource→Batch Operation** page.

3. Click the expand icon to the left of **Device Configuration** to expand the batch operations in **Device Configuration** section to access the **Reboot Device** option.

4. Click **Add** to select the devices to apply this batch mode operation to.

You can add devices using either the **View** or **Advanced** query option. See "Adding devices by **View**" (page 85) and "Adding devices by **Advanced query**" (page 85).

5. Run the batch mode save configuration task now or schedule it to run once at a later date by selecting from the following:

   o To run the batch mode save configuration task now, select **Immediately** from the **Schedule Information** list, or
   o To schedule to run once in the future, select **Once**.

   If you selected **Once**:
a. Enter a date and time in the field next to the **Schedule Information**.
b. Enter the date and time manually or enter it by clicking on the calendar icon located to the right of the field.

   A popup calendar appears.
c. Select the date from the calendar. To enter it manually, the valid date format is YYYY-MM-DD HH:MM:SS where YYYY refers to the four-digit year, MM refers two-digit month, DD refers to the two-digit day, HH refers to the two-digit hour, MM refers to the two-digit minute, and SS refers to the two-digit second values.

6. Click **OK**.

   The **Plan List** displays along with the status of the batch mode operation task in the **Status** field.

7. Click **Refresh** to update the **Plan List** and the **Status** field.

   When the task is complete, the **Status** field updates to **Finished**.

8. Click the **Details** icon associated with the task to view detailed results of the batch mode task.

   If you opted to run the batch mode operation at a later date, you can review the results of this batch operation task by clicking **Edit Plan** to the right of **Save Configuration**.

### Using batch mode to configure management status on interfaces

Using batch mode, you can configure the management status of one or more interfaces for one or more devices. You can also schedule IMC to run the batch mode operation once.

To configure the management status of one or more interfaces using batch mode:

1. Navigate to **Resource**→**Batch Operation**→**Configure Interfaces**:
   a. Click the **Resource** tab from the tabular navigation system on the top.
   b. Click **Resource Management** on the navigation tree on the left.
   c. Click **Batch Operation** under **Resource Management** from the navigation system on the left.

2. Click the **Configure Interface** link from the **Device Configuration** section of the **Resource**→**Batch Operation** page.

3. Click the expand icon to the left of **Device Configuration** to expand the batch operations in **Device Configuration** section to access the **Configure Interface** option.

4. Click **Add** to select the device interfaces to apply this batch mode operation to.

   You can add devices using either the **View** or **Advanced** query option. See "Adding devices by View" (page 85) and "Adding devices by Advanced query" (page 85).

5. Select the management status for the selected interfaces from the **Management Status** list.

6. Run the batch mode save configuration task now or schedule it to run once at a later date by selecting from the following:
   a. To run the batch mode save configuration task now, select **Immediately** from the **Schedule Information** list, or
   b. To schedule to run once in the future, select **Once**.

   If you selected **Once**:
   
   a. Enter a date and time in the field next to the **Schedule Information**.
b. Enter the date and time manually or enter it by clicking on the calendar icon located to the right of the field.

   A popup calendar appears.

c. Select the date from the calendar. To enter it manually, the valid date format is YYYY-MM-DD HH:MM:SS where YYYY refers to the four-digit year, MM refers two-digit month, DD refers to the two-digit day, HH refers to the two-digit hour, MM refers to the two-digit minute, and SS refers to the two-digit second values.

7. Click OK.

   The Plan List displays along with the status of the batch mode operation task in the Status field.

8. Click Refresh to update the Plan List and the Status field.

   When the task has been completed the Status field updates to Finished.

9. Click the Details icon associated with the task to view detailed results of the batch mode task.

   If you opted to run the batch mode operation at a later date, you can review the results of this batch operation task by clicking on [Edit Plan] to the right of Configure Interface.

Using batch mode to implement energy saving policies

Using batch mode, you can configure Power over Ethernet (PoE) settings on one or more interfaces for one or more devices. You can also schedule this batch mode operation once.

To configure PoE settings using batch mode:

1. Navigate to Resource → Batch Operation → Energy Saving Policy.

   a. Click the Resource tab from the tabular navigation system on the top.

   b. Click Resource Management on the navigation tree on the left.

   c. Click Batch Operation under Resource Management from the navigation system on the left.

2. Click the Energy Saving Policy link from the Device Configuration section of the Resource → Batch Operation page.

3. Click the expand icon to the left of Device Configuration to expand the batch operations in Device Configuration section to access the Energy Saving Policy option.

4. Click Add to select the device interfaces to apply this batch mode operation to.

   You can add devices using either the View or Advanced query option. See "Adding devices by View" (page 85) and "Adding devices by Advanced query" (page 85).

5. Enter the PSE power setting in the PSE Power field.

   The range is 1-806 Watts.

⚠️ WARNING:

The status of PSE must be enabled and the maximum PSE power must be greater than or equal to the sum of the maximum power of all critical PoE interfaces on the PSE to guarantee power to the PoE interfaces.

6. Enter the power for the PoE interfaces in the Power of the PoE Interface field.

   The range is 1-17000mW.

7. Select the priority for this PoE setting from the Priority list.
8. Run the batch mode save configuration task now or schedule it to run once at a later date by selecting from the following:
   • To run the batch mode save configuration task now, select **Immediately** from the **Schedule Information** list, or
   • To schedule to run once in the future, select **Once**.
   
   If you selected **Once**:
   a. Enter a date and time in the field next to the **Schedule Information**.
   b. Enter the date and time manually or enter it by clicking on the calendar icon located to the right of the field.
      A popup calendar appears.
   c. Select the date from the calendar. To enter it manually, the valid date format is YYYY-MM-DD HH:MM:SS where YYYY refers to the four-digit year, MM refers two-digit month, DD refers to the two-digit day, HH refers to the two-digit hour, MM refers to the two-digit minute, and SS refers to the two-digit second values.

9. Click **OK**.
   The **Plan List** displays along with the status of the batch mode operation task in the **Status** field.

10. Click **Refresh** to update the **Plan List** and the **Status** field.
    When the task is complete, the **Status** field updates to **Finished**.

11. Click the **Details** icon associated with the task to view detailed results of the batch mode task.
    If you opted to run the batch mode operation at a later date, you can review the results of this batch operation task by clicking on **Edit Plan** to the right of **Save Configuration**.

**Using batch mode to configure trap destinations**

Using batch mode, you can configure the trap destination for one or more devices. You can also schedule IMC to run the trap destination configuration batch operation once.

To configure the trap destination using batch mode:

1. Navigate to **Resource**→**Batch Operation**→**Configure Trap Destination**:
   a. Click the **Resource** tab from the tabular navigation system on the top.
   b. Click **Resource Management** on the navigation tree on the left.
   c. Click **Batch Operation** under **Resource Management** from the navigation system on the left.

2. Click the **Configure Trap Destination** link from the **Device Configuration** section of the **Resource**→**Batch Operation** page.

3. Click the expand icon to the left of **Device Configuration** to expand the batch operations in **Device Configuration** section to access the **Configure Trap Destination** option.

4. Click **Add** to select the devices to apply this batch mode operation to.
   You can add devices using either the **View** or **Advanced** query option. See "Adding devices by View" (page 85) and "Adding devices by Advanced query" (page 85).
5. Enter the IP address or hostname of the device that serves as the trap destination in the Host field.

6. Enter the UDP port configured on the trap destination for receiving SNMP traps in the UDP Port field.
   The default UDP port for SNMP traps is 162.

7. Do one of the following:
   o If you are using SNMP v1 or v2c, enter the trap community string configured on the trap destination in the Authentication Parameters field, or
   o If you are using SNMPv3, enter the username that is configured on the trap destination in the Authentication Parameters field.

8. Select the version of SNMP that is configured on the trap destination from the SNMP Version list.

9. If you selected SNMPv3, select the security model from the Security Model list.

10. Click the checkbox □ to the left of Clear Trap Destination if you want to configure the same host as the recipient for clear traps.

11. Run the batch mode save configuration task now or schedule it to run once at a later date by selecting from the following:
   o To run the batch mode save configuration task now, select Immediately from the Schedule Information list, or
   o To schedule to run once in the future, select Once.
   If you selected Once:
   a. Enter a date and time in the field next to the Schedule Information.
   b. Enter the date and time manually or enter it by clicking on the calendar □ icon located to the right of the field.
   A popup calendar appears.
   c. Select the date from the calendar. To enter it manually, the valid date format is YYYY-MM-DD HH:MM:SS where YYYY refers to the four-digit year, MM refers two-digit month, DD refers to the two-digit day, HH refers to the two-digit hour, MM refers to the two-digit minute, and SS refers to the two-digit second values.

12. Click OK.
   The Plan List displays along with the status of the batch mode operation task in the Status field.

13. Click Refresh to update the Plan List and the Status field.
   When the task is complete, the Status field updates to Finished.

14. Click the Details icon 📇 associated with the task to view detailed results of the batch mode task.
   If you opted to run the batch mode operation at a later date, you can review the results of this batch operation task by clicking on [Edit Plan] to the right of Configure Trap Destination.

Using batch mode to configure spanning tree protocol on switches

Using batch mode, you can apply Spanning Tree configurations to one or more devices. You can also schedule IMC to run the Spanning Tree configuration batch operation once.
To configure the Spanning Tree using batch mode:

1. Navigate to Resource→Batch Operation→Configure Spanning Tree:
   a. Click the Resource tab from the tabular navigation system on the top.
   b. Click Resource Management on the navigation tree on the left.
   c. Click 📦 Batch Operation under Resource Management from the navigation system on the left.

2. Click the Configure STP link from the Device Configuration section of the Resource→Batch Operation page.

3. Click the expand icon 📊 to the left of Device Configuration to expand the batch operations in Device Configuration section to access the Configure STP option.

4. Click Add to select the devices to apply this batch mode operation to.
   You can add devices using either the View or Advanced query option. See "Adding devices by View" (page 85) and "Adding devices by Advanced query" (page 85).

5. To enable Spanning Tree mode, select Enabled from the Spanning Tree Mode list in the Configure Spanning Tree window.
   Selecting Enabled activates the remaining Spanning Tree configuration options listed below.

6. To configure bridge priority for the selected devices, click the checkbox ☑ to the left of the Bridge Priority field.

7. Select the bridge priority number from the Bridge Priority list.
   The list lists all valid bridge priority numbers.

8. To configure the Hello Time for packets sent between switches in a Spanning Tree to determine when the root switch has failed for the selected devices, click the checkbox ☑ to the left of the Hello Time field.
   The range is 1–10 seconds and the default is 2 seconds.

9. To configure the maximum age of a Hello packet, enter the max age value in the Max Age field.
   The range is 6–40 seconds and the default is 20 seconds.

10. To configure the Forward Delay settings for Hello packets, enter the value in seconds in the Forward Delay field.
    The range is 4–30 seconds and the default is 15 seconds.

11. Run the batch mode save configuration task now or schedule it to run once at a later date by selecting from the following:
    o To run the batch mode save configuration task now, select Immediately from the Schedule Information list, or
    o To schedule to run once in the future, select Once.
    If you selected Once:
    a. Enter a date and time in the field next to the Schedule Information.
    b. Enter the date and time manually or enter it by clicking on the calendar 🗓 icon located to the right of the field.
       A popup calendar appears.
c. Select the date from the calendar. To enter it manually, the valid date format is YYYY-MM-DD HH:MM:SS where YYYY refers to the four-digit year, MM refers two-digit month, DD refers to the two-digit day, HH refers to the two-digit hour, MM refers to the two-digit minute, and SS refers to the two-digit second values.

12. Click OK. The Plan List displays along with the status of the batch mode operation task in the Status field.

13. Click Refresh to update the Plan List and the Status field. When the task is complete, the Status field updates to Finished.

14. Click the Details icon associated with the task to view detailed results of the batch mode task. If you opted to run the batch mode operation at a later date, you can review the results of this batch operation task by clicking on [Edit Plan] to the right of Configure STP.

**Using batch mode to configure spanning tree protocol on interfaces**

Using batch mode, you can apply Spanning Tree configurations to one or more interfaces. You can also schedule IMC to run the Spanning Tree interface configuration batch operation once.

To configure the Spanning Tree on interfaces using batch mode:

1. Navigate to Resource → Batch Operation → Energy Saving Policy.
   a. Click the Resource tab from the tabular navigation system on the top.
   b. Click Resource Management on the navigation tree on the left.
   c. Click Batch Operation under Resource Management from the navigation system on the left.

2. Click the Configure STP Interface link from the Device Configuration section of the Resource → Batch Operation page.

3. Click the expand icon to the left of Device Configuration to expand the batch operations in Device Configuration section to access the Configure STP Interface option.

4. Click Add to select the device interfaces to apply this batch mode operation to. You can add devices using either the View or Advanced query option. See "Adding devices by View" (page 85) and "Adding devices by Advanced query" (page 85).

5. To configure the port path cost for the selected interfaces, first verify that the checkbox to the left of the Port Path Cost field is checked.

6. Enter the port path cost in the Port Path Cost field. The Port Path Cost field must contain an integer that is greater than or equal to zero.

7. To enable Spanning Tree Fast Start, first verify that the checkbox to the left of the Spanning Tree Fast Start field is checked.


9. Run the batch mode save configuration task now or schedule it to run once at a later date by selecting from the following:
   o To run the batch mode save configuration task now, select Immediately from the Schedule Information list, or
   o To schedule to run once in the future, select Once.
If you selected **Once**:

**a.** Enter a date and time in the field next to the **Schedule Information**.

**b.** Enter the date and time manually or enter it by clicking on the calendar icon located to the right of the field.

A popup calendar appears.

**c.** Select the date from the calendar. To enter it manually, the valid date format is YYYY-MM-DD HH:MM:SS where YYYY refers to the four-digit year, MM refers two-digit month, DD refers to the two-digit day, HH refers to the two-digit hour, MM refers to the two-digit minute, and SS refers to the two-digit second values.

10. **Click OK.**

The **Plan List** displays along with the status of the batch mode operation task in the **Status** field.

11. **Click Refresh** to update the **Plan List** and the **Status** field.

When the task is complete, the **Status** field updates to **Finished**.

12. **Click the Details icon** associated with the task to view detailed results of the batch mode task.

   If you opted to run the batch mode operation at a later date, you can review the results of this batch operation task by clicking on **[Edit Plan]** to the right of **Configure STP Interface**.

**Using batch mode to configure LACP**

Using batch mode, you can apply Link Aggregation Control Protocol (LACP) configurations to one or more interfaces. You can also schedule IMC to run the LACP configuration batch operation once.

To configure the LACP on interfaces using batch mode:

1. Navigate to **Resource→Batch Operation→Energy Saving Policy**.
   **a.** Click the **Resource** tab from the tabular navigation system on the top.
   **b.** Click **Resource Management** on the navigation tree on the left.
   **c.** Click **Batch Operation** under **Resource Management** from the navigation system on the left.

2. Click the **Configure LACP** link from the **Device Configuration** section of the **Resource→Batch Operation** page.

3. Click the expand icon **+** to the left of **Device Configuration** to expand the batch operations in **Device Configuration** section to access the **Configure STP Interface** option.

4. **Click Add** to select the device interfaces to apply this batch mode operation to.

   You can add devices using either the **View** or **Advanced** query option. See "Adding devices by View" (page 85) and "Adding devices by Advanced query" (page 85).

5. To enable LACP on the selected devices, select **Enabled** from the **LACP State** list.

6. Run the batch mode save configuration task now or schedule it to run once at a later date by selecting from the following:
   **o** To run the batch mode save configuration task now, select **Immediately** from the **Schedule Information** list, or
   **o** To schedule to run once in the future, select **Once**.

   If you selected **Once**:
a. Enter a date and time in the field next to the **Schedule Information**.

b. Enter the date and time manually or enter it by clicking on the calendar icon located to the right of the field.

A popup calendar appears.

c. Select the date from the calendar. To enter it manually, the valid date format is YYYY-MM-DD HH:MM:SS where YYYY refers to the four-digit year, MM refers two-digit month, DD refers to the two-digit day, HH refers to the two-digit hour, MM refers to the two-digit minute, and SS refers to the two-digit second values.

7. Click **OK**.

The **Plan List** displays along with the status of the batch mode operation task in the **Status** field.

8. Click **Refresh** to update the **Plan List** and the **Status** field.

When the task is complete, the **Status** field updates to **Finished**.

9. Click the **Details** icon associated with the task to view detailed results of the batch mode task.

If you opted to run the batch mode operation at a later date, you can review the results of this batch operation task by clicking on [Edit Plan] to the right of **Configure LACP**.

### Using batch mode to configure devices

By creating a batch device configuration plan, you can configure multiple devices in batch. You can configure a batch device configuration plan according to the requirements of each component. In a practical service that involves multiple component operations, you can create a batch device configuration plan to apply the integrated operations.

To configure device using batch mode:

1. Navigate to **Resource→Batch Operation→Save Configuration**:
   a. Click the **Resource** tab from the tabular navigation system on the top.
   b. Click **Resource Management** on the navigation tree on the left.
   c. Click **Batch Operation** under **Resource Management** from the navigation system on the left.

2. Click the **Device Configuration Guide** link from the **Device Configuration** section of the **Batch Operation** page.

The **Deployment Window** appears.

3. Click the expand icon to the left of **Device Configuration** to expand the batch operations in **Device Configuration** section to access the **Configure STP Interface** option.

4. Select operations and devices.

The selected operations are to be performed on all the selected devices.

5. Click **Add** under the **Operation List**.

6. The **Select Operations** window appears.

7. Click **.expand** to expand all operations. Click **.** to collapse all operations.

   o At the same time, you can click **.** to the left of an operation type to expand all operations of this type, and click **.** to collapse all operations of this type.

293
After you deploy the components that the batch operations support, the batch operations display in the operation list.

8. Do one of the following:
   - Click the checkbox to the left of the parameters you want to select, or
   - To select all operations of a certain type, click on the checkbox to the left of the type. If you have installed other service components, the corresponding operations appear.

9. Click OK.

10. Confirm that the operations you have selected now appear in the Operation List.

11. Do one of the following:
   - Click the checkbox to the left of the parameters you want to move, or
   - Click Delete to delete the parameters and then click the icon in the Delete field to delete the association operation, or

12. Click one of the icons in the Sort field to reorder the parameters in the operation list:
   - Use to move the parameter up one position.
   - Use to move the parameter to the top of the parameter list.
   - Use to move the parameter down one position.
   - Use to move the parameter to the bottom of the list.

13. Click Add under the Device List to select the devices to apply this batch mode operation to. You can add devices using either the View or Advanced query option. See "Adding devices by View" (page 85) and "Adding devices by Advanced query" (page 85).

14. Click Next.

15. To configure parameters for the operation, do one of the following:

   **Add VLAN**
   - **VLAN ID**: Enter the VLAN ID.
   - **VLAN Name**: Enter a name for the VLAN.

   **Delete VLAN**
   - **VLAN ID**: Select a VLAN from the VLAN ID list. Note that the selected VLAN is deleted from all selected devices, and the VLAN must already exist in the IMC.
   - When you configure multiple devices at a time, the available VLAN IDs are the intersection of the VLANs on all devices.

   **Modify VLAN Name**
   - **VLAN ID**: Select a VLAN from the VLAN ID list.
   - **VLAN Name**: Enter a new name for the VLAN.
Add Virtual Interface

**VLAN ID**: Select a VLAN from the VLAN ID list.

**IP Address Type**: Select a type for the virtual interface from the IP Address Type list.

**DHCP Enabled**: Specify whether to enable DHCP.

**IP Address**: Enter an IP address for the virtual interface. This property is required if you do not enable DHCP.

**Mask**: Enter a mask for the IP address. This property is required if DHCP is not enabled.

Delete Virtual Interface

**VLAN ID**: Enter the VLAN ID you want to delete. The VLAN deletes the ID from all the devices you select.

**IP Address Type**: Select a type for the virtual interface from the IP Address Type list.

**DHCP Enabled**: Select whether to enable DHCP.

**IP Address**: Enter IP address for the virtual interface. This property is required if DHCP is not enabled.

**Mask**: Enter a mask for the IP address. This property is required if DHCP is not enabled.

When you configure multiple devices at a time, the available VLAN IDs are the intersection of the VLANs on all devices.

16. Do one of the following:
   - Click the Copy link to the right of an operation to copy the operation to create an operation that uses the default parameters, or
   - Click the Delete link to the right of an operation to delete the operation.

   You can apply up to 30 operations (including operations of the same name) at a time. If you apply more than 30 operations, the copying operation fails, and you cannot enter the next configuration procedure.

17. Click Next to enter the Set Task Attributes page.
18. Enter a name for this task in the Task Name field.
19. Select the type of deployment schedule you want to apply to this task from the Schedule Type list.
20. Do one of the following:
   - Select Once and go to Step 20, if you want IMC to execute this task one time, or
   - Select Cycle and go to Step 21 if you want this configuration deployment task to be executed on a scheduled basis.
21. If you select Once in the Schedule Type field, do the following:
   - Select the time you want IMC to execute this task from the Schedule Time list. Options include Scheduled and Immediately.
   - Do one of the following:
     - If you selected Immediately, go to Step 22.
     - If you selected Scheduled, click the calendar icon to populate the date and time for the execution of this task. A popup calendar appears. Select the date from the calendar.
Go to Step 22.

22. If you selected **Cycle** from the **Schedule Type** list, do the following:
   
a. Select the frequency with which you want IMC to execute this task from the **Operation Frequency** list.

b. If you selected **Every Week** from the **Operation Frequency** list, select the date of the week you want IMC to execute this task from the list to the right of the **Operation Frequency** list and go to Step 21d

c. If you selected **Every Month** from the **Operation Frequency** list, select the day of the month you want IMC to execute this task from the list to the right of the **Operation Frequency** list and go to Step 21e

d. Enter the time you want IMC to execute this task in the field to the far right of the **Operation Frequency** list. Enter the time in HH:MM:SS format where HH denotes a two digit hour value, MM denotes a two digit minute value and SS denotes a two digit second value.

e. Enter the beginning date and time you want IMC to execute this task in the **Start Time** field. Click the calendar icon to populate the date and time for the execution of this task. A popup calendar will be displayed. Select the start date from the calendar.

f. Enter the ending date and time you want IMC to execute this task in the **End Time** field. Click the calendar icon to populate the date and time for the execution of this task. A popup calendar appears. Select the end date from the calendar.

23. Define how you want IMC to handle errors that arise in the deployment process, by selecting one of the following:
   
o If you want IMC to continue the deployment for the device if an error arises during deployment, select **Continue deployment on the current device** from the **Error Handling** list, or

   o If you want IMC to abandon the deployment for the device if an error arises during deployment, select **Stop deployment on the current device** from the **Error Handling** list.

24. Click **OK**.

**Using batch mode to configure interface**

By creating a batch interface configuration plan, you can configure multiple interfaces in batch. You can configure a batch interface configuration plan according to the requirements of each component. In a practical service that involves multiple component operations, you can create a batch interface configuration plan to apply the integrated operations.

To configure interface using batch mode

1. Navigate to **Resource→Batch Operation→Save Configuration**:
   
a. Click the **Resource** tab from the tabular navigation system on the top.

b. Click **Resource Management** on the navigation tree on the left.

c. Click 📊 **Batch Operation** under **Resource Management** from the navigation system on the left.

2. Click the **Interface Configuration Guide** link from the **Device Configuration** section of the **Batch Operation** page. The **Deployment** window appears.

3. To expand the batch operations in **Device Configuration** section to access the **Interface Configuration Wizard** option.
4. Click the expand icon  to the left of Device Configuration.
5. Click Add under the Operation List. The Select Operations window appears.
6. Click  to expand all operations. Click  to collapse all operations.
7. Click  to the left of an operation type to expand all operations of this type, and click  to collapse all operations of this type.
   After you deploy the components that the batch operations support, the batch operations are displayed on the following operation list. This section takes the VLAN component for example.
8. Click the checkbox  to the left of the parameters you want to select.
9. Click the checkbox to the left of a type to select all operations of this type.
   The operation include Add Ports to VLAN, Delete ports from VLAN, Modify Access Port PVID, Add Hybrid Port, Delete Hybrid Port, Modify Hybrid Port, Add Trunk Port, Delete Trunk Port, Modify Trunk Port. If you have installed other service components, the corresponding operations appear.
10. Click OK.
11. Confirm that the operations you have selected now appear in the Operation List.
12. Click the checkbox  to the left of the parameters you want to move.
13. Click Delete to delete the parameters.
14. To reorder the parameters in the operation list using the icons located in the Sort field:
   o Use  to move the parameter up one position. or
   o Use  to move the parameter to the top of the parameter list, or
   o Use  to move the parameter down one position, or
   o Use  to move the parameter to the bottom of the list.
15. Click the  icon in the Delete field to delete the association operation.
16. Click Add under the Interface List to select the interfaces to apply this batch mode operation to.
   You can add devices by using either the View or the Advanced query option. See "Adding devices by View" (page 85) and "Adding devices by Advanced query" (page 85).
17. Click Next.
   The Configure Parameters page appears.
18. Configure the following parameters:
   o Add ports to VLAN
     - VLAN ID: Select a VLAN ID in the list. The VLANs in the VLANs are the intersection of all VLANs on the devices.
   o Delete port from VLAN
     - VLAN ID: Select the VLAN ID you want to delete from the interfaces in the list.
   o Modify Access Port PVID
     - Destination PVID: Select a VLAN in the list as the PVID of the port.
   o Add Hybrid Port
- **PVID**: Enter the PVID for the ports.
- **Tagged VLAN**: Enter the tagged VLAN IDs.
- **Enable Untagged VLAN**: Specify whether to enable the untagged VLAN feature.
- **Untagged VLAN**: Enter the untagged VLAN IDs if you have enabled the untagged VLAN feature.
- **Enable Forbidden VLAN**: Specify whether to enable the forbidden VLAN feature. If you enable the feature, you can prevent the hybrid port from being assigned to the specified VLAN.
- **Forbidden VLAN**: Enter the forbidden VLAN IDs.

**Modify Hybrid Port**
- **PVID**: Enter the port VLAN ID (PVID).
- **Tagged VLAN**: Enter the tagged VLAN IDs.
- **Enable Untagged VLAN**: Specify whether to enable the untagged VLAN feature.
- **Untagged VLAN**: Enter the untagged VLAN IDs if you have enabled the untagged VLAN feature.
- **Enable Forbidden VLAN**: Specify whether to enable the forbidden VLAN feature. If you enable the feature, you can prevent the hybrid port from being assigned to the specified VLANs.
- **Forbidden VLAN**: Enter the forbidden VLAN IDs.

**Add Trunk Port**
- **PVID**: Enter the PVID of the trunk port.
- **Allowed VLAN**: Enter the VLAN IDs allowed on the trunk port.

**Modify Trunk Port**
- **PVID**: Enter the PVID of the trunk port.
- **Allowed VLAN**: Enter the VLAN IDs allowed on the trunk port.

When you configure multiple devices at a time, the VLAN IDs available for selection are the intersection of the VLANs of all devices.

19. Do one of the following:
   - Click the **Copy** link to the right of an operation to copy the operation to create a new operation, which uses the default parameters, or
   - Click the **Delete** link to the right of an operation to delete the operation.

You can apply up to 30 operations (including operations of the same name) at a time. If you apply more than 30 operations, the copying operation fails, and you cannot enter the next configuration procedure.

20. Click **Next** to enter the **Set Task Attributes** page.

21. Enter a name for this task in the **Task Name** field.

22. Select the type of deployment schedule you want to apply to this task from the **Schedule Type** list:
   - Select **Once** if you want IMC to execute this task one time, or
Select Cycle if you want this configuration deployment task to be executed on a scheduled basis.

23. If you select Once in the Schedule Type field, complete the following steps.
   o Select the time you want IMC to execute this task from the Schedule Time list. Options include Scheduled and Immediately.
   a. If you selected Scheduled, click the calendar icon to populate the date and time for the execution of this task.
      A popup calendar appears.
   b. Select the date from the calendar.

24. If you selected Cycle from the Schedule Type list, complete the following steps.
   a. Select the frequency with which you want IMC to execute this task from the Operation Frequency list.
   b. If you selected Every Week from the Operation Frequency list, select the date of the week you want IMC to execute this task from the list to the right of the Operation Frequency list.
   c. If you selected Every Month from the Operation Frequency list, select the day of the month you want IMC to execute this task from the list to the right of the Operation Frequency list.
   d. Enter the time you want IMC to execute this task in the field to the far right of the Operation Frequency list.
   e. Enter the time in HH:MM:SS format where HH denotes a two digit hour value, MM denotes a two digit minute value and SS denotes a two digit second value.
   f. Enter the beginning date and time you want IMC to execute this task in the Start Time field.
   g. Click the calendar icon to populate the date and time for the execution of this task.
      A popup calendar appears.
   h. Select the start date from the calendar.
   i. Enter the ending date and time you want IMC to execute this task in the End Time field.
   j. Click the calendar icon to populate the date and time for the execution of this task.
      A popup calendar appears.
   k. Select the end date from the calendar.

25. Do one of the following to define how you want IMC to handle errors that arise in the deployment process:
   o If you want IMC to continue the deployment for the device if an error arises during deployment, select Continue deployment on the current device from the Error Handling list, or
   o If you want IMC to abandon the deployment for the device if an error arises during deployment, select Stop deployment on the current device from the Error Handling list.

26. Click OK.

Managing multiple devices from the device list

From the Device List page, IMC offers you the ability to manage and unmanage, synchronize, refresh and deploy batch operations for one or more devices. In addition, the Device List offers quick access
to batch operations for SNMP, Telnet, SSH, Poll configurations, rebooting, saving and backing up configurations and deploying software.

All of these options can be performed from the **Device List**. Device lists can be accessed from the **Device View**, the **IP View**, and **Custom Views** simply by clicking the device, IP, or custom group.

**Navigating to the device list**

The features that enable you to manage multiple devices are available from the **Device List**. The **Device List** can be accessed from the **Device View**, the **IP View**, and the **Custom View**. To navigate to the **Device List** from the **Device View**:

1. Navigate to **Resource**→**View Management**→**View-<Device Type>**:  
   - a. Click the **Resource** tab from the tabular navigation system on the top.
   - b. Click **View Management** on the navigation tree on the left.
   - c. Click **Device View** under **View Management** from the navigation system on the left.

2. Click the expand icon  to the left of the **Device View** on the navigation tree on the left.

3. Click the category of device view you want to access.

4. The **Device List** for the device category you choose appears.

5. Click **Device View** from the navigation system for the **Device List** for all devices.

6. To view all device groups under **Device View**, you may need to click the expand icon .

7. To view various lists, select from the following:

   o For the **Device List** for routers, click Routers under **Device View** from the navigation system on the left, or

   o For the **Device List** for switches, click Switches under **Device View** from the navigation system on the left, or

   o For the **Device List** for servers, click Servers under **Device View** from the navigation system on the left, or

   o For the **Device List** for all security devices, click Security under **Device View** from the navigation system on the left, or

   o For the **Device List** for all wireless devices, click Wireless under **Device View** from the navigation system on the left, or

   o Click Storage under **Device View** from the navigation tree on the left for a summary view of all storage devices, or

   o For the **Device List** for voice devices, click Voice under **Device View** from the navigation system on the left, or

   o For the **Device List** for desktop devices, click Desktop under **Device View** from the navigation system on the left, or
For the **Device List** for other devices, click Other under **Device View** from the navigation system on the left.

**Navigating to the device list from the IP view**

To navigate to the Device List from the IP View:

1. Navigate to **Resource → IP View → Subnet-<Subnet IP Address>**:
   a. Click the **Resource** tab from the tabular navigation system on the top.
   b. Click **IP View** on the navigation tree on the left.
   c. To view all IP subnets under **IP View**, you may need to click the expand icon  to the left of **IP View**.
   d. Click the IP subnet view you want to access.
   e. The **Device List** for the IP subnet you choose appears.
      IMC displays all devices in the **IP View** in the **Device List** displayed in the main pane of the **IP View** window.

**Navigating to the device list from a custom view**

To navigate to the Device List from a Custom View:

1. Navigate to **Resource → Custom View → <View Name>**.
   a. Click the **Resource** tab from the tabular navigation system on the top.
   b. Click **View Management** on the navigation tree on the left.
   c. Click **Custom View** under **View Management** from the navigation system on the left.
   d. To view all custom views under **Custom View**, you may need to click the expand icon  to the left of the **Custom View** tree.
   2. Click the custom view you want to access.
      The **Device List** for the custom view you choose appears. IMC displays all devices in the **Custom View** in the **Device List** displayed in the main pane of the **Custom View**.

**Device list management options**

From the **Device List**, you can add, remove, delete, manage, and unmanage devices as well as synchronize and refresh data for device details. In addition, you can select one or more devices from the **Device List** and then launch batch operations for configuring SNMP, Telnet, and SSH settings as well as checking Telnet and SSH settings.

You can also launch batch operations for one or more devices from the **Device List** for configuring status and configuration polling intervals, rebooting devices, saving device configurations, deploying software, and backing up configurations.

**Add**

This feature, available only for **Custom View Device Lists**, allows you and you to add devices that already exist in IMC to the current **Custom View**.

To add a device to the current custom view:

1. Navigate to the **Custom View** that you want to add devices to.
For information on navigating to a **Device List** from a custom view, see "Navigating to the device list from a custom view" (page 301).

2. Click **Add** from the selected Custom View’s **Device List**.

3. Add devices by using either the **View** or the **Advanced** query option.
   See "Adding devices by View" (page 85) and "Adding devices by Advanced query" (page 85).

4. Click **OK**.
5. Confirm that the devices now appear in the custom view **Device List**.

### Remove

This feature, available only from **Custom View Device Lists**, allows you to remove devices from the current **Custom View**. The **Remove** feature is only available for **Custom Views** and only from the **Device List** level of a **Custom View**.

To remove a device from the current custom view:

1. Navigate to the **Custom View** that you want to remove devices from.
   For information on navigating to a **Device List** from a custom view, see "Navigating to the device list from a custom view" (page 301).

2. Click the checkbox □ to the left of the devices you want to remove from the selected custom view’s **Device List**.
   For information on navigating to a **Device List**, see "Navigating to the device list from a custom view" (page 301).

3. Click **Remove** to remove the devices from the selected custom view’s **Device List**.

4. Click **OK** to confirm the removal of the selected devices from the custom view.

### Delete

Delete removes the selected devices from IMC. IMC purges all data associated with the deleted devices immediately. The **Delete** feature is only available for **Device Views** and **IP Views**.

To delete devices from the current view:

1. Navigate to a **Device List** that contains the devices that you want to delete.
   For information on navigating to a **Device List**, see "Navigating to the device list" (page 300).

2. Click the checkbox □ to the left of the devices you want to delete from a **Device View** or **IP View Device List**.

3. Click **Delete** to manage the selected devices.

4. Review the results of the operation in the **Device List** page.

⚠️ **WARNING:**

You cannot recover a device or associated data once you have deleted it. Use this feature with caution.

### Manage

Managing a device enables all relevant IMC management, monitoring, and reporting features to be applied to the selected devices. Managing a device therefore consumes IMC node licenses.
To manage devices from the current view:

1. Navigate to a **Device List** that contains the devices that you want to manage.
   
   For information on navigating to a **Device List**, see "Navigating to the device list" (page 300).

2. Click the checkbox ☒ to the left of the devices you want to manage from the selected view’s **Device List**.

3. Click **Manage** to manage the selected devices.

4. Review the results of the operation in the **Device List** page.

⚠️ **WARNING:**

Be aware of the impact of managing devices. Managed devices consume node licenses in IMC. For a current license count, click the **About** link in the upper right corner of IMC.

### Unmanage

Unmanaging a device disables all relevant IMC management, monitoring, and reporting features from the selected devices. Unmanaged devices also need IMC node licenses.

To unmanage devices from the current view:

1. Navigate to a **Device List** that contains the devices that you want to unmanage.
   
   For information on navigating to a **Device List**, see "Navigating to the device list" (page 300).

2. Click the checkbox ☐ to the left of the devices you want to unmanage from the selected view’s **Device List**.

3. Click **Unmanage** to unmanage the selected devices.

4. Review the results of the operation in the **Device List** page.

   Unmanaging devices does not remove them from views nor does it delete the devices from IMC. To remove devices from custom views, see "Remove" (page 302).

   To delete devices from IMC, see "Delete" (page 302).

### Synchronize

With the **Synchronize** option, you can update IMC views with current data for the selected devices. When an operator uses the **Synchronize** option, IMC queries the selected device and then updates the current page with any updated information.

To synchronize devices from the current view:

1. Navigate to a **Device List** that contains the devices that you want to synchronize.
   
   For information on navigating to a **Device List**, see "Navigating to the device list" (page 300).

2. Click the checkbox ☐ to the left of the devices you want to synchronize from the selected view’s **Device List**.

3. Click **Synchronize** to synchronize the selected devices.

4. Review the results of the operation in the **Device List** page.

5. Click **Refresh** to update the current page with current information from the **Synchronize** process.
Refresh

With the **Refresh** option, you can reload the current **Device List** page and capture any updates to device details or other dynamic data found on this page. This feature is particularly useful when you use the **Synchronize** option to query the selected device for updated information.

To refresh devices from the current view:

1. Navigate to a **Device List** that contains the devices that you want to refresh.
   For information on navigating to a **Device List**, see "Navigating to the device list" (page 300).

2. Click the checkbox to the left of the devices you want to refresh from the selected view’s **Device List**.

3. Click **Refresh** to refresh the selected devices.
   The refreshed page appears.

SNMP settings

From the **Device List**, you can easily and quickly access IMC’s batch operation feature for configuring **SNMP** settings for one or more devices.

To access IMC’s Batch Operation for **SNMP** settings for devices from the **Device List**:

1. Navigate to a **Device List** that contains the devices that you want to configure **SNMP** settings for.
   For information on navigating to a **Device List**, see "Navigating to the device list" (page 300).

2. Click the checkbox to the left of the devices you want to manage the **SNMP** settings for from the selected view’s **Device List**.

3. Click **More**.

4. Select **SNMP Settings** from the list.
   The **Resource**→**Batch Operation**→**SNMP Settings** page appears.

5. Configure and apply the **SNMP** settings for batch mode operation.
   For information on using batch operations in to configure multiple devices, see "Using batch mode to configure **SNMP** settings" (page 276).

Telnet settings

From the **Device List**, you can easily and quickly access IMC’s batch operation feature for configuring **Telnet** settings for one or more devices.

To access IMC’s Batch Operation for **Telnet** settings for devices from the **Device List**:

1. Navigate to a **Device List** that contains the devices that you want to configure **Telnet** settings for.
   For information on navigating to a **Device List**, see "Navigating to the device list" (page 300).

2. Click the checkbox to the left of the devices you want to manage the **Telnet** settings for from the selected view’s **Device List**.

3. Click **More**.

4. Select **Telnet Settings** from the list.
   The **Resource**→**Batch Operation**→**Telnet Settings** page appears.

5. Configure and apply the **Telnet** settings for batch mode operation.
For information on using batch operations to configure Telnet settings on multiple devices, see "Using batch mode to configure Telnet settings" (page 278).

**Check Telnet settings**

You can also check Telnet settings on managed devices using IMC’s batch operations feature accessed from the *Device List*.

To check IMC’s Telnet settings for devices from the *Device List* using batch operations:

1. Navigate to a *Device List* that contains the devices that you want to check Telnet settings for. For information on navigating to a *Device List*, see "Navigating to the device list" (page 300).
2. Click the checkbox to the left of the devices you want to check the Telnet settings for from the selected view’s *Device List*.
3. Click *More*.
4. Select *Check Telnet Settings* from the list. The *Resource*→*Batch Operation*→*Check Telnet Settings* page appears.
5. Configure and apply the *Check Telnet Settings* for batch mode operation. For information on using Batch Operations to check the Telnet settings for multiple devices see "Using batch mode to check Telnet settings" (page 283).

**SSH settings**

You can also easily and quickly access IMC’s batch operations for configuring SSH settings directly from the *Device List*.

To configure IMC’s SSH settings for devices from the *Device List* using batch operations:

1. Navigate to a *Device List* that contains the devices that you want to configure SSH settings for. For information on navigating to a *Device List*, see "Navigating to the device list" (page 300).
2. Click the checkbox to the left of the devices you want to manage the SSH settings for from the selected view’s *Device List*.
3. Click *More*.
4. Select *SSH Settings* from the list. The *Resource*→*Batch Operation*→*SSH Settings* page appears.
5. Configure and apply the *SSH Settings* for batch mode operation. For information on using Batch Operations to configure SSH settings on multiple devices, see "Using batch mode to configure SSH settings" (page 279).

**Check SSH settings**

You can also check SSH settings on managed devices using IMC’s batch operations feature accessed from the *Device List*.

To check IMC’s SSH settings for devices from the *Device List* using batch operations:

1. Navigate to a *Device List* that contains the devices that you want to check SSH settings for. For information on navigating to a *Device List*, see "Navigating to the device list" (page 300).
2. Click the checkbox to the left of the devices you want to manage the SSH settings for from the selected view’s *Device List*. 
3. Click More.

4. Select **Check SSH Settings** from the list.
   The Resource → Batch Operation → Check SSH Settings page appears.

5. Configure and apply the **Check SSH Settings** for batch mode operation.
   For information on using Batch Operations to check SSH settings on multiple devices, see "Using batch mode to check SSH settings" (page 283).

**Poll interval settings**

You can also modify configuration and status poll settings on managed devices using IMC’s batch operations feature accessed from the **Device List**.

To configure IMC’s configuration and status poll settings for devices from the **Device List** using batch operations:

1. Navigate to a **Device List** that contains the devices that you want to configure configuration and status polling settings for.
   For information on navigating to a **Device List**, see "Navigating to the device list" (page 300).

2. Click the checkbox to the left of the devices you want to manage the poll configurations for from the selected view’s **Device List**.

3. Click More.

4. Select **Poll Interval Settings** from the list.
   The Resource → Batch Operation → Poll Interval page appears.

5. Configure and apply the **Poll Interval** settings for batch mode operation.
   For information on using Batch Operations to configure polling intervals on multiple devices, see "Using batch mode to configure polling intervals" (page 280).

**Save configuration**

You can also save the configurations of one or more managed devices using IMC’s batch operations feature accessed from the **Device List**.

To save the configuration for one or more devices from the **Device List** using batch operations:

1. Navigate to a **Device List** that contains the devices that you want to save the configuration of.
   For information on navigating to a **Device List**, see "Navigating to the device list" (page 300).

2. Click the checkbox to the left of the devices you want to save the configuration of from the selected view’s **Device List**.

3. Click More.

4. Select **Save Configuration** from the list.
   The Resource → Batch Operation → Save Configuration page appears.

5. Configure and apply the **Save Configuration** settings for batch mode operation.
   For information on using Batch Operations to save the configuration of multiple devices, see "Using batch mode to save device configurations" (page 284).
Reboot device

You can also reboot one or more devices using IMC’s batch operations feature accessed from the Device List.

To reboot one or more devices from the Device List using batch operations:

1. Navigate to a Device List that contains the devices that you want to reboot.
   For information on navigating to a Device List, see "Navigating to the device list" (page 300).
2. Click the checkbox to the left of the devices you want to reboot from the selected view’s Device List.
3. Click More.
4. Select Reboot Device from the list.
   The Resource→Batch Operation→Reboot Device page appears.
5. Configure and apply the Reboot Device settings for batch mode operation.
   For information on using Batch Operations to reboot multiple devices, see "Using batch mode to reboot devices" (page 285).

Add monitor

You can also monitor one or more devices from the Device List.

To monitor one or more devices from the Device List:

1. Navigate to a Device List that contains the devices that you want to monitor.
   For information on navigating to a Device List, see "Navigating to the device list" (page 300).
2. Click the checkbox to the left of the devices you want to monitor from the selected view’s Device List.
3. Click More.
4. Select Add Monitor from the list.
   The Add Monitor dialog box appears.
5. Configure and apply the Add Monitor settings.
   For information on using Add Monitor to monitor multiple devices, see "Adding a monitor" (page 637).

Cancel monitor

You can also cancel monitor to one or more devices from the Device List.

To cancel monitor to one or more devices from the Device List:

1. Navigate to a Device List that contains the devices that you want to cancel monitor.
   For information on navigating to a Device List, see "Navigating to the device list" (page 300).
2. Click the checkbox to the left of the devices you want to cancel monitor from the selected view’s Device List.
3. Click More.
4. Select Cancel Monitor from the list.
   The Cancel Monitor dialog box appears.
5. Click **OK** to cancel monitoring the selected devices.

   For information on using Batch Operations to cancel monitor to multiple devices, see "Deleting a monitor" (page 638).

**Deploy software**

You can also deploy software to one or more devices using IMC’s configuration center features directly from the **Device List**.

**To deploy software to one or more devices from the **Device List**:**

1. Navigate to a **Device List** that contains the devices that you want to deploy software to.

   For information on navigating to a **Device List**, see "Navigating to the device list" (page 300).

2. Click the checkbox □ to the left of the devices you want to deploy software to from the selected view’s **Device List**.

3. Click **More**.

4. Select **Deploy Software** from the list.

   The **Resource→Batch Operation→Deploy Software** page appears.

5. Configure and apply the **Deploy Software** settings.

   For information on deploying software in IMC using IMC’s configuration center, see "Deploying configurations and software by using IMC’s deployment guide" (page 442).

**Backup configuration**

You can also back up device configurations for one or more devices using IMC’s configuration center features directly from the **Device List**.

**To back up device configurations for one or more devices from the **Device List**:**

1. Navigate to a **Device List** that contains the devices that you want to backup the configuration of.

   For information on navigating to a **Device List**, see "Navigating to the device list" (page 300).

2. Click the checkbox □ to the left of the devices you want to backup the configuration of from the selected view’s **Device List**.

3. Click **More**.

4. Select **Backup Configuration** from the list.

   IMC initiates the backup request upon selection of this menu option. IMC also updates the page with the **Configuration File Backup Results**.

   For information on backing up device configurations in IMC using IMC’s configuration center, see "Managing automatic backup plans" (page 475).

**Navigating to the device list**

The Device list lets you manage multiple devices. You can access the Device List from the **Device View**, the **IP View**, and the **Custom View**. This section explains the navigation options to the Device List.

**Navigating to the device list from the device view**

To navigate to the **Device List** from the **Device View**: 

1. **Navigate to Resource→View Management→View←Device Type**.
2. Click the **Resource** tab from the tabular navigation system on the top.
3. Click **View Management** on the navigation tree on the left.
4. Click **Device View** under **View Management** from the navigation system on the left.
5. Click the expand icon 📚 to the left of the **Device View** on the navigation tree on the left.
6. Click the category of device view you want to access. The **Device List** for the device category you choose appears.
7. Click **Device View** from the navigation system for the Device List for all devices.
8. For the **Device List** for all devices, click **Device View** from the navigation system.
9. To view all device groups under **Device View**, click the expand icon 📚.
   - For the **Device List** for routers, click 📚 Routers under **Device View** from the navigation system on the left, or
   - For the **Device List** for switches, click 📚 Switches under **Device View** from the navigation system on the left, or
   - For the **Device List** for servers, click 📚 Servers under **Device View** from the navigation system on the left, or
   - For the **Device List** for all security devices, click 📚 Security under **Device View** from the navigation system on the left, or
   - For the **Device List** for all wireless devices, click 📚 Wireless under **Device View** from the navigation system on the left, or
   - Click 📚 Storage under **Device View** from the navigation tree on the left for a summary view of all storage devices, or
   - For the **Device List** for voice devices, click 📚 Voice under **Device View** from the navigation system on the left, or
   - For the **Device List** for desktop devices, click 📚 Desktop under **Device View** from the navigation system on the left, or
   - For the **Device List** for other devices, click 📚 other under **Device View** from the navigation system on the left.

**Navigating to the device list from the IP view**

To navigate to the device list from the IP View:
1. Navigate to **Resource → IP View → Subnet-<Subnet IP Address>**.
2. Click the **Resource** tab from the tabular navigation system on the top.
3. Click **IP View** on the navigation tree on the left. To view all IP subnets under **IP View**, click the expand icon 📚 to the left of **IP View**.
4. Click the IP subnet view you want to access. The **Device List** for the IP subnet you choose appears.
IMC displays all devices in the IP View in the Device List displayed in the main pane of the IP View window.

Navigating to the device list from a custom view:

To navigate to the device list from a custom view:
1. Navigate to Resource → Custom View → <View Name>.
2. Click the Resource tab from the tabular navigation system on the top.
3. Click View Management on the navigation tree on the left.
4. Click Custom View under View Management from the navigation system on the left.
5. To view all custom views under Custom View, click the expand icon to the left of the Custom View tree.
6. Click the custom view you want to access. The Device List for the custom view you choose appears.
IMC displays all devices in the Custom View in the Device List displayed in the main pane of the Custom View.

Device list management options

From the Device List, you can add, remove, delete, manage/unmanage devices, and synchronize and refresh data for device details. You can also select one or more devices from the Device List and then launch batch operations for configuring SNMP, Telnet, and SSH settings. In addition, you can check Telnet and SSH settings.

Add

The Add option lets you add devices that already exist in IMC to the current custom view. The Add feature is only available for Custom Views.
To add a device to the current custom view:
1. Navigate to the Custom View in which you want to add devices
   For information on navigating to a Device List from a custom view, see "Navigating to the Device List of a Custom View."
2. Click Add from the selected Custom View’s Device List.
   You can add devices by using either the View or Advanced query option. See "Adding devices by View" (page 85) and "Adding devices by Advanced query" (page 85).
3. Highlight the devices you want to select and click the Add selected add them to the Selected Devices list.
4. Do one of the following:
   o To select all of the devices displayed in the Devices Found list, click Add all, or
   o To remove one or more devices, select them and click Remove selected, or
   o To remove all of the selected devices, click Remove all.
5. Confirm that the devices you have found is added to the Selected Devices portion of the configuration window.
6. Click OK.
7. Confirm that the devices now appear in the custom view Device List.

Remove

The Remove feature is only available for Custom Views and only from the Device List level of a Custom View.

To remove a device from the current custom view:

1. Navigate to the Custom View in which you want to remove devices.
2. Click the checkbox □ to the left of the devices you want to remove from the selected custom view’s Device List.
   For information on navigating to a Device List from a custom view, see “Navigating to the device list from a custom view” (page 301).
3. Click the checkbox □ to the left of the devices you want to remove from the selected custom view’s Device List.
   For information on navigating to a Device List, see “Navigating to the” (page 300).
4. Click Remove to remove the devices from the selected custom view’s Device List.
5. Click OK to confirm the removal of the selected devices from the custom view.

Delete

Delete removes the selected devices from IMC. IMC immediately purges all data associated with the deleted devices. The Delete feature is only available for Device Views and IP Views.

To delete devices from the current view:

1. Navigate to a Device List that contains the devices that you want to delete.
   For information on navigating to a Device List, see “Navigating to the” (page 300).
2. Click the checkbox □ to the left of the devices you want to delete from a Device View or IP View Device List.
3. Click Delete to manage the selected devices.
4. Review the results of the operation in the Device List page.

⚠️ WARNING:
You cannot recover a device or associated data once you have deleted it. Use this feature with caution.

Manage

Managing a device enables all relevant IMC management, monitoring, and reporting features to be applied to the selected devices. Managing a device therefore consumes IMC node licenses.

To manage devices from the current view:

1. Navigate to a Device List that contains the devices that you want to manage.
   For information on navigating to a Device List, see “Navigating to the” (page 300).
2. Click the checkbox □ to the left of the devices you want to manage from the selected view’s Device List.
3. Click Manage to manage the selected devices.
4. Review the results of the operation in the **Device List** page.

⚠️ **WARNING:**
Be aware of the impact of managing devices. Managed devices consume node licenses in IMC. For a current license count, click the **About** link in the upper right corner of IMC.

**Unmanage**

Unmanaging a device disables all relevant IMC management, monitoring, and reporting features for the selected devices. Unmanaging a device therefore recovers IMC node licenses.

To unmanage devices from the current view:
1. Navigate to a **Device List** that contains the devices that you want to unmanage.
   For information on navigating to a **Device List**, see "Navigating to the **Device List**" (page 300).
2. Click the checkbox ☐ to the left of the devices you want to unmanage from the selected view’s **Device List**.
3. Click **Unmanage** to unmanage the selected devices.
4. Review the results of the operation in the **Device List** page.

Unmanaging devices does not remove them from views nor does it delete the devices from IMC. To remove devices from custom views, see "Remove" (page 302).
To delete devices from IMC, see "Delete" (page 302).

**Synchronize**

With the **Synchronize** option, you can update IMC views with current data for the selected devices. When an operator uses the **Synchronize** option, IMC queries the selected device and then updates the current page with any updated information.

To synchronize devices from the current view:
1. Navigate to a **Device List** that contains the devices that you want to synchronize.
   For information on navigating to a **Device List**, see "Navigating to the **Device List**" (page 300).
2. Click the checkbox ☐ to the left of the devices you want to synchronize from the selected view’s **Device List**.
3. Click **Synchronize** to synchronize the selected devices.
4. Review the results of the operation in the **Device List** page.
5. Click **Refresh** to update the current page with current information from the **Synchronize** process.

**Refresh**

With the **Refresh** option, you can reload the current **Device List** page and capture any updates to device details or other dynamic data found on this page. This feature is useful when you use the **Synchronize** option to query the selected device for updated information.

To refresh devices from the current view:
1. Navigate to a **Device List** that contains the devices that you want to refresh.
   For information on navigating to a **Device List**, see "Navigating to the **Device List**" (page 300).
2. Click the checkbox ☑ to the left of the devices you want to refresh from the selected view’s **Device List**.
3. Click **Refresh** to refresh the selected devices.
   The refreshed page appears.

**SNMP settings**

From the **Device List**, you can quickly access the batch operation feature for configuring SNMP settings for one or more devices.

To access the batch operation for SNMP settings for devices from the **Device List**:
1. Navigate to a **Device List** that contains the devices in which you want to configure SNMP settings.
   For information on navigating to a **Device List**, see “Navigating to the” (page 300).
2. Click the checkbox ☑ to the left of the devices you want to manage the SNMP settings for from the selected view’s **Device List**.
3. Click **More**.
4. Select **SNMP Settings** from the list.
   The **Resource→Batch Operation→SNMP Settings** page appears.
5. Configure and apply the SNMP settings for batch mode operation.
   For information on using batch operations in to configure multiple devices, see "Using batch mode to configure SNMP settings" (page 276).

**Telnet settings**

From the **Device List**, you can quickly access the batch operation feature for configuring Telnet settings for one or more devices.

To access the batch operation for Telnet settings for devices from the **Device List**:
1. Navigate to a **Device List** that contains the devices for which you want to configure Telnet settings.
   For information on navigating to a **Device List**, see “Navigating to the” (page 300).
2. Click the checkbox ☑ to the left of the devices you want to manage the Telnet settings for from the selected view’s **Device List**.
3. Click **More**.
4. Select **Telnet Settings** from the list.
   The **Resource→Batch Operation→Telnet Settings** page appears.
5. Configure and apply the Telnet settings for batch mode operation.
   For information on using Batch Operations to configure Telnet settings on multiple devices, see "Using batch mode to configure Telnet settings" (page 278).

**Check Telnet settings**

You can check Telnet settings on managed devices using the IMC batch operations feature accessed from the **Device List**.

To check the Telnet settings for devices from the **Device List** using batch operations:
1. Navigate to a Device List that contains the devices in which you want to check Telnet settings.
   For information on navigating to a Device List, see "Navigating to the Device List" (page 300).

2. Click the checkbox to the left of the devices you want to check the Telnet settings for from the selected view’s Device List.

3. Click More.

4. Select Check Telnet Settings from the list.

   The Resource → Batch Operation → Check Telnet Settings page appears.

5. Configure and apply the Check Telnet Settings for batch mode operation.

   For information on using Batch Operations to check the Telnet settings for multiple devices, see "Using batch mode to configure Telnet settings" (page 278).

### SSH settings

You can quickly access the Batch Operations for configuring SSH settings directly from the Device List.

To configure SSH settings for devices from the Device List using batch operations:

1. Navigate to a Device List in which contains the devices that you want to configure SSH settings.
   For information on navigating to a Device List, see "Navigating to the device list" (page 300).

2. Click the checkbox to the left of the devices you want to manage the SSH settings for from the selected view’s Device List.

3. Click More.

4. Select SSH Settings from the list.

   The Resource → Batch Operation → SSH Settings page appears.

5. Configure and apply the SSH Settings for batch mode operation.

   For information on using Batch Operations to configure SSH settings on multiple devices, see "Using batch mode to configure SSH settings" (page 279).

### Check SSH settings

You can check SSH settings on managed devices using the IMC batch operations feature accessed from the Device List.

To check the SSH settings for devices from the Device List using batch operations:

1. Navigate to a Device List that contains the devices in which you want to check SSH settings.
   For information on navigating to a Device List, see "Navigating to the device list" (page 300).

2. Click the checkbox to the left of the devices you want to manage the SSH settings for from the selected view’s Device List.

3. Click More.

4. Select Check SSH Settings from the list.

   The Resource → Batch Operation → Check SSH Settings page appears.

5. Configure and apply the Check SSH Settings for batch mode operation.

   For information on using Batch Operations to check SSH settings on multiple devices, see "Using batch mode to check SSH settings" (page 283).
Poll interval settings

You can modify Configuration and Status poll settings on managed devices using the IMC batch operations feature accessed from the Device List.

To configure configuration and status poll settings for devices from the Device List using batch operations:

1. Navigate to a Device List that contains the devices in which you want to configure configuration and status polling settings.
   For information on navigating to a Device List, see "Navigating to the device list" (page 300).
2. Click the checkbox to the left of the devices you want to manage the poll configurations for from the selected view’s Device List.
3. Click More.
4. Select Poll Interval Settings from the list.
   The Resource→Batch Operation→Poll Interval page appears.
5. Configure and apply the Poll Interval settings for batch mode operation.
   For information on using Batch Operations to configure polling intervals on multiple devices, see "Using batch mode to configure polling intervals" (page 280).

Save configuration

You can save the configurations of one or more managed devices using the IMC batch operations feature accessed from the Device List.

To save the configuration for one or more devices from the Device List using batch operations:

1. Navigate to a Device List that contains the devices in which you want to save the configuration.
   For information on navigating to a Device List, see "Navigating to the device list" (page 300).
2. Click the checkbox to the left of the devices you want to save the configuration of from the selected view’s Device List.
3. Click More.
4. Select Save Configuration from the list.
   The Resource→Batch Operation→Save Configuration page appears.
5. Configure and apply the Save Configuration settings for batch mode operation.
   For information on using Batch Operations to save the configuration of multiple devices, see "Using batch mode to save device configurations" (page 284).

Reboot device

You can reboot one or more devices using the IMC batch operations feature accessed from the Device List.

To reboot one or more devices from the Device List using batch operations:

1. Navigate to a Device List that contains the devices that you want to reboot.
   For information on navigating to a Device List, see "Navigating to the device list" (page 300).
2. Click the checkbox to the left of the devices you want to reboot from the selected view’s Device List.
3. Click More.
4. Select Reboot Device from the list.
   The Resource→Batch Operation→Reboot Device page appears.
5. Configure and apply the Reboot Device settings for batch mode operation.
   For information on using Batch Operations to reboot multiple devices, see "Using batch mode to reboot devices" (page 285).

Add monitor

You can monitor one or more devices from the Device List.

To monitor one or more devices from the Device List:
1. Navigate to a Device List that contains the devices that you want to monitor.
   For information on navigating to a Device List, see "Navigating to the device list" (page 300).
2. Click the checkbox ☑ to the left of the devices you want to monitor from the selected view’s Device List.
3. Click More.
4. Select Add Monitor from the list.
5. The Add Monitor dialog box appears.
6. Configure and apply the Add Monitor settings.
   For information on using Add Monitor to monitor multiple devices, see "Add monitor" (page 307).

Cancel monitor

You can cancel monitor to one or more devices from the Device List.

To cancel monitor to one or more devices from the Device List:
1. Navigate to a Device List that contains the devices that you want to cancel monitor.
   For information on navigating to a Device List, see "Navigating to the device list" (page 300).
2. Click the checkbox ☑ to the left of the devices you want to cancel monitor from the selected view’s Device List.
3. Click More.
4. Select Cancel Monitor from the list.
   The Cancel Monitor dialog box appears.
5. Click OK to cancel monitoring the selected devices.
   For information on using Batch Operations to cancel monitor to multiple devices, see "Cancel monitor" (page 307).

Deploy software

You can deploy software to one or more devices using the IMC configuration center features directly from the Device List.

To deploy software to one or more devices from the Device List:
1. Navigate to a Device List that contains the devices that you want to deploy software to.
For information on navigating to a Device List, see "Navigating to the device list" (page 300).

2. Click the checkbox ☑ to the left of the devices you want to deploy software to from the selected view’s Device List.

3. Click More.

4. Select Deploy Software from the list.
   The Resource → Batch Operation → Deploy Software page appears.

5. Configure and apply the Deploy Software settings.
   For information on deploying software in IMC using the IMC configuration center, see "Deploying configurations and software by using IMC’s deployment guide" (page 442).

Backup configuration

You can back up device configurations for one or more devices using IMC’s configuration center features directly from the Device List.

To back up device configurations for one or more devices from the Device List:

1. Navigate to a Device List that contains the devices for which you want to backup the configuration.
   For information on navigating to a Device List, see "Navigating to the device list" (page 300).

2. Click the checkbox to the left of the devices you want to backup the configuration of from the selected view’s Device List.

3. Click More.

4. Select Backup Configuration from the list.
   IMC initiates the backup request upon selection of this menu option. IMC also updates the page with the Configuration File Backup Results.
   For information on backing up device configurations in IMC using the IMC configuration center, see "Managing automatic backup plans" (page 475).

Terminal access

IMC lets you manage IP address resources in IMC. You can track, locate, allocate, and bind desktop IP addresses to network access resources. While the primary focus of IP address management in IMC is the desktop servers, printers and other devices can also be tracked using the IMC Terminal Access features.

The purpose of allocating and binding IP addresses in IMC is to enable IMC to track its intended use, such as when an operator binds a terminal to some interfaces or an interface to some terminal and to alarm when its use has changed. Therefore, allocating and binding IP addresses to network access devices is done in IMC only, not on the device itself.

To support effective IP address management, IMC lets you add IP addresses to the IMC database and centrally manage their allocation and binding. You can manually add IP addresses or they can be added automatically using the IMC auto scan feature. In addition, you can define IP segments based on departments or work areas.

IMC lets you manage the allocation of IP addresses for reporting and alarming purposes. When an operator assigns an IP address to a device in IMC, it tracks that assignment and reports on any
changes to the assignment. This feature provides visibility into which IP addresses have been assigned, and when unauthorized uses of IP addresses occur.

IMC also supports the ability to bind terminal resources for security purposes. You can bind an IP address to a MAC address. In addition, you can bind a terminal to some interfaces. Binding IP addresses enables IMC to track IP and MAC address usage to a specific resource and to proactively notify you when that resource is not used in the way it was intended.

You can bind IP addresses to MAC addresses manually or they can use the auto-scanning feature. With this feature, IMC identifies IP address and MAC address combination pairs, in which you then can selectively apply binding.

With terminal access binding and switch access binding, you can link the MAC address of an end device to an interface on an access device. This enables IMC to identify when a device has been moved or when a new device is accessing the network through an interface not assigned to it.

IMC also lets you locate IP or MAC addresses in the network infrastructure. This feature is useful for pinpointing to which access device a particular user is located when some information about the user is known. This is useful both for troubleshooting network issues and tracking down security problems in the network infrastructure.

**Allocating IP addresses**

IMC lets you manage the allocation of IP addresses for reporting and alarming purposes. You can add an IP segment and perform an auto scan for or assign IP addresses to the IP segment. You can create child IP segments under an IP segment, and can build an IP segment structure of at most five levels. You can perform a global auto scan, and then IMC automatically adds the IP addresses to existing IP segments. If the IP addresses do not belong to any existing IP segment, IMC adds them to the system default IP segment.

In addition, you can batch import IP addresses to IMC from a file, such as the IP address file of a DHCP server. The following section provides you with information on the IMCIP address allocation features.

**Viewing the IP segment list**

IMC provides you with the ability to view existing IP address allocations.

To view IMC existing IP address allocations:

1. Navigate to Resource→IP Address Allocation.
2. Click the Resource tab from the tabular navigation system on the top.
3. Click Terminal Access on the navigation tree on the left.
4. Click IP Address Allocation under Terminal Access from the navigation tree on the left.

The IP Segment List is displayed in the IP Address Allocation page.

**IP Segment List**

- **IP Segment**: Contains the IP segments that have been created. The IP segment serves as an active link to display allocated IP list of the IP segment.

**Allocated IP List**

- **IP Address**: Contains the IP address that has been allocated.
Adding an IP segment

You can manually add an IP segment in IMC in advance according to the actual IP segment plan.

To manually add an IP segment in IMC:

1. Navigate to Resource→IP Address Allocation.
2. Click the Resource tab from the tabular navigation system on the top.
3. Click Terminal Access on the navigation tree on the left.
4. Click IP Address Allocation under Terminal Access from the navigation tree on the left. The IP Segment List is displayed in the IP Address Allocation page.
5. Click Add IP Segment.
6. Enter the start IP address to be allocated in the Start IP field.
7. Enter the end IP address to be allocated in the End IP field.
8. Enter the owner of the IP segment in the Owner field.
9. Select one or more operator groups in Operator Group field.

Operators in different operator groups can have different rights to the IP segment. Using IIP Address allocation auto scanning feature discovers IP addresses and the devices associated
with them. IMC auto populates the device name, type and description fields when the information is available, thus ensuring consistency in naming conventions across management modules in IMC. HP recommends using the auto scanning feature whenever possible.

10. Enter a brief description for this IP segment in the Description field.
11. Click OK.

Modifying an IP segment

To modify an existing IP segment:

1. Navigate to Resource→IP Address Allocation.
2. Click the Resource tab from the tabular navigation system on the top.
3. Click Terminal Access on the navigation tree on the left.
4. Click IP Address Allocation under Terminal Access from the navigation tree on the left. The IP Segment List is displayed in the IP Address Allocation page.
5. Click the Modify icon associated with the IP address allocation you want to modify. You cannot modify the start and end IP addresses once you have created the IP segment. To change the IP segment, you must delete the existing IP segment and create a new IP segment entry.
6. Modify the owner of the IP segment that is granted the IP segment in the Owner field as needed.
7. Re-select the operator group in the Operator Group field for performing this IP segment. You cannot perform this operation in a child IP segment.
8. Modify the description for this IP segment in the Description field.
9. Click OK.

Restoring an IP segment

To restore an existing IP segment:

1. Navigate to Resource→IP Address Allocation.
2. Click the Resource tab from the tabular navigation system on the top.
3. Click Terminal Access on the navigation tree on the left.
4. Click IP Address Allocation under Terminal Access from the navigation tree on the left. The IP Segment List is displayed in the IP Address Allocation page.
5. Click the Restore icon associated with the IP segment you want to restore.
6. Click OK to confirm the restoration of the IP segment.
7. Review the results of the operation on the IP Address Allocation page.

Manually allocating IP addresses

You can manually assign IP addresses in the IP segment to devices.

To allocate an IP address to a device manually:

2. Click the Resource tab from the tabular navigation system on the top.
3. Click **Terminal Access** on the navigation tree on the left.

4. Click **IP Address Allocation** under **Terminal Access** from the navigation tree on the left.

5. Click the IP segment in the **IP Address** field of the **IP Segment List** that you want to allocate an IP address from.

   The **Allocated IP List** for the selected IP segment is displayed in the lower half of the page.

6. Click **Allocate**.

7. Select an allocation type from the **IP Address Allocation Type** list.

   The options include **Allocate One IP** and **Allocate IPs in Batch**:
   - If you selected **Allocate One IP** in Step 3, enter the IP address, or
   - If you selected **Allocate IPs in Batch** in Step 3, enter the start IP address, or
   - If you selected **Allocate IPs in Batch** in Step 3, enter the end IP address.

8. Enter the owner in the **Owner** field.

9. Enter the description in the **Description** field.

10. Click **OK**.

### Allocating IP addresses using the auto scanning feature

You can use the auto scanning feature to identify all IP addresses in use and then add them to the IP address management system. This feature allows you to easily and proactively manage IP address resources.

To add IP addresses using IMC’s auto scanning feature:

1. Navigate to **Resource** → **IP Address Allocation**.
2. Click the Resource tab from the tabular navigation system on the top.
3. Click **Terminal Access** on the navigation tree on the left.
4. Click **IP Address Allocation** under **Terminal Access** from the navigation tree on the left.
   
   The **IP Segment List** appears.

5. Click the **Auto Scanning** link located in the far right corner of the **IP Segment List**.

6. Enter the first usable IP address in the range of IP addresses you want to identify in the **Start IP** field.

7. Enter the last usable IP address in the range of IP addresses you want to identify in the **End IP** field.

8. Click **Add** to add the IP Segment to the **Configured Segments** list.

9. Repeat Steps 3-5 until you have added all of the IP segments you want to scan the network for.

10. Click **OK** to begin the IP address auto scanning process.

   All IP addresses discovered by auto scanning are unallocated. You can manually allocate them to terminals.

11. Click the checkbox ☑ to the left for each IP address you want to allocate to the associated device.
12. Click the first empty checkbox in the upper left corner of the list to select all IP addresses in the list for the current page.

13. Click Allocate.

14. Review the results of your allocation in the IP Address Allocation Result list.

After auto scanning, the IP addresses are automatically added to existing IP segments. If the IP addresses do not belong to any existing IP segment, they are automatically added to the system default IP segment.

Allocating IP addresses using the import IP address feature

You can use the import IP address feature to batch import IP addresses from an IP address file or a DHCP server. This feature lets you quickly import IP addresses to Terminal Access in batches.

To add IP addresses using IMC’s import IP address feature:

1. Navigate to Resource → IP Address Allocation.
2. Click the Resource tab from the tabular navigation system on the top.
3. Click Terminal Access on the navigation tree on the left.
4. Click IP Address Allocation under Terminal Access from the navigation tree on the left. The IP Segment List appears.
5. Click Import IP Address.
6. Click Browse to select the imported file.
7. Select Yes or No in the Import First Row field.
8. Enter the separator in the Column Separator File field.
9. Enter the Index of IP Address Column.
10. Enter the owner in the Owner field.
11. Enter the description in the Description field.
12. Click OK.
13. Review the results of IP address import in the IP Import Results page.

Restoring IP address allocations

Restoring an IP address returns the IP address to the pool of available addresses.

To restore multiple IP addresses:

1. Navigate to Resource → IP Address Allocation.
2. Click the Resource tab from the tabular navigation system on the top.
3. Click Terminal Access on the navigation tree on the left.
4. Click IP Address Allocation under Terminal Access from the navigation tree on the left. The IP Segment List appears.
5. Click the IP segment that includes the IP addresses you want to restore.
   The Allocated IP List appears.
6. Click the checkbox ☑ to the left for each IP address you want to restore.
7. Click the first empty checkbox in the upper corner of the list to select all IP addresses in the list for the current page.

8. Click Restore.

9. Click OK to confirm the restoration of the selected IP addresses.

10. Review the results of your allocation in the Restore IP Address page.

To restore a single IP address, from the Allocated IP List, click the Restore icon associated with the IP address you want to restore. The child IP segments under the IP segment, if any, is also restored.

Unauthorized access

The Unauthorized Access provides you with the ability to view the terminals that did not comply with the access policies, the unauthorized access logs, and how they were handled by IMC.

Viewing unauthorized access list

The Unauthorized Access List shows you the terminals that did not comply with the access policies.

To view the Unauthorized Access List:


2. Click the Resource tab from the tabular navigation system on the top.

3. Click the Terminal Access section of the navigation tree on the left.

4. Click Unauthorized Access under Terminal Access from the navigation tree on the left.

   The Unauthorized Access List is displayed in the main portion of the Unauthorized Access page.

Unauthorized access list

- Terminal MAC: Contains the MAC address of the unauthorized access terminal.
- Terminal Name: Contains the name of the unauthorized access terminal. If a DNS server is configured in IMC system settings, IMC resolves the domain name of the terminal by using the DNS server. For more information on configuring DNS server, see System "System settings" (page 144). If the IMC cannot retrieve the terminal domain name from the DNS server and the IMC is configured with a DHCP server, the IMC retrieves the terminal domain name from the DHCP server. For how to configure the DHCP server, see the "HP Intelligent Management Center Installation Guide."
- Terminal IP: Contains the IP address of the unauthorized access terminal.
- Device Label: Contains the IMC name for the device, which, by default, is the name assigned to it in its device configuration.
- Device IP: Contains the IP address of the access device.
- Interface Description: Contains the description of the interface connected to the terminal.
- Status: Contains the process status.
- Unauthorized Access Log: Contains a link for navigating to the Unauthorized Access Log List page of the current terminal.
If the Unauthorized Access List contains enough entries, the following navigational aids are displayed:

- Click ➡️ to page forward in the Unauthorized Access List.
- Click ➡️ to page forward to the end of the Unauthorized Access List.
- Click ⬅️ to page backward in the Unauthorized Access List.
- Click ⬅️ to page backward to the front of the Unauthorized Access List.

5. Click 8, 15, 50, 100, or 200 from the right side of the main pane to configure how many items per page you want to view.

6. For the Unauthorized Access List that have more than one page, click 1, 2, 3, 4, 6, 7, 8, 9, 10... from the upper middle or bottom right side of the main pane to jump to a particular page of the list.

   You can sort the Unauthorized Access List by most fields. Click the column label to sort the list by the selected field. The column label is a toggle switch that lets you toggle between the various sort options specific to each field.

**Querying the unauthorized access list**

IMC provides the ability to query the Unauthorized Access List.

To query the Unauthorized Access List:

2. Click the Resource tab from the tabular navigation system on the top.
3. Click the Terminal Access section of the navigation tree on the left.
4. Click Unauthorized Access under Terminal Access from the navigation tree on the left.

The Unauthorized Access List displays in the main portion of the Unauthorized Access page.

5. Move the pointer over Query at the upper right corner of Unauthorized Access List, and a search criteria dialog box appears.

6. Enter one or more of the following search criteria in the dialog box:
   - **Terminal MAC**: Enter the MAC address in the Terminal MAC field.
   - **Terminal IP**: Enter the IP address in the Terminal IP field.
   - **Terminal Name**: Enter the terminal name in the Terminal Name field.
   - **Device Label**: Enter the device label in the Device Label field.
   - **Device IP**: Enter the IP address of the access device in the Device IP field.
   - **Interface Description**: Enter the description of the interface connected to the terminal in the Interface Description field.
   - **Status**: Select the process status from the Status list.

7. Click Query.
8. Click Reset when you have finished your search to restore the full Unauthorized Access List.

**Viewing the unauthorized access log list**

To view the Unauthorized Access Log List

2. Click the **Resource** tab from the tabular navigation system on the top.

3. Click the **Terminal Access** section of the navigation tree on the left.

4. Click **Unauthorized Access** under **Terminal Access** from the navigation tree on the left. The **Unauthorized Access List** is displayed in the main portion of the **Unauthorized Access** page.

5. Click the **All Unauthorized Access Log** link located in the upper right corner of the **Unauthorized Access List**.
   
   The **Unauthorized Access Log List** is displayed in the main portion of the **Unauthorized Access Log List** page.

**Unauthorized access log list**

- **Action Status**: Contains the status of the action taken for the unauthorized access.
- **Terminal MAC**: Contains the MAC address of the unauthorized access terminal.
- **Terminal Name**: Contains the name of the unauthorized access terminal. If a DNS server is configured in IMC system settings, IMC resolves the domain name of the terminal by using the DNS server. For more information on configuring DNS server, see "System settings" (page 144).
- **Terminal IP**: Contains the IP address of the unauthorized access terminal.
- **Device Label**: Contains the IMC name for the device, which, by default, is the name assigned to it in its device configuration.
- **Device IP**: Contains the IP address of the access device.
- **Interface**: Contains the description of the interface connected to the terminal.
- **Conflict Type**: Contains the conflict type.
- **Found Time**: Contains the time when the unauthorized access was detected.
- **Details**: Contains a link for navigating to the **Unauthorized Access Log List Details** page.

If the **Unauthorized Access Log List** contains enough entries, the following navigational aids appear.

- Click **»** to page forward in the **Unauthorized Access Log List**.
- Click **»»** to page forward to the end of the **Unauthorized Access Log List**.
- Click **«** to page backward in the **Unauthorized Access Log List**.
- Click **««** to page backward to the front of the **Unauthorized Access Log List**.

6. Click 8, 15, 50, 100, or 200 from the right side of the main pane to configure how many items per page you want to view.

7. For **Unauthorized Access Log List** that have more than one page, click on 1, 2, 3, 4, 5, 6, 7, 8, 9, 10... from the upper middle or bottom right side of the main pane to jump to a particular page of the list.

   You can sort the **Unauthorized Access Log List** by most fields. Click the column label to sort the list by the selected field. The column label is a toggle switch that lets you toggle between the various sort options specific to each field.

**Unauthorized access log query**

IMC provides you with the ability to query unauthorized access logs.
To query the Unauthorized Access Log List:

2. Click the Resource tab from the tabular navigation system on the top.
3. Click the Terminal Access section of the navigation tree on the left.
4. Click Unauthorized Access under Terminal Access from the navigation tree on the left. The Unauthorized Access List is displayed in the main portion of the Unauthorized Access page.
5. Click the All Unauthorized Access Log link located in the upper right corner of Unauthorized Access List.
   The Unauthorized Access Log List is displayed in the main portion of the Unauthorized Access Log List page.
6. Move the pointer over Query at the upper right corner of Unauthorized Access Log List, and a search criteria dialog box appears.
7. Enter one or more of the following search criteria in the dialog box:
   - Terminal MAC: Enter the MAC address in the Terminal MAC field.
   - Terminal IP: Enter the IP address in the Terminal IP field.
   - Terminal Name: Enter the terminal name in the Terminal Name field.
   - Conflict Type: Select the type of the conflict occurred from the Conflict Type list. Options include Terminal Access Binding Conflict, Switch Access Binding Conflict, Terminal/Switch Binding Conflict, and Undefined Access Binding Conflict.
   - Device Label: Enter the device label in the Device Label field.
   - Device IP: Enter the IP address of the access device in the Device IP field.
   - Interface: Enter the interface of the device to which the terminal connects in the Interface field.
   - Action Status: Select the action status from the Action Status list.
   - Found Start Time: Enter the start date and time for the query. Click the calendar icon to the right of the Found Start Time to input the start time using the calendar function.
   - Found End Time: Enter the end date and time for the query. Click the calendar icon to the right of the Found End Time to input the start time using the calendar function.
8. Click Query.
9. Click Reset when you have finished your search to restore the full Unauthorized Access Log List.

Terminal access binding

You can configure terminal access binding for the devices in the Unauthorized Access List.

2. Click the Resource tab from the tabular navigation system on the top.
3. Click the Terminal Access section of the navigation tree on the left.
4. Click Unauthorized Access under Terminal Access from the navigation tree on the left.
   The Unauthorized Access List is displayed in the main portion of the Unauthorized Access page.
5. Click the checkboxes to the left of terminal MAC address you want to configure terminal access binding to the associated terminal.
6. Click Terminal Access Binding. The Select Terminal Access Binding Type dialog box appears.
7. Select Yes or No from the Trusted list:
   o If Yes is selected, the terminal is allowed to access the network through any port, or
   o If No is selected, the terminal is only allowed to access the network through the binding ports.
8. Click OK.

Switch access binding
To configure switch access binding for the terminals in the Unauthorized Access List:
2. Click the Resource tab from the tabular navigation system on the top.
3. Click the Terminal Access section of the navigation tree on the left.
4. Click Unauthorized Access under Terminal Access from the navigation tree on the left.
5. Click the checkboxes to the left of terminal MAC address you want to configure switch access binding to the associated terminal.
6. Click Switch Access Binding. The Select Switch Access Binding Type dialog box appears.
7. Select Yes or No from the Trusted list:
   o If Yes is selected, the port allow any terminal to access the network through this port, or
   o If No is selected, the port only allow the binding terminals to access the network through this port.
8. Click OK to confirm your operation.

Delete unauthorized access entries
To delete one or more unauthorized access entries:
2. Click the Resource tab from the tabular navigation system on the top.
3. Click the Terminal Access section of the navigation tree on the left.
4. Click Unauthorized Access under Terminal Access from the navigation tree on the left.
   The Unauthorized Access List is displayed in the main portion of the Unauthorized Access page.
5. Click the checkboxes to the left for each unauthorized access entry you want to delete.
6. Click Delete.
7. Click OK to confirm your operation.

Cancel action
In the unauthorized access processing policy, you can cancel the action of shutting down a port. The canceling action is effective when the action is in the waiting state.
To cancel an action:
2. Click the Resource tab from the tabular navigation system on the top.
3. Click the Terminal Access section of the navigation tree on the left.
4. Click Unauthorized Access under Terminal Access from the navigation tree on the left. The Unauthorized Access List is displayed in the main portion of the Unauthorized Access page.
5. Click the All Unauthorized Access Log link located in the upper right corner of Unauthorized Access List. The Unauthorized Access Log List is displayed in the main portion of the Unauthorized Access Log List page.
6. Click the checkboxes to the left for each action status you want to cancel to the associated unauthorized access log entries.
7. Click Cancel Action.
8. Click OK to confirm your operation.

Refreshing the unauthorized access list
To refresh the Unauthorized Access List page:
2. Click the Resource tab from the tabular navigation system on the top.
3. Click the Terminal Access section of the navigation tree on the left.
4. Click Unauthorized Access under Terminal Access from the navigation tree on the left. The Unauthorized Access List is displayed in the main portion of the Unauthorized Access page.
5. Click Refresh to reload the web page and review any updated information.

Refreshing the unauthorized access log list
To refresh the Unauthorized Access Log List page
2. Click the Resource tab from the tabular navigation system on the top.
3. Click the Terminal Access section of the navigation tree on the left.
4. Click Unauthorized Access under Terminal Access from the navigation tree on the left. The Unauthorized Access List is displayed in the main portion of the Unauthorized Access page.
5. Click the All Unauthorized Access Log link located in the upper right corner of Unauthorized Access List. The Unauthorized Access Log List is displayed in the main portion of the Unauthorized Access Log List page.
6. Click Refresh to reload the web page and review any updated information.
History access log

With the History Access Log function, you can view history access logs of terminals in the network. IMC obtains the MAC addresses and terminal names on the device by polling the device. IMC displays the information in the format of history access logs, facilitating IP address management.

Viewing history access log list

To view the History Access Log List:
2. Click the Resource tab from the tabular navigation system on the top.
3. Click the Terminal Access section of the navigation tree on the left.
4. Click History Access Log under Terminal Access from the navigation tree on the left. The History Access Log List is displayed in the main portion of the History Access Log page.

History access log list

- **Terminal MAC**: contains the MAC address of the terminal.
- **Terminal Name**: contains the name of the terminal. If a DNS server is configured in IMC system settings, IMC resolves the domain name of the terminal by using the DNS server. For more information on configuring DNS server, "System settings" (page 144). If the IMC cannot retrieve the terminal domain name from the DNS server and the IMC is configured with a DHCP server, the IMC retrieves the terminal domain name from the DHCP server. For how to configure the DHCP server, see the "HP Intelligent Management Center Installation Guide."
- **Terminal IP**: Contains the IP address of the terminal.
- **Device Label**: Contains the IMC name for the device, which, by default, is the name assigned to it in its device configuration.
- **Device IP**: Contains the IP address of the device.
- **Interface**: Contains the interface of the terminal.
- **VLAN**: Contains the VLAN to which the terminal belongs.
- **Login Time**: Contains the time when the terminal logged in.
- **Logout Time**: Contains the time when the terminal logged out.

If the History Access Log List contains enough entries, the following navigational aids appear.

- Click to page forward in the History Access Log List.
- Click to page forward to the end of the History Access Log List.
- Click to page backward in the History Access Log List.
- Click to page backward to the front of the History Access Log List.

5. Click 8, 15, 50, 100, or 200 from the right side of the main pane to configure how many items per page you want to view.

6. For History Access Log lists that have more than one page, click 1, 2, 3, 4, 5, 6, 7, 8, 9, 10... from the upper middle or bottom right side of the main pane to jump to a particular page of the list.
Periodically retrieve data

To retrieve the data on the History Access Log page:
2. Click the Resource tab from the tabular navigation system on the top.
3. Click the Terminal Access section of the navigation tree on the left.
4. Click History Access Log under Terminal Access from the navigation tree on the left.
   The History Access Log List is displayed in the main portion of the History Access Log page.
5. Click the checkbox to the left of the Periodically Retrieve Data.

Real-time location

This feature lets you view the latest access information for a terminal by IP or MAC address.
2. Click the Resource tab from the tabular navigation system on the top.
3. Click the Terminal Access section of the navigation tree on the left.
4. Click History Access Log under Terminal Access from the navigation tree on the left.
   The History Access Log List displays in the main portion of the History Access Log page.
5. Click Real-Time Location link located in the far right corner of the History Access List.

Retrieve now

To immediately retrieve the History Access Log List:
2. Click the Resource tab from the tabular navigation system on the top.
3. Click the Terminal Access section of the navigation tree on the left.
4. Click History Access Log under Terminal Access from the navigation tree on the left.
   The History Access Log List displays in the main portion of the History Access Log page.
5. Click Retrieve Now link located in the far right corner of the History Access List.
6. Click the Back link to return to the History Access List, which displays the latest data.

History access log query

IMC provides you with the ability to query specified access logs.

To query history access logs:
2. Click the Resource tab from the tabular navigation system on the top.
3. Click the Terminal Access section of the navigation tree on the left.
4. Click History Access Log under Terminal Access from the navigation tree on the left.
   The History Access Log List is displayed in the main portion of the History Access Log page.
5. Move the pointer over **Query** at the upper right corner of **History Access Log List**, and a search criteria dialog box appears.

6. Enter one or more of the following search criteria in the dialog box:
   - **Terminal MAC**: Enter the MAC address in the **Terminal MAC** field.
   - **Terminal IP**: Enter the IP address in the **Terminal IP** field.
   - **Terminal Name**: Enter the terminal name in the **Terminal Name** field.
   - **Device Label**: Enter the device label in the **Device Label** field.
   - **Device IP**: Enter the IP address of the access device in the **Device IP** field.
   - **Interface**: Enter the interface that connects the terminal to the device in the **Interface** field.
   - **VLAN**: Enter the ID of the VLAN to which the terminal belongs in the **VLAN** field.
   - **Online from**: Enter a date and time to query online start time. Click the calendar icon to the right of the **Online from** to input the start time using the calendar function.
   - **Online to**: Enter a date and time to query online end time. Click the calendar icon to the right of the **Online to** input the end time using the calendar function.

7. Click **Query**.

8. Click **Reset** when you have finished your search to restore the full **History Access Log list**.

**Deleting history access logs**

To delete one or more history access logs:

1. Navigate to **Resource→History Access Log**.
2. Click the **Resource** tab from the tabular navigation system on the top.
3. Click the **Terminal Access** section of the navigation tree on the left.
4. Click **History Access Log** under **Terminal Access** from the navigation tree on the left.
5. Click the checkboxes to the left for each action status you want to delete to the associated history access log entries.
6. Click **Delete**.
7. Click **OK**.

**Refreshing the history access log page**

To refresh the **History Access Log page**

1. Navigate to **Resource→History Access Log**.
2. Click the **Resource** tab from the tabular navigation system on the top.
3. Click the **Terminal Access** section of the navigation tree on the left.
4. Click **History Access Log** under **Terminal Access** from the navigation tree on the left.
5. Click **Refresh** to reload the web page and review any updated information.
Real-time location

IMC lets you locate IP or MAC addresses in the network infrastructure. This feature is useful for pinpointing to which access device a particular user is located when some information about the user is known. IMC distinguishes end user devices or desktops from network infrastructure devices and therefore only returns search results that are end stations or desktop devices.

A Real-Time Location query initiates a poll of the network to discover in real time in which access device an IP or MAC address is connected.

Upon entering search criteria, IMC returns the IP address, MAC address, access device, Device IP address, interface, and VLAN information. This supports troubleshooting network problems and security issues.

IP address location query

To locate an IP address using a real-time location query:

1. Navigate to Resource→Real-Time Location.
2. Click the Resource tab from the tabular navigation system on the top.
3. Click Terminal Access on the navigation tree on the left.
4. Click Real-Time Location under Terminal Access from the navigation tree on the left.
   The Real-Time Location page appears.
5. Select IP Address from the Location Type field. Select MAC Address if you have the MAC address of the terminal you want to locate.
6. Enter the IP or MAC address that you want to locate.
7. Click OK.
   The results of your query display in the Real-Time Location Result list.

Real-time location result

- Location Address: Contains the IP address that has been located.
- Device IP: Contains the IP address of the access device that provides network connectivity for the IP or MAC address that has been located.
- Interface: Contains the description of the interface that the located IP/MAC address is or was connected to.
- View Access Device Topology: Contains a link for accessing the network topology. In the topology, you can check the position of the device that connects to the terminal with this address.

8. Click Reset when you have finished your search to restore the full Real-Time Location Result list.

MAC address location query

To locate an MAC address using a Real-Time Location query.

1. Navigate to Resource→Real-Time Location.
2. Click the Resource tab from the tabular navigation system on the top.
3. Click Terminal Access on the navigation tree on the left.
4. Click Real-Time Location under Terminal Access from the navigation tree on the left.
The Real-Time Location page appears.

5. Select MAC Address from the Location Type field. Select IP Address if you have the IP address of the device you want to locate.

6. Enter the IP or MAC address that you want to locate.

7. Click OK.

The results of your query display in the Real-Time Location Result list.

Real-Time location result
- Location Address: Contains the MAC address that has been located.
- Device IP: Contains the IP address of the access device that provides network connectivity for the IP or MAC address that has been located.
- Interface: Contains the description of the interface that the located IP/MAC address is or was connected to.
- View Access Device Topology: Contains a link for accessing the network topology. In the topology, you can check the position of the device that connects to the terminal with this address.

8. Click Reset when you have finished your search to restore the full Real-Time Location Result list.

Access configuration

You can bind an IP address to a MAC address for security purposes. In addition, you can bind a MAC address to an interface. When an IP address is bound to a MAC address or when a MAC address is bound to an interface, the binding takes place in IMC only. The address is not bound on the device, but rather the address is bound in IMC. Binding has the result of enabling IMC to track IP and MAC address usage to a specific resource and proactively notify you when that resource is not be used in the way it was allocated or intended.

Terminal access binding

You can define rules to restrict terminal access to the network. In IMC, you can bind all interfaces, which means a terminal can access the network from any location. In addition, you can bind one or more interfaces to allow a terminal to access the network from specified locations.

After specifying binding policies, you can configure an Unauthorized Access Processing Policy to take actions such as sending alarms or shutting down ports against terminals that violate the policy. For more information about unauthorized access processing policies, see "Unauthorized access (page 344).

Viewing the terminal access binding list

To view the Terminal Access Binding list:

2. Click the Resource tab from the tabular navigation system on the top.
3. Click Terminal Access on the navigation tree on the left.
4. Click Access Configuration under Terminal Access from the navigation tree on the left.
5. Click "Terminal Access Binding" on the Access Configuration page.

The Terminal Access Binding List appears.

Terminal Access Binding List

- **Terminal MAC**: Contains the MAC address for the terminal associated with the IP address.
- **Terminal Name**: Contains the name of the terminal.
- **Terminal IP**: Contains the IP address of the terminal that is connected to the terminal access device.
- **Trusted**: Contains information about whether or not the terminal is trusted on all interfaces.
- **Device Label**: Contains the label of the device that the terminal connects to. In addition, it provides a link for entering the Device Details page.
- **Device IP**: Contains the IP address that has been allocated to the device. The IP address serves as an active link for drilling down to the Device Details page.
- **Interface**: Contains the interface to which the associated MAC address is bound.
- **Details**: Contains a link for viewing the MAC/Interface Binding details page for the associated MAC/Interface binding entry.
- **Modify**: Contains a link for modifying the Terminal Access Binding entry.

If the Terminal Access Binding List contains enough entries, the following navigational aids are displayed.

- Click to page forward in the Terminal Access Binding List.
- Click to page forward to the end of the Terminal Access Binding List.
- Click to page backward in the Terminal Access Binding List.
- Click to page backward to the front of the Terminal Access Binding List.

6. Click 8, 15, 50, 100, or 200 from the right side of the main pane to configure how many items per page you want to view.

7. For lists that have more than one page, click 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 … from the upper middle or bottom right side of the main pane to jump to a particular page of the list.

You can sort the Terminal Access Binding List by most fields. Click the column label to sort the list by the selected field. The column label is a toggle switch that lets you toggle between the various sort options specific to each field.

**Searching for terminal access bindings**

To search IMC for an existing terminal access binding:

2. Click the Resource tab from the tabular navigation system on the top.
3. Click Terminal Access on the navigation tree on the left.
4. Click Access Configuration under Terminal Access from the navigation tree on the left.
5. Click "Terminal Access Binding" on the Access Configuration page.

The Terminal Access Binding List is displayed in the Terminal Access Binding page.
6. Move the pointer over **Query** at the upper right corner of **Terminal Access Binding List**, and a search criteria dialog box appears.

7. Enter one or more of the following search criteria:
   - **Terminal MAC**: Enter the MAC address for the terminal associated in the **Terminal MAC** field.
   - **Terminal IP**: Enter the IP address that you want to locate a binding for in the **Terminal IP** field.
   - **Terminal Name**: Enter the name for the terminal you want to locate a binding in the **Terminal Name** field.
   - **Trusted**: Select whether to trust the terminal from the **Trusted** list.
   - **Device Label**: Enter the device label you want to search for.
   - **Device IP**: Enter the IP address of the access device in the **Device IP** field.
   - **Interface**: Enter the interface to which the associated MAC address is bound.

8. Click **Query**.

9. Click **Reset** when you finish your search to restore the full **Terminal Access Binding** list.

**Manually binding a terminal to interfaces**

To bind a terminal to one or more interfaces in IMC:

1. Navigate to **Resource**→**Terminal Access Binding**.
2. Click the **Resource** tab from the tabular navigation system on the top.
3. Click **Terminal Access** on the navigation tree on the left.
4. Click **Access Configuration** under **Terminal Access** from the navigation tree on the left.
5. Click **Terminal Access Binding** on the **Access Configuration** page. The **Terminal Access Binding List** appears.
6. Click **Add Binding**.
7. Enter the MAC address for the binding you want to create in the **Terminal MAC** field. Valid MAC address format includes ##:##:##:##:##:##.
   
   For example, 00:24:82:1e:3b:81 is a valid entry.

8. Enter the Terminal Name in the **Terminal Name** Field.
9. Enter the maintainer in the **Maintainer** field.
10. Select whether to bind all interfaces in the **Trusted** list.
11. Enter the device label in the **Device Label** field.
12. Enter the device IP in the **Device IP** field.
13. Click **Select** located to the right of the **Interface** field.
14. Add interfaces using either the **View** or **Advanced** query option.

Adding interfaces uses the same process as adding devices. See "Adding devices by View" (page 85) and "Adding devices by Advanced query" (page 85).

**Manually unbinding a terminal from one or more interfaces**

To manually unbind a Terminal from one or more interfaces:
2. Click the Resource tab from the tabular navigation system on the top.
3. Click Terminal Access on the navigation tree on the left.
4. Click Access Configuration under Terminal Access from the navigation tree on the left.
5. Click Terminal Access Binding on the Access Configuration page.
   The Terminal Access Binding List is displayed in the Terminal Access Binding page.
6. Click the checkboxes to the left of the terminal access binding entries you want to unbind.
7. Click Unbind.
8. Click OK to confirm the unbinding request.

**Binding multiple terminal to interfaces using the Auto Scanning feature**

You can use the auto scanning feature to also bind a terminal to the current interface associated with them. You can easily and proactively secure network resources using this feature.

To add Terminal Access binding in IMC (not on the device) using IMC’s auto scanning feature:
2. Click the Resource tab from the tabular navigation system on the top.
3. Click Terminal Access on the navigation tree on the left.
4. Click Access Configuration under Terminal Access from the navigation tree on the left.
5. Click Terminal Access Binding on the Access Configuration page.
   The Terminal Access Binding List is displayed in the Terminal Access Binding page.
6. Click the Auto Scanning link located in the far right corner of the Terminal Access Binding List.
7. Click Add Device to add devices to the Device List.
8. Add devices using the By View and by Advanced query option.
   See "Adding devices by View" (page 85) and "Adding devices by Advanced query" (page 85).

**Refreshing the terminal access binding list**

To refresh Terminal Access Binding List:
2. Click the Resource tab from the tabular navigation system on the top.
3. Click Terminal Access on the navigation tree on the left.
4. Click Access Configuration under Terminal Access from the navigation tree on the left.
5. Click Terminal Access Binding on the Access Configuration page.
   The Terminal Access Binding List displays in the Terminal Access Binding page.
6. Click Refresh to reload the web page and review any updated information.
Switch access binding

Using the Switch Access Binding feature, you can bind an interface on the switch to the MAC address of one or more terminals to control terminal access to the network.

Viewing the switch access binding list

To view the Switch Access Binding List:
2. Click the Resource tab from the tabular navigation system on the top.
3. Click Terminal Access on the navigation tree on the left.
4. Click Access Configuration under Terminal Access from the navigation tree on the left.
5. Click Switch Access Binding on the Access Configuration page.

The Switch Access Binding List appears.

Switch access binding list

- **Interface Description**: Contains the interface to which the associated MAC address is bound. The interface description serves as an active link for drilling down to the Interface Details page.
- **Device Label**: Contains the device label of the access device. The device label serves as an active link for drilling down to the Device Details page.
- **Device IP**: Contains the IP address of access device. The IP address serves as an active link for drilling down to the Device Details page.
- **Trusted**: Contains information about whether or not the terminal is trusted on all interfaces.
- **Terminal MAC**: Contains the MAC address for the terminal associated with the interface.
- **Terminal IP**: Contains the IP address of the terminal that is connected to the terminal access device.
- **Terminal Name**: Contains the name of the terminal.
- **Details**: Contains a link to viewing the Switch Access Binding Details page for the associated switch access binding entry.
- **Modify**: Contains a link for modifying the switch access binding entry.

If the Switch Access Binding List contains enough entries, the following navigational aids appear.

- Click to page forward in the Switch Access Binding List.
- Click to page forward to the end of the Switch Access Binding List.
- Click to page backward in the Switch Access Binding List.
- Click to page backward to the front of the Switch Access Binding List.

6. Click 8, 15, 50, 100, or 200 from the right side of the main pane to configure how many items per page you want to view.

7. For lists that have more than one page, click on 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 … from the upper middle or bottom right side of the main pane to jump to a particular page of the list.
You can sort the **Switch Access Binding List** by most fields. Click the column label to sort the list by the selected field. The column label is a toggle switch that lets you toggle between the various sort options specific to each field.

**Searching for switch access bindings**

To search IMC for an existing terminal access binding:
2. Click the Resource tab from the tabular navigation system on the top.
3. Click Terminal Access on the navigation tree on the left.
4. Click Access Configuration under Switch Access from the navigation tree on the left.
5. Click ![Switch Access Binding](image) on the Access Configuration page.
   The **Switch Access Binding List** appears.
6. Move the pointer over Query at the upper right corner of **Switch Access Binding List**.
   The search criteria dialog box appears.
7. Enter one or more of the following search criteria:
   - **Interface Description**: Enter the interface description to which the associated MAC address is bound.
   - **Device Label**: Enter the label of the device where the interface resides.
   - **Device IP**: Enter the IP address of the device where the interface resides.
   - **Trusted**: Select whether to trust the terminal from the Trusted list.
   - **Terminal MAC**: Enter the MAC address for the terminal associated in the **Terminal MAC** field.
   - **Terminal IP**: Enter the IP address that you want to locate a binding for in the **Terminal IP** field.
   - **Terminal Name**: Enter the name for the terminal you want to locate a binding in the **Terminal Name** field.
8. Click Query.
9. Click Reset when you finish your search to restore the full **Switch Access Binding** list.

**Manually binding interfaces to one or more terminals**

You can bind interfaces to one or more terminals. In addition, you can define trusted interfaces. The trusted interfaces allow any terminals to access the network through them.

To bind an interface to one or more terminals in IMC:
2. Click the Resource tab from the tabular navigation system on the top.
3. Click Terminal Access on the navigation tree on the left.
4. Click Access Configuration under Terminal Access from the navigation tree on the left.
5. Click ![Switch Access Binding](image) on the Access Configuration page.
   The **Switch Access Binding List** appears.
6. Click **Add Binding**.
7. Click **Select** to select the interface to be bound.
8. Add devices by using either the **View** or **Advanced** query option.
    See "Adding devices by View" (page 85) and "Adding devices by Advanced query" (page 85).

**Manually unbinding one or more terminals from interfaces**

To manually unbind one or more Terminals from an interface:
1. Navigate to **Resource** → **Switch Access Binding**.
2. Click the **Resource** tab from the tabular navigation system on the top.
3. Click **Terminal Access** on the navigation tree on the left.
4. Click **Access Configuration** under **Terminal Access** from the navigation tree on the left.
5. Click **Switch Access Binding** in the **Access Configuration** page.
    The **Switch Access Binding List** appears.
6. Click the checkboxes to the left of the terminal access binding entries you want to unbind.
7. Click **Unbind**.
8. Click **OK** to confirm the unbinding request.

**Switch access binding by using the auto-scanning feature**

You can use the auto scanning feature to also bind interfaces to the current terminal associated with them. You can easily and proactively secure network resources using this feature.

To add Switch Access binding in IMC (not on the device) using IMC’s auto scanning feature:
1. Navigate to **Resource** → **Switch Access Binding**.
2. Click the **Resource** tab from the tabular navigation system on the top.
3. Click **Terminal Access** on the navigation tree on the left.
4. Click **Access Configuration** under **Terminal Access** from the navigation tree on the left.
5. Click **Switch Access Binding** in the **Access Configuration** page.
    The **Switch Access Binding List** appears.
6. Click the **Auto Scanning** link located in the far right corner of the Switch Access Binding List.
7. Click **Add Device** to add devices to the **Device List**.
8. You can add devices using the **By View** and by **Advanced** query option.
    See "Adding devices by View" (page 85) and "Adding devices by Advanced query" (page 85).

**Refresh switch access binding list**

To refresh **Switch Access Binding List**:
1. Navigate to **Resource** → **Access Configuration** → **Switch Access Binding**.
2. Click the **Resource** tab from the tabular navigation system on the top.
3. Click **Terminal Access** on the navigation tree on the left.

4. Click **Access Configuration** under **Terminal Access** from the navigation tree on the left.

5. Click **Switch Access Binding** on the **Access Configuration** page.
   The **Switch Access Binding List** appears.

6. Click **Refresh** to reload the web page and review any updated information.

### IP to MAC address binding

Using the IP/MAC Address Binding feature, you can bind an IP address to a MAC address within IMC (not on the device). When IMC detects an invalid IP address and MAC address pairing, it generates an alarm notifying you of this event. The benefits of this feature are as follows: 1) IP addresses cannot be changed without notification of changes; 2) Supports the centralized management of IP address resources; and 3) Helps defend against security threats.

You can bind IP addresses to MAC addresses manually or they can use the auto-scanning feature. With the auto-scanning feature, IMC identifies IP address and MAC address combination pairs, which you then can selectively apply binding to. IMC version 5.1 supports 5,000 IP address to MAC address bindings. The following section provides details on IP to MAC address binding.

#### Viewing the IP/MAC binding list

To view the IP/MAC binding list:

1. Navigate to **Resource**→**Access Configuration**→**IP/MAC Binding**.
2. Click the **Resource** tab from the tabular navigation system on the top.
3. Click **Terminal Access** on the navigation tree on the left.
4. Click **Access Configuration** under **Terminal Access** from the navigation tree on the left.
5. Click **IP/MAC Binding** in the **Access Configuration** page.
   The **IP/MAC Binding List** is displayed in the **IP/MAC Binding** page.

**IP/MAC Binding List**

- **IP Address**: Contains the IP address that has been allocated.
- **MAC Address**: Contains the MAC address for the device associated with the IP address.
- **Owner**: Contains the name of the IP address owner.
- **Details**: Contains a link to viewing the IP/MAC Binding details page for the associated IP/MAC binding entry.
- **Unbind**: Contains a link for unbinding the IP address allocation from the MAC address.

If the **IP/MAC Binding List** contains enough entries, the following navigational aids are displayed.

- Click ▶️ to page forward in the **IP/MAC Binding List**.
- Click ▶️ to page forward to the end of the **IP/MAC Binding List**.
- Click ▼️ to page backward in the **IP/MAC Binding List**.
- Click ▶️ to page backward to the front of the **IP/MAC Binding List**.
6. Click 8, 15, 50, 100, or 200 from the right side of the main pane to configure how many items per page you want to view.

7. For lists that have more than one page, click 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 … from the upper middle or bottom right side of the main pane to jump to a particular page of the list.

You can sort the **IP/MAC Binding List** by most fields. Click the column label to sort the list by the selected field. The column label is a toggle switch that lets you toggle between the various sort options specific to each field.

**Searching for IP/MAC bindings**

IMC provides you with the ability to search for existing IP address to MAC address bindings.

To search IMC for an existing IP/MAC binding:

2. Click the Resource tab from the tabular navigation system on the top.
3. Click Terminal Access on the navigation tree on the left.
4. Click Access Configuration under Terminal Access from the navigation tree on the left.
5. Click ![IP/MAC Binding] on the Access Configuration page.
   
   The **IP/MAC Binding List** is displayed in the **IP/MAC Binding** page.
6. Move the pointer over Query at the upper right corner of IP/MAC Binding List, and a search criteria dialog box appears.
7. Enter one or more of the following search criteria in the dialog box:
   - **IP Address**: Enter the IP address that you want to locate a binding for in the IP Address field.
   - **MAC Address**: Enter the MAC address for the device associated in the MAC Address field.
   - **Owner**: Enter the owner of the IP address.
8. Click Query.
9. Click Reset when you have finished your search to restore the full IP/MAC Binding list.

**Manually binding an IP address to a MAC address**

To bind an IP address to a MAC address in IMC:

2. Click the Resource tab from the tabular navigation system on the top.
3. Click Terminal Access on the navigation tree on the left.
4. Click Access Configuration under Terminal Access from the navigation tree on the left.
5. Click ![IP/MAC Binding] on the Access Configuration page.
   
   The **IP/MAC Binding List** is displayed in the **IP/MAC Binding** page.
6. Click Add.
7. To select the IP address to bind, click Select located to the right of the IP address field. In the Select an IP Address dialog box, enter one or more of the following search criteria in the fields provided:
- **IP Address**: Enter a partial or complete IP address for the IP address you want to bind in the **IP Address** field.
- **Owner**: Enter the owner for the IP address in the **Owner** field.

8. Click **Query** to begin your search.

9. Click on the radio button ◐ to the left of the search result entry that you want to bind.

10. Click **OK** to accept your selection and return to the **IP/MAC binding** page.

Only an IP address that has been allocated using the IP Address Allocation feature can be bound to a MAC address. If the IP address you want to bind is not displayed in the query results, check the IP Address Allocation list to verify that the IP address you want to bind has already been allocated. For more information on allocating IP addresses, see “Allocating IP addresses” (page 318).

11. Enter the MAC address for the binding you want to create in the **MAC Address** field. A valid MAC address format is ##:##:##:##:##:##.
   
   For example, 00:24:82:1e:3b:81 is a valid entry.

   Using the IP/MAC auto scanning feature discovers IP addresses and the current MAC addresses associated with them. IMC auto populates the **IP Address**, **MAC Address**, **Device Name and Device Type** fields when the information is available, thus ensuring consistency in naming conventions across management modules in IMC. HP recommends using the auto scanning feature whenever possible.

12. Enter the owner of the binding in the **Owner** field.

13. Click **OK**.

**Manually unbinding an IP address from a MAC address**

To manually unbind an IP address from a MAC address in IMC:

1. Navigate to **Resource → Access Configuration → IP/MAC Binding**.
2. Click the **Resource** tab from the tabular navigation system on the top.
3. Click **Terminal Access** on the navigation tree on the left.
4. Click **Access Configuration** under **Terminal Access** from the navigation tree on the left.
5. Click **IP/MAC Binding** in the **Access Configuration** page.
   The **IP/MAC Binding List** is displayed in the **IP/MAC Binding** page.
6. Click **Unbind** ❌ associated with the IP/MAC address binding you want to unbind.
7. Click **OK** to confirm the unbinding request.

**Binding multiple IP/MAC addresses using the auto scanning feature**

You can use the auto scanning feature to also bind IP addresses to the current MAC addresses associated with them.

To add IP/MAC binding in IMC (not on the device) using auto scanning:

1. Navigate to **Resource → Access Configuration → IP/MAC Binding**.
2. Click the **Resource** tab from the tabular navigation system on the top.
3. Click **Terminal Access** on the navigation tree on the left.
4. Click **Access Configuration** under **Terminal Access** from the navigation tree on the left.

5. Click **IP/MAC Binding** in the **Access Configuration** page.  
The **IP/MAC Binding List** is displayed in the **IP/MAC Binding** page.

6. Click the **Auto Scanning** link located in the far right corner of the **IP/MAC Binding List**.

7. Enter the first usable IP address in the range of IP addresses you want to identify in the **Start IP Address** field.

8. Enter the last usable IP address in the range of IP addresses you want to identify in the **End IP Address** field.

9. Click **Add** to add the IP Segment to the **Configured Segments** list.

10. Repeat **Steps 3-9** until you have added all of the IP segments you want to scan the network for.

11. Click **OK**, IMC scans the network and return all IP addresses and the MAC addresses associated with them.

12. Click the checkbox to the left for each IP address you want to bind.  
Clicking the first empty checkbox in the upper corner of the list selects all entries in the list for the current page.

13. Click **Bind** to bind the IP addresses to their associated MAC addresses.

14. Review the results of your allocation in the **Binding Result List**.

**Unbinding multiple IP/MAC address bindings**

You can unbind multiple IP addresses from the MAC addresses.

To unbind multiple IP/MAC address bindings in IMC:

1. Navigate to **Resource**→**Access Configuration**→**IP/MAC Binding**.

2. Click the **Resource** tab from the tabular navigation system on the top.

3. Click **Terminal Access** on the navigation tree on the left.

4. Click **Access Configuration** under **Terminal Access** from the navigation tree on the left.

5. Click **IP/MAC Binding** in the **Access Configuration** page.  
The **IP/MAC Binding List** appears.

6. Click the checkboxes to the left for each IP/MAC binding you want to unbind.  
Clicking the first empty checkbox in the upper left corner of the list selects all IP addresses in the list for the current page.

7. Click **Unbind**.

8. Click **OK** to confirm the unbinding of the selected IP addresses.

9. Review the results of your allocation in the **Unbinding Result List** page.

**Refresh IP/MAC binding list**

To refresh **IP/MAC Binding List**:

1. Navigate to **Resource**→**Access Configuration**→**IP/MAC Binding**.

2. Click the **Resource** tab from the tabular navigation system on the top.
3. Click **Terminal Access** on the navigation tree on the left.
4. Click **Access Configuration** under **Terminal Access** from the navigation tree on the left.
5. Click **IP/MAC Binding** in the **Access Configuration** page.
The IP/MAC Binding List is displayed in the IP/MAC Binding page.
6. Click **Refresh** to reload the web page and review any updated information.

### Unauthorized access processing policy

After completing Terminal Access Binding, Switch Access Binding, and IP/MAC Binding, you can use an Unauthorized Access Processing Policy to configure rules for taking actions against terminals that violate the rules. For example, sending alarms or shutting down ports can help the administrator control unauthorized terminal access.

To configure an **Unauthorized Access Processing Policy**:
1. Navigate to **Resource** → **Unauthorized Access Processing Policy**.
2. Click the **Resource** tab from the tabular navigation system on the top.
3. Click **Terminal Access** on the navigation tree on the left.
4. Click **Access Configuration** under **Terminal Access** from the navigation tree on the left.
5. Click **Unauthorized Access Processing Policy** in the **Access Configuration** page.
The Unauthorized Access Processing Policy page appears.

### Configure conflict processing policy

1. Select Yes or No in the **Send Alarm** list.
2. Select an interface shutdown policy in the **Interface Shutdown** list. If you select Do not shut down, you go to the next section.
3. Configure the duration before the interface is shut down in the **Shut Down the Interface in** (5-1800 seconds) field, if prompted.
4. Select the operation to be performed after the interface is shut down in the **After the Interface is Down for a Period** list, if prompted.
5. Configure the duration before the interface is brought up in the **Bring up the Interface in** (5-1800 seconds) field, if prompted.

### Configure an undefined access processing policy

1. Select Illegal in the **Undefined Access** list. If you select Legal, you go to the next section.
2. Select Yes or No, in the **Send Alarm** list.
3. Select an interface shutdown policy in the **Interface Shutdown** list.
4. Configure the duration before the interface is shut down in the **Shut Down the Interface in** (5-1800 seconds) field, if prompted.
5. Select the operation to be performed after the interface is shut down in the **After the Interface is Down for a Period** list, if prompted.
6. Configure the duration before the interface is brought up in the **Bring up the Interface in** (5-1800 seconds) field, if prompted.
7. Adopt the default IP/MAC Mismatch Processing Policy, which is **Send Alarm**.
8. Click **OK**.

**Network Asset Manager**

The **Network Asset Manager** lets you track and modify assets and make changes to these assets. Using this feature, you can view asset lists and drill down into individual device details or device audit details, query IMC for specific audit records and manage the auditing process.

The asset OID feature lets you manage the device OID information and identify the asset type by its OID, and facilitates the device management and statistics. At the same time, the physical asset attributes of the asset OID feature let you identify the physical assets and non-physical assets.

**Viewing network assets**

You can view device specific details including component level details. From the **Network Asset List**, you can view asset details that include device specific and module specific information. From this view you can also access the **Device Details** page for the selected device and audit histories.

**Network asset list**

To view the Network Asset List:

1. Navigate to **Resource→Network Assets**.
2. Click the **Resource** tab from the tabular navigation system on the top.
3. Click the **Network Assets** section of the navigation tree on the left.
4. Click **Network Assets** under **Network Assets** from the navigation tree on the left. The **Network Asset List** is displayed in the main portion of the **Network Assets** page.

**Network asset list**

- **Asset Name**: Contains the asset name. The contents of this field serve as an active link for navigating to the **Network Asset Details** page. At the device level, the asset name is derived from the device label in IMC. Device labels are derived from sysName if it is configured and if the operator has not manually configured it. Asset names for component level assets are defined in the MIB for the device.
- **Asset Description**: Contains a description for the asset. If the asset is a device, this field contains the device label. If it is a component, it contains the system description or sysDescr provided by the vendor if this information is available.
- **Class**: Contains the asset classification for the asset type. Asset classes are defined by values defined in the Entity MIB.
- **Device Label**: Contains the IMC name for the device, which, by default, is the name assigned to it in its device configuration. This field also contains the IP address. The device label serves as an active link for drilling down into the **Device Details** page, which offers you convenient access to device management features.
- **Device Type**: Contains IMC’s categorization of the device. If the asset is a component, it inherits the device type from the parent device.
Service Time: Contains the date and time stamp marking the start date of the asset’s time in service.

Physical Asset: Contains the physical attributes of the asset. Yes indicates that the asset is a physical asset, and No indicates that the asset is a non-physical asset.

Modify: Contains a link for modifying the network asset entry.

If the Network Asset List contains enough entries, the following navigational aids are displayed.

Click ▶ to page forward in the Network Asset List.

Click ▶ to page forward to the end of the Network Asset List.

Click ▶ to page backward in the Network Asset List.

Click ▶ to page backward to the front of the Network Asset List.

5. **Click 8, 15, 50, 100, or 200** from the right side of the main pane to configure how many items per page you want to view.

6. For Network Asset lists that have more than one page, click 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 … from the upper middle or bottom right side of the main pane to jump to a particular page of the list.

You can sort the Network Asset List by the Asset Name, Asset Description, Class, Device Label, Service Time, and Physical Asset fields. Click the column label to sort the list by the selected field. The column label is a toggle switch that lets you toggle between the various sort options specific to each field.

You can view asset information only for the devices to which they have been granted management access.

### Viewing device level network asset details

Device level asset information includes device specific asset details on the manufacturer, build, software, and hardware versions, IMC information on the specific device and operator remarks. It also includes sub module information, access to the interface list and an audit history for the individual device.

Device level network asset information is displayed in the Network Asset Details page. This page has several sections: The Basic Information section, a Sub Module List of components, and an Audit History and a quick link to the Interfaces List for the selected device.

### Accessing the network assets page

To access network asset details:

2. Click the Resource tab from the tabular navigation system on the top.
3. Click the Network Assets section of the navigation tree on the left.
4. Click Network Assets under Network Assets from the navigation tree on the left. The Network Asset List is displayed in the main portion of the Network Assets page.
5. Click the link in the Asset Name field for the device you want to view asset details for. The Network Asset Details page is displayed for the selected.
Viewing network asset details

The Network Asset Details page contains network assets, Device Information, and Net Asset Information. Network asset information includes all asset information such as device chassis and modules.

Click **Hide Non Physical Asset** to display only physical assets and hide all non-physical assets. Click **Show Non Physical Asset** to display all assets. Device Information contains two links, **Device Label** and **Interface List** for entering the **Device Details** page and **Interface List** page. Net asset information for network devices includes IMC specific device information and information gathered from the asset by IMC.

Information about the device and its components that is gathered from it includes Asset Name, Asset Class, Asset Description, Manufacturer, Model, Serial Number, FRU, Asset Number, Alias, Manufacture Date, Building Version, Hardware Version, Firmware Version, Software Version, Card Serial Number, BOM Code, CLEI Code, and Remarks. IMC displays this information if it can be polled from the asset.

Some of the fields in the **Network Asset Details** page include:

- **Device Label**: Contains the IMC name for the device, which by default is the name assigned to it in its device configuration. This field also contains the IP address. The device label serves as an active link for drilling down into the **Device Details** page, which offers you convenient access to device management features.

- **Asset Name**: Contains the asset name. At the device level, the asset name is derived from the device label in IMC. IMC populates the device label value with the sysName if it has been configured on the device and if the operator has not manually changed the device label in IMC.

- **Asset Class**: Contains the asset classification for the asset type.

- **Asset Description**: Contains a description for the asset. If the asset is a device, this field contains the device label. If it is a component, it contains the system description or sysDescr provided by the vendor if this information is available.

- **Service Time**: Contains the date and time stamp marking the start date of the asset’s time in service.

- **Last Poll Time**: Contains the date and time stamp for the asset audit that captured the current information.

You can view asset information only for the devices to which they have been granted management access.

Viewing audit history

The **Audit History** section of the **Network Asset Details** page provides you with a list of all asset audits performed on the selected device.

1. To access the **Audit History** list, click the **Audit History** link in the upper right corner of the **Network Asset Details** page.

Asset audit list

- **Audit Time**: Contains a date and time stamp for the entry in the **Audit History** list.

- **Device Label**: Contains the IMC name for the devices, which by default, is the name assigned to it in its device configuration. This field also contains the IP address. The device
label serves as an active link for drilling down into the Device Details page, which offers you convenient access to device management features.

- **Asset Class**: Contains the asset classification for the device.
- **Asset Name**: Contains the asset name. At the device level, the asset name is derived from the device label in IMC. IMC populates the device label value with the sysName if it has been configured on the device and if the operator has not manually changed the device label in IMC.
- **Audit Options**: Contains type of audit action performed. Possible audit actions include: add asset, modify firmware version, modify alias, delete asset, modify software version, modify asset ID, modify asset name, modify serial number, modify build information, modify hardware version, and modify model name.
- **Before Change**: Contains a description of the asset prior to the change.
- **After Change**: Contains a description of the asset after the change.

If the Audit History list contains enough entries, the following navigational aids are displayed.

- Click ⏏ to page forward in the Audit History List.
- Click ⏎ to page forward to the end of the Audit History List.
- Click ⏋ to page backward in the Audit History List.
- Click ⏐ to page backward to the front of the Audit History List.

2. Click 8, 15, 50, 100, or 200 from the right side of the main pane to configure how many items per page you want to view.

3. For Audit History lists that have more than one page, click on 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 … from the bottom right side of the main pane to jump to a particular page of the list.

**Viewing interface list**

The Interface section of the Network Asset Details page provides you with a list of interfaces on the selected device.

To access the Interface List, click the Interface List link below the Device Information section of the Network Asset Details page.

**Network asset query**

You can query the Network Asset List for audit records for specific devices. You have two options for querying: a basic query and an advanced query. The following sections provide information on each of these query methods.

**Basic query**

To perform a basic query:

2. Click the Resource tab from the tabular navigation system on the top.
3. Click Network Assets section of the navigation tree on the left.
4. Click Network Assets under Network Assets from the navigation tree on the left. The Network Asset List is displayed in the main portion of the Network Assets page.
The Network Asset Query section of the Network Assets page is located at the top of the main pane.

The Basic Query section is displayed (by default) above the Network Asset list. The link to the far right is a toggle between Basic Query and Advanced Query. If the link is Advanced Query, then you are in the Basic Query mode.

5. Enter one or more search criteria in the fields provided.
   - **Asset Name**: Enter the name of the asset in the Asset Name field.
   - **Device Label**: Enter the IMC name for the device in the Device Label field.
   - **Device IP**: Enter the IP address of the device you want to locate audit records for in the Device IP field. You can use the asterisk (*) as a wildcard for one or more digits in the IP address.
   - **Class**: Select the asset class from the Class list.

6. Click Query. The results of the query are displayed in the Network Asset List portion of the page.

**Advanced Query**

To perform an advanced query:

2. Click the Resource tab from the tabular navigation system on the top.
3. Click the Network Assets section of the navigation tree on the left.
4. Click Network Assets under Network Assets from the navigation tree on the left. The Network Asset List is displayed in the main portion of the Network Assets page.

The Network Asset Query section of the Network Assets page is located at the top of the main pane.

5. The Basic Query section is displayed (by default) above the Network Asset list. The link to the far right is a toggle between Basic Query and Advanced Query. If the link is Advanced Query, then you are in the Basic Query mode. Click Advanced Query to navigate to the Advanced Query page.

6. Enter one or more search criteria in the fields provided.
   - **Asset Name**: Enter the name of the asset in the Asset Name field.
   - **Asset Description**: Enter a portion of or the entire description in the Asset Description field.
   - **Class**: Select the asset class from the Class list.
   - **Serial Number**: Enter the serial number of the asset in the Serial Number field.
   - **Service Start Time**: Enter a date and time when the asset you want to find was entered into service or entered into the Network Asset Manager. Click on the calendar icon to the right of the Service Start Time to input the start time using the calendar function.
   - **Service End Time**: Enter a date and time the asset you want to find was removed from service or removed from the Network Asset Manager. Click the calendar icon to the right of the Service End Time to input the end time using the calendar function.
   - **FRU**: Specify whether the asset is hot swappable.
- Physical Asset: Select the asset's physical attributes from the Physical Asset list.
- Asset OID: Enter the OID of the asset that you want to query.
- Device Label: Enter the IMC name or device label in the Device Label field.
- Device IP: Enter the IP address of the device you want to locate audit records for in the Device IP field. You can use the asterisk (*) as a wildcard for one or more digits in the IP address.
- Device Type: Select IMC’s categorization of the asset type you want to locate from the Device Type list.
- Device Status: Select the status from the Device Status list for the assets you want to locate.

7. Click Query. The results of the query are displayed in the Network Asset List portion of the page.
8. Click Reset when you have finished and restored the Network Asset List to a complete display of all assets.

Asset OID

In the network asset manager, the assets fall into physical assets and non-physical assets. The IMC uses the OIDs to identify the asset types. You can add, modify, delete, and query the asset OIDs. Among the IMC reports, the device asset-related reports display only physical assets (by default).

Asset OID list

To view the asset OID list:
1. Navigate to Resource→Asset OID.
2. Click the Resource tab from the tabular navigation system on the top.
3. Click the Network Assets section of the navigation tree on the left.
4. Click Asset OID under Network Assets from the navigation tree on the left. The Asset OID List page is displayed in the main portion of the Asset OID page.

Asset OID list

- OID: Contains the OID.
- Name: Contains the name of the OID and specifies the asset type of the OID, for example, switch or port.
- Type: Contains the OID generation type, which can be Predefined or User-defined.
- Physical Asset: Contains the asset property. Yes indicates that the asset is a physical asset, and No indicates that the asset is a non-physical asset.
- Description: Contains some description about the OID.
- Modify: Contains a link for modifying the asset OID entry. You can modify only the user-defined OIDs.
- Delete: Contains a link to delete the asset OID from the IMC. You can delete only the user-defined OIDs.

If the Asset OID List contains enough entries, the following navigational aids are displayed.
- Click to page forward in the Network Asset List.
5. Click 8, 15, 50, 100, or 200 from the right side of the main pane to configure how many items per page you want to view.

6. For Network Asset lists that have more than one page, click 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 … from the upper middle or bottom right side of the main pane to jump to a particular page of the list. You can sort the Asset OID List by the OID, Name, Type, Physical Asset, and Description. Click the column label to sort the list by the selected field. The column label is a toggle switch lets you toggle between the various sort options specific to each field.

Asset OID query

You can query the OIDs by setting the query conditions. The following section describes how to query OIDs.

To query an asset OID:
1. Navigate to Resource→Asset OID.
2. Click the Resource tab from the tabular navigation system on the top.
3. Click Network Assets section of the navigation tree on the left.

4. Click Asset OID under Network Assets from the navigation tree on the left. The Asset OID List page is displayed in the main portion of the Asset OID page.

The Query Asset OID section of the Network Assets page is located at the top of the main pane.

5. Enter one or more search criteria in the fields provided.
   - **OID**: Enter the partial or complete OID.
   - **Name**: Enter the partial or complete name of the OID.
   - **Type**: Select the OID generation type, which can be Predefined or User-defined.
   - **Physical Asset**: Select the asset property. Select Yes to query physical assets, and select No to query non-physical assets.

6. Click Query. The results of the query are displayed in the Network Asset List portion of the page.

7. Click Reset when you have finished and restored the Network Asset List to a complete display of all assets.

Adding an asset OID

To manually add an asset OID to the IMC:
1. Navigate to Resource→Asset OID.
2. Click the Resource tab from the tabular navigation system on the top.
3. Click Network Assets section of the navigation tree on the left.

4. Click Asset OID under Network Assets from the navigation tree on the left. The Asset OID List page is displayed in the main portion of the Asset OID page.
5. Click Add.
The Add Asset OID page appears.

6. Enter the following information.
   - **OID**: Enter the OID, which is defined by the vendor. The OID must start and end with a digit and contain no wildcard, for example, 1.3.6.1.4.1.2011.10.3.1.
   - **Name**: Enter the name of the OID. This field specifies the asset type of the OID, for example, switch or port.
   - **Physical Asset**: Select the asset property. Select **Yes** if the OID is a physical asset, and select **No** when the OID is a non-physical asset.
   - **Description**: Enter any description of the OID.

7. Click **OK**.

8. Confirm that the OID you added appears in the **Asset OID List**.

**Modify an asset OID**

To modify an asset OID to the IMC:

1. Navigate to **Resource**→**Asset OID**.
2. Click the **Resource** tab from the tabular navigation system on the top.
3. Click **Network Assets** section of the navigation tree on the left.
4. Click **Asset OID** under **Network Assets** from the navigation tree on the left. The **Asset OID List** is displayed in the main portion of the **Asset OID** page.
5. Click the **Modify** link located in the upper right corner of the **Asset OID List** page.
   
   The **Modify Asset OID** page appears.
6. You can modify **Name**, **Physical Asset**, and **Description**. You can modify any of the following options as needed.
   - **Name**: Enter the new name in the **Name** field.
   - **Physical Asset**: Select the asset property. Select **Yes** if the OID is a physical asset, and select **No** if the asset is a non-physical asset.
   - **Description**: Enter any description of the OID.
7. Click **OK**.

**Delete an asset OID**

To delete an asset OID from the IMC:

1. Navigate to **Resource**→**Asset OID**.
2. Click the **Resource** tab from the tabular navigation system on the top.
3. Click **Network Assets** section of the navigation tree on the left.
4. Click **Asset OID** under **Network Assets** from the navigation tree on the left. The **Asset OID List** is displayed in the main portion of the **Asset OID** page.
5. Click the **Delete** link located in the upper right corner of the **Asset OID** page.
6. Click **OK**. Confirm that the OID is deleted from the IMC.
Managing asset information in Network Asset Manager

You can manually add, modify, remove, audit assets, and modify property.

Manually adding a network asset

To manually add a network device to the Network Asset Manager:

2. Click the Resource tab from the tabular navigation system on the top.
3. Click Network Assets section of the navigation tree on the left.
4. Click Network Assets under Network Assets from the navigation tree on the left. The Network Asset List is displayed in the main portion of the Network Assets page.
5. Click Add.
The Add Devices to the Network Asset Manager page appears.
6. Click Add.
You can add devices by using either the View or Advanced query option. See "Adding devices by View" (page 85) and "Adding devices by Advanced query" (page 85).

Modifying a network asset

To modify a network asset:

2. Click the Resource tab from the tabular navigation system on the top.
3. Click Network Assets section of the navigation tree on the left.
4. Click Network Assets under Network Assets from the navigation tree on the left. The Network Asset List is displayed in the main portion of the Network Assets page.
5. Click the link in the Asset Name field for the device you want to modify. The Network Asset Details page is displayed for the selected device.
6. Click the Modify link located in the upper right corner of the Network Asset Details page.
7. Do one of the following:
   - Modify the service time by entering a new service time in the Service Time field. A valid service time entry is YYYY-MM-DD HH:MM:SS.
   - Click the calendar function located to the right of the Service Time field to select the date and time.
8. Enter any comments in the Remarks field.
9. Click OK to accept your changes.

Modify property

To modify a network asset property:

2. Click the Resource tab from the tabular navigation system on the top.
3. Click Network Assets section of the navigation tree on the left.
4. Click Network Assets under Network Assets from the navigation tree on the left. The Network Asset List is displayed in the main portion of the Network Assets page.

5. Click the checkbox to the left of the asset name to select asset you want to modify.

6. Click Modify Property.

   The Modify Property page appears.

7. The Network Asset List contains information of selected assets.
   - **Asset Name**: Contains the asset name. The contents of this field serve as an active link for navigating to the Network Asset Details page. At the device level, the asset name is derived from the device label in IMC. Device labels are derived from sysName if it is configured and if the operator has not manually configured it. Asset names for component level assets are defined in the MIB for the device.
   - **Asset Description**: Contains a description for the asset. If the asset is a device, this field contains the device label. If it is a component, it contains the system description or sysDescr provided by the vendor if this information is available.
   - **Class**: Contains the asset classification for the asset type. Asset classes are defined by values defined in the Entity MIB.
   - **Device Label**: Contains the IMC name for the device, which, by default, is the name assigned to it in its device configuration. This field also contains the IP address. The device label serves as an active link for drilling down into the Device Details page, which offers you convenient access to device management features.
   - **Device Type**: Contains IMC’s categorization of the device. If the asset is a component, it inherits the device type from the parent device.
   - **Service Time**: Contains the date and time stamp marking the start date of the asset’s time in service.
   - **Physical Asset**: displays the physical property of the asset. **Yes** is displayed for a physical asset, and **No** is displayed for a non-physical asset.
   - **Remove**: Contains a link to delete the asset you want.

8. Click the icon to delete the assets whose physical properties you do not want to modify. Click Delete All to delete all assets.

9. Select the property from the Physical Asset list, which contains three options: **Computed by system**, **Yes**, and **No**. If you select the **Computed by system**, IMC determines whether an asset is physical in the following workflow:
   - If an asset is pluggable but is not an IRF member device, it is recognized as a physical asset.
   - If the OID of an asset is not suffixed with .0, the asset uses the physical property specified in the Asset OID entry.
   - If the OID of an asset is suffixed with .0 and the name does not contain the term "virtual" (case-insensitive), the asset is recognized as a physical asset.
   - If all these conditions are not satisfied, the asset is recognized as a non-physical asset.

10. If you select the **Yes**, the asset is recognized as a physical asset by force.

11. If you select the **No**, the asset is recognized as a non-physical asset by force.
12. If you have selected Yes or No for a device, when the physical properties of the device change, the physical properties of the device are not changed in the IMC after the IMC synchronizes the device.

13. Click OK.

14. Check whether the Physical Asset properties of the assets modified are synchronized in the Network Asset List.

Auditing a network asset

To perform an audit for a selected device:

2. Click the Resource tab from the tabular navigation system on the top.
3. Click the Network Assets section of the navigation tree on the left.
4. Click Network Assets under Network Assets from the navigation tree on the left. The Network Asset List is displayed in the main portion of the Network Assets page.
5. Click the link in the Asset Name field for the device you want to execute an audit for. The Network Asset Details page is displayed for the selected device.
6. Click the Audit link located in the upper right corner of the Network Asset Details page. IMC immediately initiates an audit for the selected device.
7. Click Refresh to reload the web page and view an updated Network Asset Details page for the selected device.

Refreshing a network asset details view

To refresh a Network Asset Details page:

2. Click the Resource tab from the tabular navigation system on the top.
3. Click the Network Assets section of the navigation tree on the left.
4. Click Network Assets under Network Assets from the navigation tree on the left. The Network Asset List is displayed in the main portion of the Network Assets page.
5. Click the link in the Asset Name field for the device you want to view asset details for. The Network Asset Details page is displayed for the selected device.
6. Click the Refresh link located in the upper right corner of the Network Asset Details page to reload the web page and review any updated information for the selected device.

Removing a network asset

To remove a Network Asset Details page:

2. Click the Resource tab from the tabular navigation system on the top.
3. Click the Network Assets section of the navigation tree on the left.
4. Click Network Assets under Network Assets from the navigation tree on the left. The Network Asset is displayed in the main portion of the Network Assets page.
5. Click the link in the **Asset Name** field for the device you want to view asset details for. The **Network Asset Details** page is displayed for the selected device.

6. Click the **Remove** link located in the upper right corner of the **Network Asset Details** page.

7. Click **OK** to confirm the removal of the selected device from the **Network Asset Manager**.

Review the results of the removal operation from the **Network Assets** page.

---

**Network asset auditing**

With Network Asset Auditing, you can view change information for the managed network assets. Asset changes can include adding, modifying, and removing assets, modifying asset names and modifying hardware versions. From this page, you can also query the **Asset Audit** database using the **Asset Audit List** basic and advanced query features.

**Viewing the asset audit list**

The **Asset Audit List** provides you with a view of asset audit entries.

To view the **Asset Audit List**:

1. Navigate to **Resource→Asset Audit**.
2. Click the **Resource** tab from the tabular navigation system on the top.

3. Click the **Asset Audit** section of the navigation tree on the left.

   The **Network Asset List** is displayed in the main portion of the **Asset Audit** page.

**Asset Audit List**

- **Audit Time**: Contains the date and time stamp for the asset’s audit.
- **Device Label**: Contains the IMC name for the device, which, by default, is the name assigned to it in its device configuration. This field also contains the IP address. The device label serves as an active link for drilling down into the **Device Details** page, which offers you convenient access to device management features.
- **Asset Class**: Contains the asset classification for the asset type.
- **Asset Name**: Contains the asset name. The contents of this field serve as an active link for navigating to the **Network Asset Details** page. For more information on the Network Asset Details page, see "Viewing device level network asset details" (page 346).

At the device level, the asset name is derived from the device label in IMC. Device labels are derived from `sysName` if it is configured and if the operator has not manually configured it.

- **Audit Option**: Contains information on the type of change that was discovered in the audit process. Audit options include **Add Asset**, **Delete Asset**, **Modify Asset Name**, **Modify Hardware Version**, **Modify Firmware Version**, **Modify Software Version**, **Modify Serial Number**, **Modify Model Name**, **Modify Alias**, **Modify Asset ID**, and **Modify Building Information**.
- **Before Change**: Contains a description of the asset prior to the change.
- **After Change**: Contains a description of the asset after the change.

If the **Asset Audit List** contains enough entries, the following navigational aids are displayed.

- Click **»** to page forward in the **Asset Audit List**.
Click to page forward to the end of the Asset Audit List.
Click to page backward in the Asset Audit List.
Click to page backward to the front of the Asset Audit List.

4. Click 8, 15, 50, 100, or 200 from the right side of the main pane to configure how many items per page you want to view.

5. For lists that have more than one page, click 1, 2, 3, 4, 5, 6, 7, 8, 9, 10… from the bottom right side of the main pane to jump to a particular page of the list.
You can view asset information only for the devices to which they have been granted management access.

Asset audit query

You can query the Asset Audit List for audit records for specific devices. You have two options for querying: a basic query and an advanced query. The following sections provide information on each of these query methods.

Basic query

To perform a basic query:

1. Navigate to Resource → Asset Audit.
2. Click the Resource tab from the tabular navigation system on the top.
3. Click the Network Assets section of the navigation tree on the left.
4. Click Asset Audit under Network Assets from the navigation tree on the left. The Asset Audit List is displayed in the main portion of the Network Assets page.

The Asset Audit Query section of the Network Assets page is located at the top of the main pane.

The Basic Query dialog box is displayed (by default) above the Network Asset list. The link to the far right is a toggle between Basic Query and Advanced Query. If the link is Advanced Query, then you are in the Basic Query mode.

5. Enter one or more search criteria in the fields provided.
   - Device IP: Enter the IP address of the device you want to locate audit records for in the Device IP field. You can use the asterisk (*) as a wildcard for one or more digits in the IP address.
   - Device Label: Enter the IMC name for the device in the Device Label field.
   - Asset Name: Enter the name of the asset in the Asset Name field.

6. Click Query. The result of the query is displayed in the Asset Audit List portion of the page.

Advanced query

To perform an advanced query:

2. Click the Resource tab from the tabular navigation system on the top.
3. Click the Network Assets section of the navigation tree on the left.
4. Click Asset Audit under Network Assets from the navigation tree on the left. The Asset Audit List is displayed in the main portion of the Asset Audit page.
The Network Asset Query section of the **Network Assets** page is located at the top of the main pane.

The Basic Query dialog box is displayed (by default) above the Network Asset list. The link to the far right is a toggle between Basic Query and Advanced Query. If the link is Advanced Query, then you are in the Basic Query mode. Click **Advanced Query** to navigate to the Advanced Query page.

5. Enter one or more search criteria in the fields provided.
   - **Device IP**: Enter the IP address of the device you want to locate audit records for in the Device IP field. You can use the asterisk (*) as a wildcard for one or more digits in the IP address.
   - **Device Label**: Enter the IMC name for the device in the Device Label field.
   - **Asset Name**: Enter the name of the asset in the Asset Name field.
   - **Asset Class**: Select the asset class you want to locate audit records for from the Asset Class list. Options include **All Classes** and **Subassembly**. If you choose **All Classes**, IMC locates audit records for all asset classes. If you choose **Subassembly**, the page updates to include a list of audit records for sub assembly asset classes only. By default, all subassembly options are selected. To remove options from the search, deselect the subassembly classes you do not want to search for by clicking the check marked box ✔ to the left of each subassembly type.
   - **Audit Options**: This option lets you search for all or specific types of audit records. To locate all audit records, verify that the radio button ○ to the left of **All** is selected. To locate specific audit records, click on the radio button ○ to the left of **Selected**. By default, all audit record types are selected. To remove options from the search, deselect the type of audit records you do not want to search for by clicking the check marked box ✔ to the left of each audit record type.
   - **Audit Start Time**: Enter a date and time for the audit start time for the assets you want to locate. Click on the calendar icon ☀ to the right of the **Audit Start Time** to input the start time using the calendar function.
   - **Audit End Time**: Enter a date and time for the audit end time for the assets you want to locate. Click on the calendar icon ☀ to the right of the **Audit End Time** to input the end time using the calendar function.

6. Click **Query**. The result of the query is displayed in the **Network Asset List** portion of the page.
7. Click **Reset** when you have finished restoring the **Network Asset List** to a complete display of all asset audit records.

**Network Asset Global Configuration Options**

You can add devices to network asset management when devices are added to IMC. In addition, IMC lets you configure how frequently automatic asset audit synchronization occurs. For more information on this option, see "Configuring network asset audit options" (page 152).

**Virtual Network Manager**

VNM provides lets you manage virtual network devices such as physical servers, vManager (a server that manages virtual servers), virtual machines, and virtual switches. You can view virtual network
resource configuration in Virtual Network View. By creating a vSwitch or port group, you can plan and manage your network. VNM can manage two types of vManagers, Microsoft Virtual Machine Manager and VMware vCenter Server.

In addition, VNM provides the virtual machine migration function. You can migrate a virtual machine from a physical server with limited resources to a physical server with enough resources to ensure the efficiency of the virtual machine. VNM automatically collects data on the vManager. In the Migration Recommendation List, you can select manual or automatic migration. After the migration is complete, you can view the migration report.

The vManager users must be granted proper privileges to exchange data between VNM and the vManager, add modify, and delete vSwitches and port groups, and perform virtual machine migration.

To read data from VMware vCenter Server, the user must have at least the read-only privilege. To add, modify, or delete a vSwitch or port group, the user must be an administrator or have the network configuration privilege on vCenter Server. To perform application or virtual machine migration, the user must be an administrator or have the following privileges on vCenter Server:

- Resource > Querying VMotion
- Resource > Migration
- Resource > Migration recommendation
- Resource > Assigning virtual machines to resource pools
- Resource > Redirect

Only the root user can read data from an ESX server or perform other operations when the user directly accesses the ESX server through VNM.

The domain users can perform all operations on Microsoft Virtual Machine Manager after they join the local Users group of the VNM server. To enable VNM to read data from or perform other operations on a Hyper-V server, make sure that the related user belongs to the Administrators group on the Hyper-V server.

With the Topology function, you can see the virtual network architecture, facilitating planning a virtual network.

### Viewing virtual network

Virtual Network View displays all resources and their relationship in a virtual network in a list. The list can expand and collapse, and includes three levels. In the list, the first-level nodes are physical servers (for example, VMware ESX server or Microsoft Hyper-V server), the second-level nodes are virtual switches created on the servers, and the third-level nodes are virtual machines connected to the virtual switches. You can click a resource name to view detailed resource information and perform operations on different resources.

### Virtual network view

To view the virtual network:

2. Click the Resource tab from the tabular navigation system on the top.
3. Click the Virtual Network Manager section of the navigation tree on the left.
4. Click Virtual Network View under Virtual Network Manager from the navigation tree on the left. The Virtual Network View is displayed in the main portion of the Virtual Network Manager page.

Virtual network view

- **Expand/Collapse icon**: Contains the expand/collapse icon to expand or collapse the associated resources (physical server). Click the icon to expand the associated physical server to view the virtual switches and virtual machines performed on the server. Click the icon to collapse the physical server.
- **Resource Name**: Contains the server IP address and device label. The server name serves as a link for navigating to the Server Details page. For more information on server details, see “Viewing server level details” (page 359).
- **Status**: Contains the alarming status of the server.
- **Operation**: Contains the Topology icon. Clicking the topology icon navigates you to the VNM Topology.
- **Vendor**: Contains the vendor of the server.
- **Model**: Contains the model of the server.
- **Data Center**: Contains the name of the data center where the server resides.
- **vManager**: Contains information about the vManager for managing the server.
- **Memory**: Contains the memory size of the server.
- **CPU**: Contains the CPU information of the server.
- **Support Migration**: Contains information about whether or not the server supports migration.

Viewing the resource list for a server

The resource list includes the server, virtual switch, and virtual machine.

To view the resource list for a server:

2. Click the Resource tab from the tabular navigation system on the top.
3. Click the Virtual Network Manager section of the navigation tree on the left.
4. Click Virtual Network View under Virtual Network Manager from the navigation tree on the left. The Virtual Network View is displayed in the main portion of the Virtual Network Manager page.
5. Click the expand icon located to the left of the server that you want to view the resource list for.

The resource list of the server appears.

Resource list

- **Resource Name**: Contains the name of the virtual network device. The contents of this field serve as an active link for navigating to the details page.
- **Status**: Contains the status of the virtual network device. For a physical server, this field displays the alarming status; for a virtual machine, this field displays Started, Closed, and Suspend; for a virtual switch, this field displays no data.
- **Type**: Contains the virtual network device type.
- **IP Address**: Contains the IP Address of the virtual network device.
- **Operation**: Contains five operations, including Topology, Join IMC, Manual Migration (the Manual Migration icon is displayed only when the device joins IMC), Migration Recommendations, and Migration Reports.

**Viewing server level details**

The Server Details page provides virtual network resources such as virtual machines and vSwitch, and allocation of the resources. The tree graph on the left displays the relationship between items under the server. The tabs on the right display the server information, virtual machine configuration, vSwitch configuration, Port Group configuration, Network Card configuration, and Storage Device configuration. Four common buttons are provided at the upper right corner. They let you perform add vSwitch, add port group, synchronize, and quickly refresh operations.

**Accessing the server details page**

To access physical server details:

2. Click the Resource tab from the tabular navigation system on the top.
3. Click the Virtual Network Manager section of the navigation tree on the left.
4. Click Virtual Network View under Virtual Network Manager from the navigation tree on the left. The Virtual Network View is displayed in the main portion of the Virtual Network Manager page.
5. Click the link in the Resource Name field for the server you want to view details for. The Server Details page is displayed for the selected server.

**Server**

Server details contains the server information that the IMC server obtains, including Server Name, IP Address, Vendor, CPU, Memory, whether migration is supported, Datacenter, and vManager.

Some of the fields in the Server tab include:

- **Server Name**: Contains the name of the server.
- **Status**: Contains the alarming status of the server.
- **IP Address**: Contains the IP address of the server.
- **Label**: Contains the label of the server. The value can be modified in the device details information.
- **Vendor**: Contains the vendor of the server.
- **Model**: Contains the model of the server.
- **CPU**: Contains the CPU information of the server.
- **Memory**: Contains the memory size of the server.
- **Support Migration**: Contains information about whether the server supports migration.
• **Datacenter**: Contains the name of the data center where the server resides.
• **vManager**: Contains information about vManager for managing the server.

**Virtual machine**
The virtual machines of the **Server Details** page provide a list of all virtual machines for the selected server.

To access the Virtual Machine list, click the Virtual Machine tab in the Detail of Server page:

• **Virtual Machine Name**: Contains the name for the Virtual Machine. You can click the name link to enter the details page of the virtual machine. On this page, you can view the hardware configuration, status, virtual network information, and the storage device information of the virtual machine.
• **IP Address**: Contains the IP Address of the Virtual Machine.
• **Status**: Contains the status of the Virtual Machine, including Started, Closed, and suspended.
• **Migration Report**: Contains a link for view virtual machine migration report.
• **Manual Migration**: Contains a link for triggering manual migration.
• **VM Profile**: Contains a link for modifying Profile.

**vSwitch**
The vSwitch tab of the **Server Details** page provides a list of all vSwitch performed on the selected servers.

To access the vSwitch list, click the vSwitch tab in the Server Details page:

• **Name**: Contains the name of the vSwitch.
• **Number of Ports**: Contains the port number of the vSwitch.
• **Modify**: Contains a link for modifying the associated vSwitch.
• **Properties**: Contains a link for modifying the advanced properties of the vSwitch.
• **Delete**: Contains a link for deleting the associated vSwitch.

**Port group**
The Port Group tab of the **Server Details** page provides a list of all port groups performed on the selected servers. The operations in the Port Group tab apply to only the VMware physical servers.

To access the Port Group list, click the Port Group tab in the Server Details page:

• **Name**: Contains the name of the port group.
• **Type**: Contains the type of the port group.
• **VLAN ID**: Contains the VLAN ID of the port group.
• **vSwitch**: Contains the vSwitch to which the port group belongs.
• **IP Address**: Contains the IP Address of the port group.
• **Mask**: Contains the mask of the IP Address.
• **Modify**: Contains a link for modifying the associated port group.
• **Properties**: Contains a link for modifying the advanced properties of a port group.
• **Remove**: Contains a link for removing the associated port group.

**Network card**
The **Network Card** tab of the **Server Details** page provides a list of all network cards on the selected servers.

To access the **Network Card** list, click the **Network Card** tab in the **Server Details** page.

- **Network Card Name**: Contains the name of the network card.
- **vSwitch**: Contains the vSwitch where the network card resides.
- **Type**: Contains the type of the network card.
- **IP Address**: Contains the IP Address of the network card.
- **Mask**: Contains the mask of the IP Address.
- **Status**: Contains the status of the network card.

**Storage**

The **Storage** tab of the **Server Details** page provides a list of all storage devices for the selected servers.

To access the **Storage** list, click the **Storage** tab in the **Server Details** page.

- **Name**: Contains the name of the storage device.
- **Type**: Contains the type of the storage device.
- **Capacity (GB)**: Contains the capacity of the storage device, in GB.
- **Free Space (GB)**: Contains the free space of the storage device, in GB.

**Viewing the virtual network topology**

To view the virtual network topology:

1. Navigate to **Resource → Virtual Network Manager**.
2. Click the **Resource** tab from the tabular navigation system on the top.
3. Click the **Virtual Network Manager** section of the navigation tree on the left.
4. Click **Virtual Network Topology** under **Virtual Network Manager** from the navigation tree on the left.
5. Or, click **Virtual Network View** under **Virtual Network Manager** from the navigation tree on the left. The **Virtual Network View** is displayed in the main portion of the **Virtual Network Manager** page. Select a server or VM in the **Virtual Network View** list. Click **Operation** in the column.

The **VNM Topology** is displayed in the **Network Topology** page.

6. You can check the connection status of the virtual network. Double click a server icon or double click the blank area of the expanded sub-view to automatically expand or collapse the view to display or hide virtual switches and virtual machines on the server.

For detailed Topology operations, see "Viewing devices via the Network Topology" (page 181).

**Server query**

You can query the **servers** for viewing detailed server information or virtual network information. The following section provides information on the query.

To perform server query:
2. Click the Resource tab from the tabular navigation system on the top.
3. Click the Virtual Network Manager section of the navigation tree on the left.
4. Click 🔄Virtual Network View under Virtual Network Manager from the navigation tree on the left. The Virtual Network View is displayed in the main portion of the Virtual Network Manager page.
5. Move the pointer over Query at the upper right corner of Virtual Network View, and a search criteria dialog box appears.
6. Enter one or more search criteria in the fields provided.
   a. Server Name: Enter the name of the server in the Server Name field.
   b. IP Address: Enter the IP address of the server you want to locate server information for in the Device IP field.
   Both options support fuzzy match.
7. Click Query. The results of the query are displayed in the Virtual Network View portion of the page.
8. Click Reset when you have finished your search to restore the full Virtual Network View list.

Refreshing virtual network view
To refresh the Virtual Network View page:
2. Click the Resource tab from the tabular navigation system on the top.
3. Click the Virtual Network Manager section of the navigation tree on the left.
4. Click 🔄Virtual Network View under Virtual Network Manager from the navigation tree on the left. The Virtual Network View is displayed in the main portion of the Virtual Network Manager page.
5. Click the 🔄Refresh link located in the upper left corner of the Virtual Network View page to reload the web page and review any updated information.

Configuring servers in Virtual Network Manager
Adding vSwitch
To add a vSwitch to a server:
2. Click the Resource tab from the tabular navigation system on the top.
3. Click the Virtual Network Manager section of the navigation tree on the left.
4. Click 🔄Virtual Network View under Virtual Network Manager from the navigation tree on the left. The Virtual Network View is displayed in the main portion of the Virtual Network Manager page.
5. Click the Resource Name or the IP Address link of the server for which you want to add vSwitch. The Server Details page appears.
6. Click on the Add vSwitch link located in the upper right corner of the Server Details page. The Add vSwitch page appears.
7. Enter the name of the vSwitch.
8. Use the scrolling bar to select Number of the Ports, which ranges from 1 to 1016.
9. Select one or more Physical Network Cards.
10. Highlight the network cards you want to select and click on the Select button.
11. To select all of the physical network cards displayed in the Physical Network Card list, click the Select All button.
12. Do one of the following:
   o To remove one or more, select them and click Remove, or
   o To remove all of the selected devices, click Remove all.
13. Confirm that the physics network cards you have found have been added.
14. Click OK.

Adding port group
To add a port group to a server:
2. Click the Resource tab from the tabular navigation system on the top.
3. Click the Virtual Network Manager section of the navigation tree on the left.
4. Click Virtual Network View under Virtual Network Manager from the navigation tree on the left. The Virtual Network View is displayed in the main portion of the Virtual Network Manager page.
5. Click the Resource Name or the IP Address link of the server for which you want to add port group. The Server Details page appears.
6. Click the Add Port Group link located in the upper right corner of the Server Details page. The Add Port Group page appears.
7. Select a type of port group from the Type list.
8. Enter the name of the port group in the Name field.
9. Enter the VLAN ID in the VLAN ID field.
10. Select a vSwitch from the vSwitch list.
11. Enter the IP Address of the network card that binds to the vSwitch.
   If you select VMkernel in Step4, this option is required.
12. Enter the Mask of the IP address in the Mask field.
   If you select VMkernel in Step4, this option is required.
13. Click OK.

Refreshing a server details page
To refresh the Server Details page:
2. Click the Resource tab from the tabular navigation system on the top.
3. Click the **Virtual Network Manager** section of the navigation tree on the left.

4. Click **Virtual Network View** under **Virtual Network Manager** from the navigation tree on the left. The **Virtual Network View** is displayed in the main portion of the **Virtual Network Manager** page.

5. Click the **Resource Name** or the **IP Address** of the server you want to view information. The **Server Details** page appears.

6. Click the **Refresh** link located in the upper right corner of the **Server Details** page to reload the web page and review any updated information.

---

**Configuring virtual machines in Virtual Network Manager**

**Joining a virtual machine in IMC**

To add a virtual machine in IMC:

1. Navigate to **Resource**→**Virtual Network View**.
2. Click the **Resource** tab from the tabular navigation system on the top.
3. Click the **Virtual Network Manager** section of the navigation tree on the left.
4. Click **Virtual Network View** under **Virtual Network Manager** from the navigation tree on the left.
   
   The **Virtual Network View** is displayed in the main portion of the **Virtual Network Manager** page.

5. In **Virtual Network View**, add a virtual machine to IMC. Click **Join IMC** in the **Operation** column.
   
   The **Add Device** page appears.

6. Enter related parameters. Click **OK**. For more information, see "Adding devices manually to IMC" (page 154).

**Manually migrating a virtual machine**

You can migrate a virtual machine only when you add it into IMC. To manually migrate a virtual machine:

1. Navigate to **Resource**→**Virtual Network View**.
2. Click the **Resource** tab from the tabular navigation system on the top.
3. Click the **Virtual Network Manager** section of the navigation tree on the left.
4. Click **Virtual Network View** under **Virtual Network Manager** from the navigation tree on the left.
   
   The **Virtual Network View** is displayed in the main portion of the **Virtual Network Manager** page.

5. Click **Manual Migration** in the **Operation** column of the virtual machine that you want to manually migrate in **Virtual Network View**.
   
   The **Manual Migration** page appears.

6. Click the **Select Resource Pool** link corresponding to Target Server.
   
   The **Resource Pool** page appears.
7. Select a resource pool from the Resource Pool list.
8. Click OK.
9. Click OK.

Configuring auto migration

To configure auto migration mode:
2. Click the Resource tab from the tabular navigation system on the top.
3. Click the Virtual Network Manager section of the navigation tree on the left.
4. Click Migration Recommendations under Virtual Network Manager from the navigation tree on the left.
   The Recommendation List is displayed in the main portion of the Virtual Network Manager page.
5. Click Mode: Auto link in the upper right corner of the Recommendation List.
   The Migration Settings page appears.
6. Select the type of virtual machine migration from the Mode list.
7. Use the scrolling bar to select the trigger time in the Execute after (minute) field.
8. Click OK.

Modifying a VM profile

To modify a VM profile:
1. Navigate to Resource→VM Profile.
2. Click the Resource tab from the tabular navigation system on the top.
3. Click the Virtual Network Manager section of the navigation tree on the left.
4. Click VM Profile under Virtual Network Manager from the navigation tree on the left.
   The VM Profile List is displayed in the main portion of the Virtual Network Manager page.

VM profile list

- **Virtual Machine**: Contains the name of the virtual network device. The contents of this field serve as an active link for navigating to the Network Asset Details page. At the device level, the asset name is derived from the device label in IMC. Device labels are derived from sysName if it is configured and if the operator has not manually configured it. Asset names for component level assets are defined in the MIB for the device.
- **IP Address**: Contains the IP Address of the virtual network device.
- **Source Server**: Contains a link of Source Server. You can click this link to enter the Detail of Server page.
- **Migration Report**: Contains a link for the associated Migration Report.
- **Modify**: Contains a link for modifying the associated VM Profile.

If the Audit History list contains enough entries, the following navigational aids are displayed.
- Click to page forward in the VM Profile List.
5. Click 8, 15, 50, 100, or 200 from the right side of the main pane to configure how many items per page you want to view.

6. For VM Profile lists that have more than one page, click 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 … from the bottom right side of the main pane to jump to a particular page of the list.

   You can sort the VM Profile List by the Virtual Machine, IP Address fields. Click the column label to sort the list by and the selected field. The column label is a toggle switch that lets you toggle between the various sort options specific to each field.

7. Click the Modify link of the virtual machine for which you want to modify profile. The Modify Profile page appears.

8. Enter the commands for configuring the switch connected to the virtual machine in the Profile field.

9. Click OK.

Viewing virtual machine recommendations

To view the Recommendations of a Virtual Machine:


2. Click the Resource tab from the tabular navigation system on the top.

3. Click the Virtual Network Manager section of the navigation tree on the left.

4. Click Migration Recommendations under Virtual Network Manager from the navigation tree on the left. The Recommendation List is displayed in the main portion of the Virtual Network Manager page.

Recommendation list

- **vManager**: Contains the vManager name and IP address. The contents of this field serve as an active link for navigating to the device details page.

- **Reason**: Contains the reason for virtual machine migration.

- **Created**: Contains the time when recommendations were created. If you select automatic migration, the system calculates the automatic migration trigger time by using this time as the start time.

- **Status**: Contains the status of the recommendations.

- **Rating**: Contains the rating of the recommendations.

- **Manually Execute**: Contains a link for triggering manual migration.

- **Source Virtual Machine**: Contains the name of the source virtual machine. The contents of this field serve as an active link for navigating to the source virtual machine details page.

- **Source Server**: Contains the name of the source server. The contents of this field serve as an active link for navigating to the Detail of Server page.

- **Target Server**: Contains the name of the destination server. The contents of this field serve as an active link for navigating to the Detail of Server page.
Migration Status: Contains the migration status.

If the Recommendation List contains enough entries, the following navigational aids are displayed.

- Click ⏳ to page forward in the Recommendation List.
- Click ⏳ to page forward to the end of the Recommendation List.
- Click ⏳ to page backward in the Recommendation List.
- Click ⏳ to page backward to the front of the Recommendation List.

5. Click 8, 15, 50, 100, or 200 from the right side of the main pane to configure how many items per page you want to view.

6. For Recommendation lists that have more than one page, click 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 … from the bottom right side of the main pane to jump to a particular page of the list.

You can sort the Recommendation List by the Reason, Created, Status, Rating, and Source Virtual Machine fields. Click the column label to sort the list by the selected field. The column label is a toggle switch that lets you toggle between the various sort options specific to each field.

**Querying migration recommendations**

To query migration recommendations:

2. Click the Resource tab from the tabular navigation system on the top.
3. Click the Virtual Network Manager section of the navigation tree on the left.
4. Click ⬤ Migration Recommendations under Virtual Network Manager from the navigation tree on the left.
   
The Recommendation List is displayed in the main portion of the Virtual Network Manager page.
5. Move the pointer over Query at the upper right corner of the Recommendation List, and a search criteria dialog box appears.
6. Enter one or more search criteria in the fields provided.
   - **Virtual Machine Name**: Enter the virtual machine name.
   - **Source Server**: Enter the source server name for virtual machine migration.
   - **Target Server**: Enter the target server name for virtual machine migration.
   - **Rating**: Select the virtual machine migration rating from Rating list.
   - **Status**: Select the virtual machine migration status from the Status list.
   - **Reason**: Enter the reason for the migration.
   - **Migration Status**: Select the migration status of the virtual machine from the Migration Status list.
   - **Created from**: Enter a date and time for the created time for the recommendations you want to locate. Click the calendar icon ⌚ to the right of the Created from to input the start time using the calendar function.
To: Enter a date and time for the end time for the recommendations you want to locate. Click the calendar icon to the right to input the end time using the calendar function.

7. Click Query. The results of the query are displayed in the Recommendation List portion of the page.

**Viewing migration reports of the virtual machine**

To view the Migration Report of the VM:

1. Navigate to Resource→Migration Reports.
2. Click the Resource tab from the tabular navigation system on the top.
3. Click the Virtual Network Manager section of the navigation tree on the left.
4. Click Migration Reports under Virtual Network Manager from the navigation tree on the left.

The Migration Report List is displayed in the main portion of the Virtual Network Manager page.

**Migration Report List**

- **Virtual Machine**: Contains the name of the virtual device. The contents of this field serve as an active link for navigating to the Virtual Machine details page.
- **Source Server**: Contains the name of the source server of the virtual machine.
- **Target Server**: Contains the name of the target server of the virtual machine. The contents of this field serve as an active link for navigating to the Detail of Server page.
- **Status**: Contains the status of virtual machine migration.
- **Type**: Contains the type of virtual machine migration, including manual and auto.
- **Start Date**: Contains the start date for virtual machine migration.
- **End Date**: Contains the end date for virtual machine migration.
- **View Report**: Contains a link for viewing the associated migration report.

If the Migration Report list contains enough entries, the following navigational aids are displayed.

- Click > to page forward in the Migration Report List.
- Click > to page forward to the end of the Migration Report List.
- Click > to page backward in the Migration Report List.
- Click > to page backward to the front of the Migration Report List.

5. Click 8, 15, 50, 100, or 200 from the right side of the main pane to configure how many items per page you want to view.

6. For Migration Report lists that have more than one page, click 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 ... from the bottom right side of the main pane to jump to a particular page of the list.

You can sort the Migration Report List by the Virtual Machine, Source Server, Status, Type, Start Date, End Date, and View Report fields. Click the column label to sort the list by the selected field. The column label is a toggle switch that lets you toggle between the various sort options specific to each field.
7. Click the View Report link corresponding to the VM that you want to migrate. The Migration Report appears.

8. In the Virtual Machine Information, you can view information such as Virtual Machine Name, IP Address, Source Server, Source Server IP, Target Server, and Target Server IP. You can view the migration steps in the Step of Migration Report list.

9. Click the upper right corner of the page to close the page.

Querying migration reports

To query migration report:
1. Navigate to Resource→Migration Reports.
2. Click the Resource tab from the tabular navigation system on the top.
3. Click the Virtual Network Manager section of the navigation tree on the left.
4. Click Migration Reports under Virtual Network Manager from the navigation tree on the left. The Migration Report List is displayed in the main portion of the Virtual Network Manager page.
5. Move the pointer over Query at the upper right corner of the Migration Report List, and a search criteria dialog box appears.
6. Enter one or more search criteria in the fields provided.
   o Virtual Machine: Enter the virtual machine name.
   o Source Server: Enter the source server name for virtual machine migration.
   o Target Server: Enter the target server name for virtual machine migration.
   o Status: Select the virtual machine migration status from the Status list.
   o Type: Select the virtual machine migration type from the Type list.
   o Start Date (From): Select a time for the start date time range. Enter a date and time for the query start time for the migration reports you want to locate. Click the calendar icon to the right of the Start Date (From) to input the date and time using the calendar function.
   o Start Date (To): Select a time for the start date time range. Enter a date and time for the query start time for the migration reports you want to locate. Click the calendar icon to the right of the Start Date (To) to input the date and time using the calendar function.
   o End Date (From): Select a time for the end date time range. Enter a date and time for the query end time for the migration reports you want to locate. Click the calendar icon to the right of the End Date (From) to input the date and time using the calendar function.
   o End Date (To): Select a time for the end date time range. Enter a date and time for the query end time for the migrations you want to locate. Click the calendar icon to the right of the End Date (To) to input the date and time using the calendar function.
7. Click Query. The result of the query is displayed in the Migration Report List portion of the page.
Modifying the advanced properties of a vSwitch or port group

To modify the advanced properties of a vSwitch or port group:

2. Click the Resource tab from the tabular navigation system on the top.
3. Click the Virtual Network Manager section of the navigation tree on the left.
4. Click Virtual Network View under Virtual Network Manager from the navigation tree on the left.
   The Virtual Network View is displayed in the main portion of the Virtual Network Manager page.
5. Click the link in the Resource Name field for the server you want to view details for.
   The Server Details page is displayed for the selected server.
6. Click the vSwitch or Port Group tab at the right part of the Server Details page.
7. On the vSwitch or Port Group tab, click the link in the Properties area of the vSwitch or port group that you want to modify to open the Properties window.
   The Properties page provides the following types of parameters: Security, Traffic Shaping, and NIC Teaming.

Security

- Promiscuous Mode: Specify whether to enable the promiscuous mode, which provides the Reject and Accept options. Selecting the Reject option configures the VM adapter to operate in non-promiscuous mode. A VM adapter operating in non-promiscuous mode does not affect the received frames. Selecting Accept configures the guest adapter to operate in promiscuous mode. In this mode, the guest adapter can detect all frames passed on the vSwitch that are allowed under the VLAN policy for the port group in which the adapter is connected.

- MAC Address Changes: Specify whether to accept the MAC address changes. This feature provides the Reject and Accept options. When you select Reject, if the VM changes the MAC address of the adapter to anything other than what is in the .VMX configuration file, all inbound frames are dropped. If the VM changes the MAC address back to match the MAC address in the .VMX configuration file, inbound frames are passed again. When you select Accept, if the VM changes the MAC address of the adapter to anything other than what is in the .VMX configuration file, frames to the new MAC address are received.

- Forget Transmits: Specify whether to filter the outbound frames. This feature provides the Reject and Accept options. If you select Reject, any outbound frame with a source MAC address that is different from the one currently set on the adapter are dropped. If you select Accept, no filtering is performed and all outbound frames are passed.

Traffic shaping

- Status: Specify whether to adjust the outbound traffic on vSwitches. This feature provides the Disable and Enable options. If you select Enable, you must configure the following parameters:
  - Average Bandwidth(Kbit/s): Average bandwidth (in Kbps) of a port.
  - Burst Size(KByte): The maximum number of bytes (in KB) allowed in a burst. If this parameter is set, a port can gain a burst bonus when it does not use all its allocated bandwidth. Whenever the port needs more bandwidth than specified by Average Bandwidth, it can be
allowed to temporarily transmit data at a higher speed if a burst bonus is available. This parameter tops the number of bytes that may be accumulated in the burst bonus and thus transferred at a higher speed.

- **Peak Bandwidth (Kbit/s)**: Set the peak bandwidth (in Kbps) of a port. The peak bandwidth specifies the maximum number of bits per second to allow across a port when it is sending a burst of traffic. This tops the bandwidth used by a port whenever it is using its burst bonus. This parameter can never be smaller than the average bandwidth.

**NIC teaming**

- **Load Balancing**: The load balancing policy determines how outgoing traffic is distributed among the network adapters assigned to a vSwitch. Incoming traffic is controlled by the load balancing policy on the physical switch. This feature provides the following options.
  - **Route based on the originating port ID**: Select an uplink based on the virtual port where the traffic entered the vSwitch.
  - **Route based on IP hash**: Select an uplink based on a hash of the source and destination IP addresses of each packet. For non-IP packets, whatever is at those offsets is used to compute the hash.
  - **Route based on source MAC hash**: Select an uplink based on a hash of the source MAC address of each packet.
  - **Use explicit failover order**: Always use the highest order uplink from the list of active adapters that passes failover detection criteria.

- **Network Failover Detection**: Set the failover detection method, which can be Link Status only or Beacon Probing.
  - **Link State only**: Relies solely on the link status that the network adapter provides. This option detects failures, such as cable pulls and physical switch power failures, but not configuration errors, such as a physical switch port being blocked by spanning tree or misconfigured to the wrong VLAN or cable pulls on the other side of a physical switch.
  - **Beacon Probing**: Sends out and listens for beacon probes on all NICs in the team and uses this information, in addition to link status, to determine link failure. This option detects many of the failures mentioned above that are not detected by link status alone.
  - **Notify Switches**: Specify that a notification is sent over the network to update the lookup tables on the physical switches whenever a virtual NIC is connected to the vSwitch or whenever that virtual NIC’s traffic is routed over a different physical NIC in the team because of a failover event. If you select Yes, whenever a virtual NIC is connected to the vSwitch or whenever that virtual NIC’s traffic is routed over a different physical NIC in the team because of a failover event, a notification is sent over the network to update the lookup tables on the physical switches. In most cases, this is desirable for the lowest latency of failover occurrences and migrations with VMotion. Do not use this option when the virtual machines using the port group are using Microsoft Network Load Balancing (NLB) in unicast mode. No such issues exist with NLB running in multicast mode.
  - **Failback**: Specify how a physical adapter is returned to active duty after recovering from a failure. If failback is set to Yes, the adapter is returned to active duty immediately on recovering, displacing the standby adapter that took over its slot, if any. If failback is set to No, a failed adapter is left inactive even after recovery until another active adapter fails, requiring its replacement.
8. Use the **Failover Order** option to specify how to distribute the work load for adapters. To use some adapters but reserve others for emergencies, you can place them into the following groups.
   - **Active Adapters**: Specifies the active adapters. The vSwitch can continue to use the adapter when the network adapter connectivity is available and active.
   - **Standby Adapters**: Specifies the standby adapters. Use this adapter if one of the active adapter’s connectivity is unavailable.
   - **Unused Adapters**: Specifies the unused adapters. Do not use this adapter.
   
   The **Active Adapters**, **Standby Adapters**, and **Unused Adapters** are in descending priority order.

9. Click the ⬆️ link of an adapter to increase the priority of the adapter in the current group. If the adapter is of the highest priority in the current group, clicking the ⬆️ link adds it to a higher-priority group.

10. Click the ⬇️ link of an adapter to decrease the priority of the adapter in the current group. If the adapter is of the lowest priority in the current group, clicking the ⬇️ link adds the adapter to a lower-priority group.

11. Click **OK**.

12. To modify the advanced properties of a **Port Group**, select the checkbox ☑️ before the properties to active the properties.
6 Extending and customizing functions to support third-party devices

The IMC basic network management platform supports extending device management and configuration functions through dynamic language scripts. You can either extend an existing function to support third-party devices by compiling interactive scripts and XML files, or customize a function by compiling interactive scripts, XML files, and UI configuration files.

In either way, you can define vendor, drive, service, and action scripts through XML files, define device interaction through standard TCL\Expect scripts, and parse or process returned information through standard Perl scripts. Before customizing a function, you must compile UI configuration files so that IMC can automatically add the operation entrance and display pages as required.

The function extension feature makes investment in IMC rewarding in a long term, and provides powerful regular expression processing capability by using the Expect and Perl language scripts.

Extending an existing function to support third-party devices

You can extend IMC components to support third-party device management by customizing scripts. For example, by default, the IMC Configuration Center component supports configuration file management and software upgrade for devices of HP, Cisco, and many other vendors.

You can enable the component to support configuration file backup and deployment and software upgrade for other third-party devices by customizing the script. By default, IMC VLAN Manager supports VLAN management for devices of HP, Cisco, and many other vendors. You can also enable the component to support VLAN management for other third-party devices by customizing the script.

Follow these steps to customize a third-party device process:

- Create a vendor folder
- Create a drive index file and a drive folder
- Create a drive definition file
- Create various service and action definition files
- Create TCL and Perl scripts

The content under the directory \iMC\server\conf\adapters\ICC can be used as a reference. The following example illustrates how to extend Configuration Center to support Cisco devices.

Creating a vendor folder

Query the vendor name in IMC, and then create the vendor folder.

1. Query the vendor name:
2. Navigate to System--Resource Management--Device Vendor
3. Click the System tab from the tabular navigation system on the top.
4. Click **Resource Management** on the navigation tree on the left.

5. Click **Device Vendor** under **Resource Management** on the left navigation.

6. Enter the **Device Vendor List** page.

7. Enter the third-party device vendor name in the field on the left of **Vendor Name**.

8. Click **Query** to display all matching vendor names on the **Device Vendor List**. Locate the target vendor name.

   If the target vendor does not exist, you can customize the vendor, series, and model. For more information, see "Configuring vendor and device information" (page 92).

9. Create a folder under the directory `iMC\server\conf\adapters\ICC`.

10. Specify the target vendor name as the folder name.

### Creating a drive index file and a drive folder

A vendor can provide devices of multiple series or models. These devices can use the same or different drive files for communication between each other. To manage the mappings between devices and drive files, create a drive index file and then create a drive folder for each drive.

1. Open the third-party device vendor folder.

2. Create a drive index file named `adapter-index.xml`.

3. Create a drive folder (with customized name) for target devices. The drive corresponds to the devices with similar command lines for configuration back and deployment and software upgrade, for example, Cisco CatNative series.

4. Query the target third-party device model.

5. Navigation to **System** → **Resource Management** → **Device Vendor**

6. Click on the **System** tab from the tabular navigation system on the top.

7. Click the **Resource Management** on the navigation tree on the left.

8. Click - the **Device Model** under **Resource Management** from the navigation system on the left.

9. Enter the **Device Model List** page.

10. Enter the query criteria, and click **Query** to display all matching device models on the **Device Model List**.

11. Get the sysOID of the target third-party device.

12. Open the `adapter-index.xml` file, and create a drive folder for the device with the specified sysOID. You must create a drive folder for each drive, and use the drive name as the folder name. The format of the `adapter-index.xml` file:

```xml
<?xml version="1.0" encoding="UTF-8"?>
<!--sysOID adapt adapter-->  
<adapters>  
<default>CiscoIOSGeneric</default>  
<adapter name="CiscoIOSGeneric">  
  <description>Cisco routers,800,1700 IOS version 12.x</description>  
  <sysOID>1.3.6.1.4.1.9.1.17</sysOID>  
  <sysOID>1.3.6.1.4.1.9.1.208</sysOID>  
  <sysOID>1.3.6.1.4.1.9.1.185</sysOID>  
</adapter>  
</adapters>
```

376
Creating drive definition file

Each drive folder contains various TCL/Expect files, service and action XML definition files, and Perl files of the drive.

1. Open the drive folder.
2. Create a drive definition file adapter.xml.

The format of the adapter.xml file:

```xml
<adapter name="CiscoIOSGeneric">
  <description>Cisco routers, 800, 1700 series, IOS version 12.x</description>
  <version>1.0.0</version>
  <services>
    <uses-adapter vendor="H3C" adapter="H3CCommon"/>
    <service name="CLICommon">
      <item type="common">Cisco_Common_CLI.xml</item>
    </service>
    <service name="CleanupParser">
      <item type="parser_definition">Cisco_Cleanup_Parser.xml</item>
      <item type="perl_script">Cisco_Cleanup_Parser_Script.pl</item>
    </service>
    <service name="ConfigBackup">
      <item type="builder_definition">Cisco_Config_Backup_Builder.xml</item>
      <item type="tcl_script">Cisco_Config_Backup_Builder_Script.xml</item>
    </service>
    <service name="ConfigDeploy">
      <item type="builder_definition">Cisco_Config_Deploy_Builder.xml</item>
    </service>
  </services>
</adapter>
```

Notes:
1. Label of drives in fixed format.
2. Default drive is used when the sysOID of the device does not match any of the following drives.
3. Drive name must be the same as the name of the drive folder.
4. Description
5. sysOIDs supported by the drive.
6. Name of another drive supported by the vendor.
<item type="tcl_script">Cisco_Config_Deploy_Builder_Script.xml</item>
<!—note 12>
</service>
<service name="ImageDeploy">
    <item type="builder_definition">Cisco_Image_Deploy_Builder.xml</item>
    <item type="tcl_script">Cisco_Image_Deploy_Builder_Script.xml</item>
<!—note 11>
</service>
<!—note 12>
</service>
</services>
</adapter>

Note 1: Drive name must be the same as the name of the drive folder.
Note 2: Description.
Note 3: Label of services in fixed format.
Note 4: If the local drive has the same services and command lines as another drive, you can specify that drive. You must define services different from the drive in use. The system automatically searches for a service in the definition file. If the search fails, the system uses the specified drive.
Note 5: Common service name, which cannot be changed.
Note 6: The type must be common.
Note 7: Parse service name, which cannot be changed.
Note 8: Parse definition file, whose type must be parser_definition.
Note 9: Parse script file, whose type must be parser_script.
Note 10: Configuration backup service name, which cannot be changed.
Note 11: Action definition file, whose type must be builder_definition.
Note 12: Action implementation file, whose type must be tcl_script.
Note 13: Configuration deployment service name, which cannot be changed.
Note 14: Software deployment service name, which cannot be changed.

3. Open the adapter.xml file, and define services that the drive supports, including common service, parse service, configuration backup, configuration deployment, and software upgrade. The services other than the common services are determined by the extended component functions. The services above apply to Configuration Center and are different from those for VLAN component function extension. The services other than the common services are optional.
   o Common service (CLICommon) defines the device login process and common functions (for example, save/reboot/delete a file).
   o Parse service (CleanupParser) provides a series of Perl script functions for parsing returned information acquired from the device.
   o Each of the configuration backup (ConfigBackup), configuration deployment (ConfigDeploy), and software deployment (ImageDeploy) services comprises an action definition file (builder_definition) and an action script file (tcl_script). The action definition file defines the actions of the service and the processing procedure of each action; the action script file specifies the execution environment and execution script for each action.
Defining the common service (CLICommon)

The common service file name is `xxxxxx_Common_CLI.xml` (xxxxxx indicates the drive name). The common service file defines the device login process and common functions for device operations (for example, save/reboot/delete a file).

The format of the common service file:

```xml
<?xml version="1.0"?>
<common>                                                   <!—note 1>
    <mode name="initialize" method="CLI">                  <!—note 2>
        <require-mode>connect</require-mode>               <!—note 3>
        <enter>                                           <!—note 4>
            initialize.tcl                                 <!—note 5>
        </enter>                                         <!—note 6>
    </mode>
    <mode name="exec" method="CLI">                         <!—note 7>
        <error>Failed to get to exec mode. </error>         <!—note 8>
        <require-mode>initialize</require-mode>             <!—note 9>
        <enter>                                           <!—note 10>
            enter_exec.tcl                                  <!—note 11>
        </enter>                                         <!—note 12>
    </mode>
    <mode name="enable" method="cli">                      <!—note 13>
        <error>Failed to get to enable mode. </error>       <!—note 14>
        <require-mode>exec</require-mode>                 <!—note 15>
        <enter>                                           <!—note 16>
            enter_enable.tcl                                 <!—note 17>
        </enter>                                         <!—note 18>
    </mode>
    <function name="delete_file" method="CLI">              <!—note 19>
        <error>An error occurred while trying to delete a file from the device.</error> <!—note 20>
        <enter>                                           <!—note 21>
            delete_file.tcl                                  <!—note 22>
        </enter>                                         <!—note 23>
    </function>
    <function name="save" method="CLI">                    <!—note 24>
        <error>An error occurred while trying to save the configuration.</error> <!—note 25>
        <enter>                                           <!—note 26>
```
Note 1: Common label in fixed format.

Note 2: Specifies the mode name and method (CLI). The common service must have the initialize mode. The label name is mode.

Note 3: Specifies the required mode for the mode. connect indicates the connection mode.

Note 4: enter label, which defines the execution script to enter the mode.

Note 5: Script file, which must be available in the drive folder.

Note 6: The initialize mode has only the enter label, and does not have the exit label.

Note 7: Defines the mode name and method.

Note 8: Error description.

Note 9: Specifies the required mode for the mode.

Note 10: enter label, which defines the execution script to enter the mode.

Note 11: exit label, which defines the execution script to exit the mode.

Note 12: Specifies the function and method. The method is CLI and label is function.

Note 13: enter label and script of the function, which must be available in the drive folder.

Note 14: The function has only the enter label, and does not have the exit label.

For example, you must implement device configuration backup in enable mode, and locate the TCL files used to log in to the enable mode based on the require-mode, including initialize.tcl, enter_exec.tcl, and enter_enable.tcl. Execute these files in sequence for login and execute the exit_enable.tcl and exit_exec.tcl files for logout.

Defining services and actions for a component

Define services in the adapter.xml file. The following illustrates how to define services for Configuration Center. For instructions on defining services for other components, see relevant configuration files of the components.

The services you can define in the adapter.xml file include configuration backup (ConfigBackup), configuration deployment (ConfigDeploy), and software deployment (ImageDeploy). Each service consists of an action definition file xxxxxx_Builder.xml and an action script file xxxxxx_Builder_SCRIPT.xml. You can define multiple actions in the action definition file; each action corresponds to an action on the Configuration Center interface. The action script file provides a specific execution script for every action in the action definition file.

Configuration Center supports the following services and actions (the action name cannot be modified):

- Configuration backup (ConfigBackup)
  - backup_running_config
  - backup_startup_config
- Configuration deployment (ConfigDeploy)
  - deploy_running_config
You must note the following guidelines when you define services for Configuration Center:

- If you have defined the ConfigBackup service in the adapter.xml file, you must define backup_running_config, backup_startup_config, or both. These actions are executed during device configuration backup.
- If you have defined the ConfigDeploy service in the adapter.xml file, you must define deploy_running_config, deploy_startup_config, or both; you must define save_config and reload_device.
  - When you deploy configurations, the deploy_running_config or deploy_startup_config action, based on your configuration, is executed. If no action is defined, the system prompts that deploy_running_config or deploy_startup_config is not supported. During deployment, both the deployment and save actions are executed. To specify the restart action, select Restart device after deployment on the Deploy Strategy page.
- If you have defined the ImageDeploy service in the adapter.xml file, you must define deploy_image, set_device_boot, and delete_image; the actions get_image_position, get_image_version, get_image_size, and get_partition_info are optional.
  - When you deploy device software, deploy_image is executed; to execute set_device_boot and delete_image, make the settings as shown on the following page.
  - Set the Current Running Software as Backup Startup Software and Delete Current Backup Startup Software are not supported. These actions are not executed even if you have selected them.
  - The actions get_image_version and get_partition_info are used during software deployment. The get_partition_info action retrieves partition name and the available space. If these actions are not defined, the system asks you to enter the storage location, and perform software deployment without checking the available space (the default space is sufficient).
  - After deployment, the get_image_size action is executed to check the software size and deployment result. If this action is not defined, the checking is not performed.

**Defining specific services**

**Defining the software deployment service**

1. **xxxxxx_Image_Deploy_Builder.xml** file format:

```xml
<?xml version="1.0"?>
<definition>                                    <!—note 1>
   <action name="deploy_image">                <!—note 2>
```

381
<step>                                           <!—note 3>
  <command name="deploy_image" description="download image via TFTP"/>                            <!—note 4>
</step>
</action>
</action name="set_device_boot">          <!—note 5>
<step>                                               <!—note 6>
  <command name="get_board_number" description="Get board number which current
image is located through CLI">                               <!—note 7>
    <result name="board_number">         <!—note 8>
      <parser parserName="CleanupParser" parserRet="board_number"
parserScript="cleanupBoardNumber"/>                    <!—note 9>
    </result>
  </command>
  <properties>                                               <!—note 10>
    <property name="board" refer="board_number"/> <!—note 11>
  </properties>
  <command name="set_device_boot" description="set OS boot order via CLI"/>
</step>
</action>
</action name="delete_image">            <!—note 12>
<step>                                               <!—note 11>
  <command name="delete_image" description="delete specified image"/>
</step>
</action>                                    <!—note 10>
</definition>

Note 1: Action definition label in fixed format.

Note 2: Action name. All the following software deployment steps are performed based on this name.

Note 3: Step. Each action can have multiple steps, which are executed in turn.

Note 4: Commands required for this step. Define all commands in the xxxxxx_Builder_Script.xml file. Each step can consist of multiple commands, which are executed until one of the commands is executed successfully. For example, if you set to download configuration files through TFTP and display configuration files at the CLI, and the first command is successfully executed, the second command is not executed.

Note 5: Action name, which is used to define the set_device_boot action.

Note 6: Get the board number.

Note 7: Command called to get the board name, which is defined in the xxxxxx_Builder_Script.xml file.

Note 8: Define the result variable board_number, which provides the result after the following parser commands are executed.

Note 9: Call the parser function. parserName specifies the parser service name; parserScript specifies the parser function; parserRet specifies the parser result variable name. You do not need to specify the parameters for the parser function. The system uses all the returned parameters of the command above by default.
Note 10: Properties label. All properties under this label are used as the variables in the TCL script of the following command. To be specific, the TCL script for set_device_boot can use the $board variable, and the variable is defined by the properties label.

Note 11: Define the board variable. You can reference the board_number value obtained in the previous step, or specify a value. For example, property name="board" value="slot1".

Note 12: Delete the software.

2.  xxxx Image_Deploy_Builder_Script.xml file format:

```xml
<?xml version="1.0"?>
<scripts> <!--note 1>

  <command name="deploy_image" method="CLI"> <!--note 2>
    <error>Failed to retrieve image in CLI. Command syntax may be incorrect, or prompts may not be what was expected.</error> <!--note 3>
    <require-mode>exec</require-mode> <!--note 4>
    <script>
      deploy_image.tcl<!--note 5>
    </script>
  </command>

  <command name="set_device_boot" method="CLI"> <!--note 6>
    <error>Failed to set boot order in CLI. Command syntax may be incorrect, or prompts may not be what was expected</error>
    <require-mode>exec</require-mode> <!--note 4>
    <script>
      set_device_boot.tcl<!--note 5>
    </script>
  </command>

  <command name="delete_image" method="CLI"> <!--note 6>
    <require-mode>enable</require-mode> <!--note 4>
    <script>
      delete_image.tcl<!--note 5>
    </script>
  </command>

</scripts>
<?xml version="1.0"?>
```

Note 1: Scripts label in fixed format.
Note 2: Command name and method. The method can be TFTP or CLI.
Note 3: Error description.
Note 4: Required mode.
Note 5: TCL script.
Note 5: set_device_boot action.

**Defining the parser service (CleanupParser)**

CleanupParser consists of parser definition file `xxxxxx_Cleanup_Parser.xml` and parser script file `xxxxxx_Cleanup_Parser_Script.pl`. `xxxxxx` refers to the drive name.
1. **xxxxx_Cleanup_Parser.xml** file format:

```xml
<?xml version="1.0"?>
<parser>
  <perlfile>Cisco_Cleanup_Parser_Script.pl</perlfile>

  <script name="cleanupConfiguration">
    <callfunction name="cleanupConfiguration">
      <parameterspec name="0" type="data_string"/>
      <result type="single">configuration</result>
    </callfunction>
  </script>

  <script name="cleanupTFTPConfiguration">
    <callfunction name="cleanupTFTPConfiguration">
      <parameterspec name="0" type="data_string"/>
      <result type="single">cleanedConfig</result>
    </callfunction>
  </script>
</parser>
```

Note 1: Parser label in fixed format.

Note 2: File that the parser script file belongs to. The label name is perlfile, which cannot be modified.

Note 3: Script name, which is used for calling.

Note 4: Called Perl function name. Perl functions are defined in the Perl file specified by the perlfile label.

Note 5: Enter the parameter name and type. Only the string type, data_string, is supported.

Note 6: Result variable. The parsing result assigns value to the variable, which is used by the caller. Array is not supported, so the type is single.

2. The parser script file **xxxxx_Cleanup_Parser_Script.pl** consists of multiple Perl functions.

```perl
sub cleanupConfiguration
{
  my($config) = @_; 
  my(@array) = ();

  $start = index($config, "!");
  if ($start == -1)
  {
    $start = 0;
  }
  ...
  ##
  # ACNS remove CLI prompts
  $config =~ s/
\S+#
/f/g;

  $cleanConfig = $config;

  return $cleanConfig;
}
```
sub cleanupTFTPConfiguration
{
    my($config) = @_;

    $start = index($config, "!");
    if ($start == -1)
    {
        $start = 0;
    }

    return substr($config, $start);
}

Defining the TCL script and Perl script

The TCL script consists of Expect commands. You do not need to compile the Telnet connection device code because the connection is performed by the Configuration Center background. You only need to compile returned value judgment and login interaction scripts, for example, enter_exec.tcl.

Some variables in the TCL script do not need to be defined. They are provided from the Configuration Center background.

• Common variables
  o ERROR_MESSAGE [OUT] (If the script has an error, you must assign a value to the variable. Configuration Center then judges the execution result based on the variable.)
  o Username [IN] (Telnet user name)
  o Password [IN]
  o enable_password [IN]

• Configuration backup variables
  o TFTPFile [IN] (local file name)
  o TFTPServer [IN]

• Configuration deployment variables
  o TFTPFile [IN](local file name)
  o TFTPServer [IN]
  o Testvalue [OUT] (This variable is used for running configuration deployment. Assign a value, true or false, to it, indicating whether the deployment is completed.)

• Deleting software variables
  o TFTPFile [IN] (device software name)
  o TFTPServer [IN] (TFTP server)
  o transfer_protocol [IN] (protocol)
  o slot [IN] (software location)

• Software upgrade variables
  o TFTPFile [IN] (local file name)
  o DestTFTPFile [IN] (destination file name)
  o TFTPServer [IN]
Variables for setting startup software
- transfer_protocol [IN] (protocol)
- slot [IN] (software storage location)

Variables for obtaining partition information
- partition_name [OUT] (partition name)
- free_size [OUT] (free space)

Variables for obtaining software version
- image_version [OUT] (software version)

Variables for obtaining software location
- image_position [OUT] (software location)

Variables for obtaining software size
- TFTPFile [IN] (software version, obtained by executing the get_image_version command)
- Slot [IN] (software location, obtained by executing the get_image_position command)
- image_size [OUT] (software size)

Use standard Perl script language to compile the Perl script.

---

IMPORTANT:
After you customize the script, restart IMC to validate new functions.

Extending a customized function

IMC supports customizing new functions and can automatically generate entrance pages for the new functions based on the definitions in the Device Configuration Guide or Interface Configuration Guide. To enter the Device Configuration Guide or Interface Configuration Guide, use one of the following ways:

- Select Resource → Batch Operation, and select Device Configuration Guide and Interface Configuration Guide from Device Configuration, or
- Select Resource → Device View. On the device list page, click More and select Device Configuration Guide, or
- In topology view, right-click a device and select Device Configuration Wizard, or
- On the device interface list page, click More and select Interface Configuration Guide, or

To extend the customized function, you must compile the background customized function script in the `<IMC installation directory>\server\conf\adapters\custom` directory. At the same time, create the following files as follows:

- Operation definition file: `<component name>_operations.xml`
- Device capability set definition file: `<component name>_devCapabilities.xml`

This file is issued to define operations supported by the component. See the following description for the file format.
This file is used to define the device capability set supported by the operations of the component. See the following description for the file format.

- **English resource file**: `<component name>.properties`

This file is used to define English resource information used in the `component name_properties` file.

**IMPORTANT:**

After you compile the files and restart IMC, the files are automatically loaded.

The content in the `iMC\server\conf\adapters\GenericConfig` directory can be used as a reference for the background custom script.

The content in the `iMC\client\web\apps\imc\gencfg\register\gencfg` directory can be used as a reference for the UI definition script.

### Defining background custom script

Enter the `iMC\server\conf\adapters\custom` directory (if it is not available, create the directory), and following these steps to compile the background custom script. For more information about the steps, see "Extending an existing function to support third-party devices" (page 375).

1. Create a vendor folder.
2. Create a drive index file and a drive folder.
3. Create drive definition file.
4. Create various services and actions definition file.
5. Create the TCL script and Perl script.

### Registering service operation and compiling operation definition file

The operation definition file is in the XML format. The file name must be `<component name>_operations.xml`. The file defines operations supported by the component. The following is an example:

```xml
#Global resource
str.gencfg.yes=Yes
str.gencfg.no=No

#Create Telnet User
str.create.telnet.user=Create Telnet User
str.telnet.user.name=User Name
str.telnet.user.name.info=Only number, '_' and English character are allowed, start with English character, no longer than 32 characters.
str.telnet.user.password.mode=Password Mode
str.telnet.user.password=Password
str.telnet.user.password.info=No longer than 32 characters.
str.telnet.user.level=User Level
str.telnet.user.service.type=Service Type
```

The following describes properties supported by the elements in the file.

**Operations**

The Operations element is the root node of the operation definition file in Table 5 (page 388).
Table 5 Properties supported by the Operations element

<table>
<thead>
<tr>
<th>Property name</th>
<th>Description</th>
<th>Required</th>
<th>Remarks</th>
</tr>
</thead>
</table>
| devCapability | Device capability set supported by the component | N | - The capability set must be defined in the `<component name>_devCapabilities.xml` file or be ALL (which means supports all devices).  
- It is ALL by default.  
- devCapability="" means not support any device.  
- The values of devCapability can be the capability sets defined in the `<component name>_devCapabilities.xml` file, separated by colons (,).

Example:

```xml
<Operations devCapability="baseDC,dcl">
  <!—-operation definition-->  
</Operations>
```

Variable

The Variable element, shown in Table 6 (page 388) is used to define a variable. The consequent operation definitions can reference the variable in the format `$()$`.

The user-defined variable takes precedence over the system-defined variable.

For more information about replaceable variables, see later sections.

Table 6 Properties supported by the Variable element

<table>
<thead>
<tr>
<th>Property name</th>
<th>Description</th>
<th>Required</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Variable name</td>
<td>Y</td>
<td>The value can contain only letters, digits, underlines (_), and dots (.).</td>
</tr>
<tr>
<td>Value</td>
<td>Variable value</td>
<td>Y</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Example:

```xml
<Variable name="RestServerIP" value="10.153.88.70" />  
```

Operation

Operations can contain multiple operation definitions, each of which defines a service operation in Table 7.

Table 7 Properties supported by the Operation element

<table>
<thead>
<tr>
<th>Property name</th>
<th>Description</th>
<th>Required</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>Operation ID</td>
<td>Y</td>
<td>A character string consisting of letters or digits; unique in a file.</td>
</tr>
</tbody>
</table>
| Label | Operation display name | Y | A resource string starting with %.
<table>
<thead>
<tr>
<th>Property name</th>
<th>Description</th>
<th>Required</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>categoryId</td>
<td>Category ID of the operation</td>
<td>Y</td>
<td>The operation category is defined in the <code>categoryDef.xml</code> file. See the later sections for more information.</td>
</tr>
<tr>
<td>actionId</td>
<td>Primary action ID</td>
<td>Y</td>
<td>Action executed for the operation. The value must have been defined in the operation. Other actions can be called secondary actions.</td>
</tr>
<tr>
<td>actionType</td>
<td>Primary action type</td>
<td>Y</td>
<td>Enumerated value: 1(REST) or 2(ASN1).</td>
</tr>
<tr>
<td>operLevel</td>
<td>Operation level</td>
<td>N</td>
<td>Indicates whether the operation is port level or device level. It is an enumerated value: 1(DIVICE) or 2(PORT). The default value is 1—device level.</td>
</tr>
<tr>
<td>devCapability</td>
<td>Device capability set</td>
<td>N</td>
<td>Indicates the device capability set supported by the operation. The capability set must be defined in the <code>&lt;component name&gt;_devCapabilities.xml</code> file. The default is the device capability set defined by the Operations element (rather than ALL).</td>
</tr>
</tbody>
</table>

The operations with the same name in different registration files are considered one operation. The following information for the operations must be consistent:

- Operation ID (id)
- Category ID of the operation (categoryId)
- Operation display name (label)
- Operation level (operLevel)
- For parameters of the actions (primary and secondary actions) of the operation, the values, numbers, sequence (compiling sequence), and property values (unique for each property) must be the same.

For the operations with the same name in different registration files, the following items are typically different.

- Capability set (devCapability) (If the capabilities are the same, the defined operations are meaningless.)
- Primary action name (actionName).
- Primary action type (actionType).
- Action (primary and secondary) properties, excluding the parameter information.

⚠️ **WARNING!**

If the operations with the same name do not satisfy the requirement of information consistency, the system discards the loaded operations and logs the event.

**Example:**
```xml
<Operation id="addXXXX" category="%str.category1" label="%str.addXXXX"
actionName="addXXXXAction" actionType="1" operLevel="1" devCapability="dc1">
  <!--action and parameter definition-->
</Operations>
```
RestAction and Asn1Action

The operation definitions include operation parameter definition and action definition. Although an operation requires one action, the operation parameter initialization typically requires additional actions, so you can define multiple actions. Only the action corresponding to actionName is executed for the operation. The system dynamically generates input interface only for this action.

Common configurations support two types of actions: REST action and ASN1 action. The REST action is executed in the REST mode; the ASN1 action is executed in the ASN1 and background communication modes, listed in Table 8.

Table 8 Properties supported by the RestAction element

<table>
<thead>
<tr>
<th>Property name</th>
<th>Description</th>
<th>Required</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Id</td>
<td>Action ID</td>
<td>Y</td>
<td>A character string consisting of letters or digits; unique in an operation.</td>
</tr>
<tr>
<td>protocol</td>
<td>Protocol</td>
<td>Y</td>
<td>HTTP or HTTPS.</td>
</tr>
<tr>
<td>ip</td>
<td>IP address</td>
<td>Y</td>
<td>Supports replaceable variable, for example, ${IMC_SERVER_IP}.</td>
</tr>
<tr>
<td>port</td>
<td>Port number</td>
<td>Y</td>
<td>Supports replaceable variable, for example, ${IMC_HTTP_PORT} or ${IMC_HTTPS_PORT}.</td>
</tr>
<tr>
<td>uri</td>
<td>URI used by the REST operation</td>
<td>Y</td>
<td>For example, /imcrs/vlan?devId=33.</td>
</tr>
<tr>
<td>userName</td>
<td>Authentication username</td>
<td>Y</td>
<td>Supports replaceable variable, for example, ${IMC_USER_NAME}.</td>
</tr>
<tr>
<td>userPassword</td>
<td>Authentication password</td>
<td>Y</td>
<td>Supports replaceable variable, for example, ${IMC_USER_PWD}.</td>
</tr>
<tr>
<td>method</td>
<td>Method used by the REST operation</td>
<td>Y</td>
<td>Enumerated value: 1(GET), 2(POST), 3.PUT), or 4(DELETE).</td>
</tr>
<tr>
<td>bufferSize</td>
<td>Buffer size</td>
<td>N</td>
<td>The default is 8192 bytes.</td>
</tr>
<tr>
<td>Timeout</td>
<td>Timeout time (in milliseconds)</td>
<td>N</td>
<td>The default is 5000 milliseconds.</td>
</tr>
<tr>
<td>Property name</td>
<td>Description</td>
<td>Required</td>
<td>Remarks</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------</td>
<td>----------</td>
<td>---------</td>
</tr>
<tr>
<td>class</td>
<td>Entity class used by the REST operation</td>
<td>N</td>
<td></td>
</tr>
</tbody>
</table>

- If the REST method is POST or PUT, this parameter is typically required. When the parameter is provided, the instantiation of an entity object is done, and an XML file is generated and sent to the REST server. At this time, the entityProperty and dataType properties must be specified for each Parameter element.

- If the REST method is GET or DELETE, this parameter is typically not required. When the parameter is not provided, the system sends the parameter value input by the user as the URL parameter to the REST server. At this time, the system ignores the entityProperty and dataType properties of the Parameter elements.

Example 1: use static URL values

```xml
<RestAction id="getXXXXAction" protocol="http" ip="10.153.88.70" port="8080" uri="/imcrs/XXXX" userName="${IMC_USER_NAME}" userPassword="${IMC_USER_PWD}" method="1">
  <Parameter name="devId" value="${DEVICE_ID}"/>
</RestAction>
```

Example 2: use replaceable URL variables

```xml
<RestAction id="getXXXXAction" protocol="http" ip="${RestServerIP}" port="${RestServerPort}" uri="/imcrs/XXXX" userName="${IMC_USER_NAME}" userPassword="${IMC_USER_PWD}" method="1">
  <Parameter name="devId" value="${DEVICE_ID}"/>
</RestAction>
```

Example 3: send REST request by using the entity class

```xml
<RestAction id="addXXXXAction" protocol="http" ip="${RestServerIP}" port="${RestServerPort}" uri="/imcrs/XXXX" userName="${IMC_USER_NAME}" userPassword="${IMC_USER_PWD}" method="2" class="com.h3c.imc.XXXEntity">
  <Parameter name="devId" value="${DEVICE_ID}" entityProperty="id" dataType="java.math.BigInteger"/>
</RestAction>
```

Example 4: send REST request by using the URL parameter

```xml
<RestAction id="getXXXXAction" protocol="http" ip="${RestServerIP}" port="${RestServerPort}" uri="/imcrs/XXXX" userName="${IMC_USER_NAME}" userPassword="${IMC_USER_PWD}" method="1">
  <Parameter name="devId" value="${DEVICE_ID}"/>
</RestAction>
```
Table 9 Properties supported by the Asn1Action element

<table>
<thead>
<tr>
<th>Property name</th>
<th>Description</th>
<th>Required</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>Action ID</td>
<td>Y</td>
<td>A character string consisting of letters or digits; unique in an operation; consistent with the actionName in the background script.</td>
</tr>
<tr>
<td>serviceName</td>
<td>Service name</td>
<td>Y</td>
<td>It must be consistent with the serviceName field in the background script.</td>
</tr>
<tr>
<td>actionName</td>
<td>Action name</td>
<td>Y</td>
<td>It must be consistent with the actionName field in the background script.</td>
</tr>
<tr>
<td>operType</td>
<td>Operation type</td>
<td>Y</td>
<td>Enumerated value: 1 (deploy configuration) or 2 (get configuration)</td>
</tr>
<tr>
<td>operMode</td>
<td>Operation mode</td>
<td>N</td>
<td>Enumerated value: 0 (any), 1 (SNMP), or 2 (CLI). The default is 0.</td>
</tr>
<tr>
<td>transProtocol</td>
<td>Transmission protocol</td>
<td>N</td>
<td>Enumerated value: 0 (any), 1 (TFTP), 2 (FTP), or 3 (SFTP). The default is 0.</td>
</tr>
<tr>
<td>execMode</td>
<td>Execution mode</td>
<td>N</td>
<td>Enumerated value: 1 (synchronous) or 2 (asynchronous). The default is 1.</td>
</tr>
<tr>
<td>timeout</td>
<td>Timeout time (in seconds)</td>
<td>N</td>
<td>The default is 300 seconds.</td>
</tr>
</tbody>
</table>

Example 5:

```xml
<Asn1Action id="getXXXXAction" serviceName="getXXXX" actionName="getXXXX" operType="2" timeout="300">
  <Parameter name="devId" value="$(DEVICE_ID)"/>
  <Parameter name="vlanId" value="1"/>
</Asn1Action>
```

Parameter

The Parameter element, shown in Table 10 (page 392) is used to define parameters for operations. Each parameter can define its own view, and whether to perform initialization, and if yes, how to perform initialization. For the view and initialization description, see later sections.

The common configuration framework generates the dynamic interface for only the primary action (identified by the actionName property of the Operation element). The sequence of parameters on the interface is consistent with that defined in the registration file.

Table 10 Properties supported by the Parameter element

<table>
<thead>
<tr>
<th>Property name</th>
<th>Description</th>
<th>Required</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Parameter name</td>
<td>Y</td>
<td>A character string consisting of letters or digits; unique in an action.</td>
</tr>
<tr>
<td>value</td>
<td>Parameter value</td>
<td>N</td>
<td>Supports replaceable variable. The system does not generate dynamic interface for the parameter whose variable is replaced.</td>
</tr>
<tr>
<td>Property name</td>
<td>Description</td>
<td>Required</td>
<td>Remarks</td>
</tr>
<tr>
<td>---------------</td>
<td>------------------------------------</td>
<td>----------</td>
<td>---------</td>
</tr>
<tr>
<td>label</td>
<td>Parameter display name</td>
<td>N</td>
<td>A resource string starting with %. If it is null, the name value is displayed.</td>
</tr>
<tr>
<td>required</td>
<td>Required or not</td>
<td>N</td>
<td>The value can be true or false. The default is true (required).</td>
</tr>
<tr>
<td>entityProperty</td>
<td>Entity class property of the parameter</td>
<td>N</td>
<td>Required when the class property of RestAction is not null. The system calls the setter of the property to assign a value to it.</td>
</tr>
<tr>
<td>dataType</td>
<td>Entity property data type of the parameter</td>
<td>N</td>
<td>Required when the class property of RestAction is not null. The following data types are supported (package name is contained in the type name):</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Basic data type:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• boolean</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• byte</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• double</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• float</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• int</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• long</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• short</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• char</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Boolean type:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• java.lang.Boolean</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>String type:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• java.lang.String</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Number type:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• java.lang.Byte</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• java.lang.Double</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• java.lang.Float</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• java.lang.Integer</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• java.lang.Long</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• java.lang.Short</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• java.math.BigInteger</td>
</tr>
<tr>
<td>validateRegEx</td>
<td>Validation with regular expression</td>
<td>N</td>
<td>Regular expression used for validation. If it is null, no validation is performed.</td>
</tr>
<tr>
<td>defaultValue</td>
<td>Default value</td>
<td>N</td>
<td>It is null by default.</td>
</tr>
<tr>
<td>info</td>
<td>Prompt information</td>
<td>N</td>
<td>Tooltip help information behind the input box. It is a resource string starting with %. Prompt information display is supported by only text boxes, combo boxes, and calendar control.</td>
</tr>
</tbody>
</table>

Example 1: a parameter, which has its view defined as SelectManyCheckbox, and has static initialization performed.

```xml
<Parameter name="param8" label="%str.param8"/>```
Parameter view control

The common configuration framework supports the following views: text box (InputText), check box (Checkbox), check box group (SelectManyCheckbox), calendar control (PopupCalendar), drop-down list (SelectOneMenu), and combo box (CompositeInputText).

- Text box (InputText)

The text box, shown in Figure 34, is used to control text input shown in Table 11.

**Figure 34 Text box view**

<table>
<thead>
<tr>
<th>Property name</th>
<th>Description</th>
<th>Required</th>
<th>Remarks</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>editable</td>
<td>Whether editing is allowed</td>
<td>N</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Example 1:

```
<View type="InputText"/>
```
Example 2: if no view is defined, the text box InputText is used by default.

```xml
<Parameter name="param6" label="%str. param6"/>
```

- Check box

The check box indicates the enabled or disabled state of a parameter.

If the check box, shown in Figure 35, is selected, the parameter value is true; if not, the parameter value is false.

**Figure 35 Check box view**

![Check box view](image)

Example:

```xml
<View type="Checkbox"/>
```

- Check box group (SelectManyCheckbox)

A check box group, shown in Figure 36, provides you multiple check boxes for selection.

**Figure 36 Check box group view**

- Add VLAN
- Delete VLAN
- Modify VLAN Name

### Table 12 Properties of the checkboxes

<table>
<thead>
<tr>
<th>Property name</th>
<th>Description</th>
<th>Required</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>layout</td>
<td>Layout</td>
<td>N</td>
<td>Enumerated value: 1 (horizontal) or 2 (vertical). The default is 1.</td>
</tr>
</tbody>
</table>

Example:

```xml
<View type="SelectManyCheckbox" layout="2">
  <SelectItem value="1" displayValue="Fragmentation"/>
  <SelectItem value="2" displayValue="Logging"/>
  <SelectItem value="3" displayValue="All Source Hosts"/>
</View>
```

If you select multiple check boxes, as shown on the page above, the parameter takes the string of the values (separated by " ", ") of the selected items, for example 2, 3.

- Calendar control (PopupCalendar)

The calendar control, shown in Figure 37 (page 396), has the following functions, listed in Table 13 (page 396):

- Lets you enter date or time in the date input box.
- Provides date format prompt information.
- Lets you change information in the input box by selecting the date and time on the calendar that appears when you click the icon behind the input box.
- Provides help information when you click the question mark on the top left corner of the calendar.
- Lets you flexibly set the view style of the calendar through the style list file.
Automatically changes the language setting based on the specified system environment.

Figure 37 Calendar control view

Table 13 Properties supported by the calendar control

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Required</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>dateformat</td>
<td>Time display format</td>
<td>N</td>
<td>The default format is: YYYY-MM-DD HH:MM</td>
</tr>
<tr>
<td>showtime</td>
<td>Whether to display time</td>
<td>N</td>
<td>The value can be true or false. The default is true.</td>
</tr>
</tbody>
</table>

Example:

```xml
<View type="PopupCalendar" dateformat="yyyy-MM-dd HH:mm" showtime="true"/>
```

Drop-down list (SelectOneMenu)

The drop-down list, shown in Figure 38, provides options from which you select one.

Figure 38 Drop-down list view

Example 1: static initialization

```xml
<View type="SelectOneMenu">
  <SelectItem value="1" displayValue="Alert"/>
  <SelectItem value="2" displayValue="%str.alarm.info"/>
  <SelectItem value="3" displayValue="Critical"/>
  <SelectItem value="4" displayValue="Information"/>
</View>
```

Example 2: dynamic initialization

```xml
<View type="SelectOneMenu">
  <Init refAction="getXXXXAction" destValueProperty="XXXXId" destDisplayProperty="XXXXName" type="1"/>
</View>
```
NOTE:

This control supports only initialization.

- Combo box, shown in Figure 39, (CompositeInputText)

**Figure 39 Enter text information in the combo box. Combo box view**

<table>
<thead>
<tr>
<th>Email</th>
<th>Add</th>
<th>Delete</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:tester4@gmail.com">tester4@gmail.com</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td><a href="mailto:tester1@gmail.com">tester1@gmail.com</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td><a href="mailto:tester2@gmail.com">tester2@gmail.com</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td><a href="mailto:tester3@gmail.com">tester3@gmail.com</a></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Example 1: static initialization**

```xml
<View type="CompositeInputText">
  <SelectItem value=" tester1@gmail.com"/>
  <SelectItem value=" tester2@gmail.com"/>
  <SelectItem value=" tester3@gmail.com"/>
</View>
```

**Example 2: dynamic initialization**

```xml
<View type="CompositeInputText">
  <Init refAction="getXXXXAction" destValueProperty="XXXXId" destDisplayProperty="XXXXName" type="1"/>
</View>
```

NOTE:

- This control supports only initialization.
- Do not enter colons (,) in the parameter.
- If you enter multiple values, as shown on the page above, the parameter takes the string of the values (separated by ",") of the entered items, for example, tester1@gmail.com, tester2@gmail.com, tester3@gmail.com.
- The displayValue property and value property of the SelectItem of the control are consistent, so only the value property is used.

**Control initialization**

The drop-down list (SelectOneMenu) and combo box (CompositeInputText) support initialization. Initialization includes static initialization, dynamic initialization, and mixed initialization. Static initialization uses static values for initialization, and uses the SelectItem element; dynamic initialization dynamically obtains data from the device for initialization, and uses the Init element; mixed initialization allows for both static and dynamic initialization, and takes the result from the union of the static and dynamic initialization results. See Table 14 (page 398).
The service component can use SelectItem to perform static initialization for the drop-down list (SelectOneMenu) and combo box (CompositeInputText) controls.

Table 14 Properties supported by SelectItem

<table>
<thead>
<tr>
<th>Property name</th>
<th>Description</th>
<th>Required</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>value</td>
<td>Item value</td>
<td>Y</td>
<td>The parameter takes the property value.</td>
</tr>
<tr>
<td>displayValue</td>
<td>Item display value</td>
<td>N</td>
<td>This property is used for display. If it is not available, the value property is displayed.</td>
</tr>
</tbody>
</table>

Example 1: drop-down list static initialization

```xml
<View type="SelectOneMenu">
  <SelectItem value="1" displayValue="Alert"/>
  <SelectItem value="2" displayValue="%str.alarm.info"/>
  <SelectItem value="3" displayValue="Critical"/>
  <SelectItem value="4" displayValue="Information"/>
</View>
```

Example 2: combo box static initialization

```xml
<View type="CompositeInputText">
  <SelectItem value=" tester1@gmail.com"/>
  <SelectItem value=" tester2@gmail.com"/>
  <SelectItem value=" tester3@gmail.com"/>
</View>
```

NOTE:
If the displayValue property and value property of the SelectItem of the combo box control are consistent, the value property is used.

- **Init**

The Init element can dynamically get data from the device to perform initialization for the drop-down list (SelectOneMenu) and combo box (CompositeInputText) controls. The following is the working process:

  o Enter parameters required by the refAction.

The control initialization action is executed after the dynamic page is generated. You do not need to enter parameters for such actions, so control initialization action parameters can only be dynamic information, such as the selected port or device.

The common configuration framework provides a group of replaceable variables related to the IMC system, device, and interface for the components. When you enter the parameters required by the refAction, if replaceable variables (with the format `$\{ DEVICE_ID \}` that starts with `$` and ends with `.`) are found in the registration file, the system automatically replaces it with the parameter related to IMC system, device, or interface. For example, the system replaces `$\{DEVICE_ID\}` with the device ID. For more information about replaceable variables supported by the common configuration framework, see later sections.

  o The system executes the refAction action.
  o Parse the execution result of the action.
When parsing the execution result of the action, the common configuration framework takes the destValueProperty value as the value property value of SelectItem, the destDisplayProperty value as the display property value of SelectItem.

If you have selected multiple devices or ports, the system executes the refAction action on all selected devices or ports to generate multiple result values. The policy to process these result values is defined by the type property. Type 1 means to take the intersection of multiple result values; type 2 means to take the union of multiple result values. See Table 15.

- Initialize the control based on the result.

### Table 15 Properties supported by Init

<table>
<thead>
<tr>
<th>Property name</th>
<th>Description</th>
<th>Required</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>refAction</td>
<td>Action for initialization</td>
<td>Y</td>
<td>The action must have been defined in the operation.</td>
</tr>
<tr>
<td>destValueProperty</td>
<td>Name of the SelectItem Value property</td>
<td>Y</td>
<td>For RestAction, the system gets an XML file. This property specifies the XML property of &quot;value&quot;. If the XML file consists of multiple elements, and each element has the property defined by destValueProperty, the property of the first element is taken. For Asn1Action, the system receives an ASN1 response message. This property specifies the property name of the SelectItem &quot;value&quot;.</td>
</tr>
<tr>
<td>destDisplayProperty</td>
<td>Name of the SelectItem displayValue property</td>
<td>Y</td>
<td>For RestAction, the system gets an XML file. This property specifies the XML property of &quot;displayValue&quot;. If the XML file consists of multiple elements, and each element has the property defined by destDisplayProperty, the property of the first element is taken. For Asn1Action, the system receives an ASN1 response message. This property specifies the property name of &quot;displayValue&quot;.</td>
</tr>
<tr>
<td>type</td>
<td>Processing method</td>
<td>N</td>
<td>Enumerated value: 1 (takes intersection of result sets) or 2 (takes union of result sets). The default is 1.</td>
</tr>
</tbody>
</table>

Example 1: drop-down list dynamic initialization

```xml
<View type="SelectOneMenu">
  <Init refAction="getVlanAction" destValueProperty="XXXXId" destDisplayProperty="XXXXName" type="1"/>
</View>
```

Example 2: combo box dynamic initialization

```xml
<View type="CompositeInputText">
  <Init refAction="getVlanAction" destValueProperty="XXXXId" destDisplayProperty="XXXXName" type="1"/>
</View>
```

If the initialization action is of the REST type, destValueProperty and destDisplayProperty require the XPath expression, as shown in example 3.

The displayValue property and value property of the combo box control are consistent, so the system uses the destValueProperty value for initialization.
Example 3: To use the device VLAN information to initialize the drop-down list by using the vlanName value as the displayValue value and the vlanId value as the value value of the component, compile the following information:

```xml
<View type="SelectOneMenu">
  <Init refAction="getVlanAction" destValueProperty="/vlan/@vlanId" destDisplayProperty="/vlan/@vlanName" type="1"/>
</View>
```

Following is the response message body for querying device VLANs.

```xml
<list>
  <vlan vlanStatus="1" vlanName="VLAN 0001" vlanId="1" />
  <vlan vlanStatus="1" vlanName="VLAN 0002" vlanId="2" />
  <vlan vlanStatus="1" vlanName="VLAN 0003" vlanId="3" />
  <vlan vlanStatus="1" vlanName="VLAN 0004" vlanId="4" />
  <vlan vlanStatus="1" vlanName="VLAN 0005" vlanId="5" />
</list>
```

• Mixed initialization

Mixed initialization allows for both static and dynamic initialization, and takes the result from the union of the static and dynamic initialization results.

Example 1: drop-down list mixed initialization

```xml
<View type="SelectOneMenu">
  <SelectItem value=" " displayValue=" "/>
  <Init refAction="getVlanAction" destValueProperty="XXXXId" destDisplayProperty="XXXXName" type="1"/>
</View>
```

Example 2: combo box mixed initialization

```xml
<View type="CompositeInputText">
  <SelectItem value=" " displayValue=" "/>
  <Init refAction="getVlanAction" destValueProperty="XXXXId" destDisplayProperty="XXXXName" type="1"/>
</View>
```

**Compiling device capability set definition file**

The device capability set definition file is an XML file, whose name must be `component name_devCapabilities.xml`. This file defines the device capability set supported by the operations of the component. The following is an example:

```xml
<?xml version="1.0" encoding="UTF-8"?>
<DevCapabilities>
  <Capability name="gencfgDC">
    <SysOID>1.3.6.1.4.1.25506</SysOID>
    <SysOID>1.3.6.1.4.1.2011</SysOID>
  </Capability>
</DevCapabilities>
```

The properties supported by the elements in the file are described as follows:

• **DevCapabilities element**
The DevCapabilities element is the root node of the operation definition file, and does not support any property.

- Capability element, shown in Table 16.

### Table 16 Properties supported by the Capability element

<table>
<thead>
<tr>
<th>Property name</th>
<th>Description</th>
<th>Required</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Name</td>
<td>Y</td>
<td>All is reserved, meaning all devices. The name must be unique in a file.</td>
</tr>
</tbody>
</table>

**SysOID element**

The content of the sysOID element is the device sysOID. sysOID can be a complete sysOID meaning a specific device model, or part of a sysOID meaning a device series.

Example: specify the capability set to support all 3Com devices and a specific Cisco device.

```
<Capability name="baseDC">
    -- support all 3Com devices-->
    <SysOID>1.3.6.1.4.1.43</SysOID>
</Capability>
```

**Replaceable variable list**

Replaceable variables are used to replace the specified property values in the registration file. For example, to replace the value property value of the Parameter element or uri property value of the RestAction element. The replaceable variable is in the format of ${VARIABLE_NAME}, and must start with $ { and end with }.

The replaceable variables include three categories: user-defined replaceable variables, system-level replaceable variables, and parameter-level replaceable variables. In certain cases, you must enter some properties or names multiple times. To address this issue, the system allows for user-defined replaceable variables in registration files; pre-defines some commonly used replaceable variables for you as shown in the table below; and lets you reference a parameter in the (parameter name) format, which is called a parameter-level replaceable variable. For the property of an action, only the parameters of the action are allowed to be used.

The system replaces the user-defined replaceable variables when loading the registration file, replaces system-level replaceable variables when executing actions, and then replaces the parameter-level replaceable variables. In the following example, ${vlanId} is a parameter-level replaceable variable.

```
<RestAction id="addPort2VlanAction" protocol="http" ip="${IMC_SERVER_IP}" port="${IMC_HTTP_PORT}" uri="/imcrs/vlan/${vlanId}" userName="${IMC_USER_NAME}" userPassword="${IMC_USER_PWD}" method="2">
    <Parameter name="devId" value="${DEVICE_ID}" />
    <Parameter name="vlanId" label="%str.vlanId" required="true" validateRegEx="[2-9]|1-3|0-9\{2,3\}|4\{0-8\}|9\{0-4\}" info="%str.vlan.id.info" />
    <Parameter name="ifIndex" value="${IF_INDEX}" />
</RestAction>
```

When dynamically generating a page, the system does not generate the view for parameters using replaceable variables in the value property. The system dynamically assigns a value to the parameter based...
on the replaceable variable when executing actions for the operation and you do not need to enter a value. Replaceable variables can also be used in the control initialization process.

The control initialization action is executed after the dynamic page is generated. Such actions do not require manual input of parameters. The control initialization action parameters can only be the dynamic information, such as the selected port or device. At this time, the service component requires using replaceable variables. When the system performs control initialization, it replaces the replaceable variables with the corresponding device or port information, shown in Table 17.

Table 17 System-level replaceable variable supported by the common configuration framework

<table>
<thead>
<tr>
<th>Category</th>
<th>Parameter name</th>
<th>Parameter description</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>System-level</td>
<td>IMC_SERVER_IP</td>
<td>IMC primary server IP address</td>
<td></td>
</tr>
<tr>
<td>variables</td>
<td>IMC_HTTP_PORT</td>
<td>IMC HTTP port number</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IMCHTTPS_PORT</td>
<td>IMC HTTPS port number</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IMC_USER_NAME</td>
<td>Current IMC user name</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IMC_USER_PWD</td>
<td>Current IMC user password</td>
<td></td>
</tr>
<tr>
<td>Device-level</td>
<td>DEVICE_ID</td>
<td>Device ID</td>
<td>Same as the returned value of getDeviceID()</td>
</tr>
<tr>
<td>variables</td>
<td></td>
<td></td>
<td>for SymbolInfo.</td>
</tr>
<tr>
<td></td>
<td>SYMBOL_ID</td>
<td>Symbol ID</td>
<td>Same as the returned value of getSymbolID()</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>for SymbolInfo.</td>
</tr>
<tr>
<td></td>
<td>DEVICE_IP</td>
<td>Device IP address</td>
<td>Same as the returned value of getIpAddress()</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>for SymbolInfo.</td>
</tr>
<tr>
<td></td>
<td>DEVICE_SYSOID</td>
<td>Device sysOID</td>
<td>Same as the returned value of getSysOID()</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>for SymbolInfo.</td>
</tr>
<tr>
<td>Interface-level</td>
<td>IF_INDEX</td>
<td>Interface index</td>
<td>Same as the returned value of getId().getIfIndex()</td>
</tr>
<tr>
<td>variables</td>
<td></td>
<td></td>
<td>for IfInfo.</td>
</tr>
<tr>
<td></td>
<td>IF_DESC</td>
<td>Interface description</td>
<td>Same as the returned value of getDesc()</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>for IfInfo.</td>
</tr>
<tr>
<td></td>
<td>IF_TYPE</td>
<td>Interface type</td>
<td>Same as the returned value of getType()</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>for IfInfo.</td>
</tr>
<tr>
<td></td>
<td>IF_IP</td>
<td>Interface IP address</td>
<td>Same as the returned value of getIfIp()</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>for IfInfo.</td>
</tr>
</tbody>
</table>
7 Configuration and change management

The **Configuration Center** service module provides change management features for managing the configuration of and changes to network resources.

The **Configuration Center** option of the **Configuration Center** service module serves as a portal for managing the configuration of one or more devices. Through this portal, you can view, backup, baseline, compare, check, and deploy startup and running configuration files. In addition, you can view and restore configuration file histories to selected devices.

From the **Configuration Center** option, you can also view, export, deploy, and restore system software and view software update histories for the selected devices. And, you can manage device space usage by removing unwanted files to make space for new software deployments.

**Configuration templates**

By using the **Configuration Templates** feature, you can create templates based on entire startup or running configuration files. Or, you can modularize the management of configurations by creating templates based on portions of configuration files called segments. You can import the contents of a template from the backup of a configuration file, thus simplifying the process of template creation.

You can also create configuration templates from scratch or they can import the contents of configuration templates. In addition, you can organize templates into nested folders for easy access to templates. Once created, deploy them to selected devices by using the **Deployment Guide**.

**Software library**

With the **Configuration Center**’s **Software Library**, you have several methods for building a software library. You can backup system or other software to IMC. Or, you can import the software from a file stored on your local computer. Once a file is imported, IMC determines to which devices the associated software can be deployed. In addition, you have the ability to designate software library entries as baselines. Lastly, you can export software from IMC. Once software has been imported into IMC, it then becomes available for deployment by using the **Deployment Guide**.

With the **Deployment Guide**, you have a step-by-step wizard for deploying configuration templates and software from the **Software Library**. In addition, the **Deployment Guide** provides you with a facility for restoring device configurations and software. When deploying configuration files, IMC evaluates the configuration template against every device selected for deployment to ensure that the template can be deployed. IMC identifies when devices do not match the configuration template.

With software deployments, IMC performs two checks. The first check evaluates whether or not the system software matches the devices current system software and identifies whether or not the software should be deployed to the device. IMC also performs a second check to verify that there is enough device space to deploy the selected software by using the deployment strategy that you have configured. You can run deployments immediately or to schedule them for a later date. For configuration deployments, you can configure recurring or periodic deployments.

While the **Deployment Guide** serves as an input queue for submitting deployment tasks to IMC, the **Deployment Task** feature of the **Configuration Center** serves the output queue. From the **Deployment Task** link, you can view, run, suspend, resume, or delete deployment tasks that have been submitted to IMC. In addition,
you can view the execution results for every job and view the step-by-step details of the configuration or software deployment. Additionally, you can view the changes that were made during the deployment.

**Configuration compare**

With the **Configuration Compare** option, you can select and view configuration files side-by-side. You can select a current startup or running configuration file and compare it against another file from the same device or another device. In addition, you can compare device startup or running configuration files that have been backed up to IMC. IMC presents both files side-by-side with the option to view the entirety of both files or the differences only. You can also step through the files and highlight every difference by using the **Next Diff** button.

**Configuration audit and reports**

With the **Configuration Audit** option, you can audit the configuration and software versions for network resources.

From the **Configuration Backup Report**, you can view, export, and restore the backup files for both startup and running configuration files for all devices managed in IMC.

With the **Configuration Baseline Report** feature, you can view the results of IMC’s evaluation of the last backup configuration file against the configured baseline file to determine if any changes have been made. In addition, you can launch the configuration compare option from the **Configuration Baseline Report** to compare the last backup configuration file against the configured baseline file.

**Software update**

With the **Software Update** feature, you can view a history of all software updates performed in IMC with the ability to launch a software restoration from the **Software Update Report**. With the **Software Baseline Report**, you can view both current and baseline software file information. In addition, IMC performs a baseline comparison to verify whether or not the baseline software running on a device is identical to the current version.

**Auto backup plan**

By using the **Auto Backup Plan**, you can schedule automated backups of configuration files for one or more devices. By using IMC’s **Backup History Report** you have visibility into the backup results for all backup tasks, including backups initiated manually and backups initiated through an auto backup plan.

**Configuration check**

The **Compliance Check** feature lets you check the configurations of devices. First, create a compliance policy and add rules in the policy. Then, create a check task, associate the compliance policy and devices to be checked with the check task, and schedule the check task to complete compliance check.

You can also specify display commands to be issued on the selected devices. IMC checks the compliancy of the display command output by using the policy rules.
Using the Configuration Center

The Configuration Center link within the Configuration Center service module provides you with a portal for managing the configurations of one or more devices. Through the Configuration Center portal, you can view the latest running and startup configuration files for managed devices in IMC. From this list, you can initiate a manual backup of the startup and running configurations of the selected devices, define a configuration baseline, set schedules for automatic backups of configuration files and deploy configuration files to the selected devices.

You can also view histories of startup and running configuration backup files for the selected device and modify, restore, compare, establish a baseline or save configuration files.

With the configuration baseline facility, you can define a startup and running configuration version as a baseline and with auditing features, identify when a device does not conform to its configuration baseline.

From the same portal, you can manage the software for managed devices. This includes viewing the software update history for the selected device. In addition, you can deploy software from IMC’s software library to selected devices from the Configuration Center portal. With the software baseline facility, you can define a software version as a baseline and with auditing features, identify when a device does not conform to its software baseline.

The Configuration Center portal also provides a convenient facility for comparing the contents of configuration files. You can compare backup startup or running configuration files with the current startup or running configuration files. IMC also provides a line-by-line comparison of the two files with changes highlighted. In addition, IMC provides a summary of identical, changes, and unique lines.

From IMC, you can remove system software, configuration files and other file types from devices by using the Clean Device Space option. IMC displays the contents of a device’s memory and with a few clicks can remove any unwanted files.

Accessing the Configuration Center

To access the Configuration Center:

1. Navigate to Service → Configuration Center.
2. Click the Service tab from the tabular navigation system on the top.
3. Do one of the following:
   - Click the Configuration Center icon located under the Resource and Configuration Management section of the Service page, or
   - Click the Configuration Center link located on the left navigation tree.

All devices that can be managed by the Configuration Center are displayed in the list in the bottom half of the Configuration Center page.

Configuration center device list

- **Device Name**: Contains the IMC name for the device, which, by default, is the name assigned to it by IMC in its device configuration. If a device is configured with a sysName, the sysName is used as the Device Label unless the Device Label is manually configured. This field also contains the IP address. The contents of the device label field serve as an active link for drilling down into the Device Details page.
- **Device Model**: Contains the device model information for the associated device. This information is the same as the Device Model information found on the Device Details page. IMC can
automatically identify H3C, 3Com, HP, Huawei, and Cisco devices. Device model information for all other devices can be configured by using the **Device Model** feature found under the **System** tab.

- **Current Version**: Contains the operating system version that is currently running on the associated device.
- **Latest Available Version**: Contains the most current version stored in IMC’s software library. A "-" in this field indicates that a newer version of the software exists but has not been added to the software library.
- **Last Backup Time**: Contains a date and time stamp for the most recent backup of the associated device’s running and startup configuration files.
- **Operation**: Contains an icon that displays links to operational tasks for the associated file, segment, or folder.

From the **Operation** popup menu, you can view the latest startup and running configuration, navigate to the configuration management page for the associated device, clean device space on the associated device, set a software baseline, or compare the device configuration with another device.

You can sort the **Configuration Center** device list by every field except the **Operation** field. Click the column label to sort the list by the selected field. The column label is a toggle switch that lets you toggle between the various sort options specific to each field.

If the **Configuration Center** device list contains enough entries, the following navigational aids are displayed.

- Click **Page Forward** to page forward in the **Configuration Center** device list.
- Click **Page Forward to The End** to page forward to the end of the **Configuration Center** device list.
- Click **Page Backward** to page backward in the **Configuration Center** device list.
- Click **Page Forward to The Front** to page backward to the front of the **Configuration Center** device list.

4. Click 8, 15, 50, 100, or 200 from the right side of the main pane to configure how many items per page you want to view.

---

**Querying for devices in the Configuration Center**

You can search for a particular device and its associated configuration information from the **Configuration Center**. You can search either by a partial or complete device name. IMC then displays only those devices that match the search criteria. Alternatively, you can filter the list by Custom View.

To filter the **Configuration Center** device list:

1. Navigate to **Service** → **Configuration Center**.
2. Click the **Service** tab from the tabular navigation system on the top.
3. Do one of the following:
   - Click the **Configuration Center** icon located under the **Resource and Configuration Management** section of the **Service** page, or
   - Click the **Configuration Center** link located on the left navigation tree.

The search conditions display in the **Query Condition** section of the **Configuration Center** page.

4. Enter one or more of the following search criteria in the **Query Condition** section of the page:
   - **Device Name**: Enter a partial or complete device label or name in the **Device Name** field.
   - **Custom View**: Select the custom view you want to search or filter the list by. You can also choose the blank option, which searches all custom views.
Device configuration options in the Configuration Center

The Operation link associated with an individual device in the Configuration Center device list provides you with access to a variety of configuration management tasks.

Viewing the latest startup configuration

To view the latest startup configuration for a device in the Configuration Center device list:

1. Navigate to Service→Configuration Center→Current Startup Configuration File.
2. Click the Service tab from the tabular navigation system on the top.
3. Do one of the following:
   - Click the Configuration Center icon located under the Resource and Configuration Management section of the Service page, or
   - Click the Configuration Center link located on the left navigation tree.
   All devices that can be managed by IMC’s Configuration Center are displayed in the list in the bottom half of the Configuration Center page.
4. Click the icon in the Operation field of the device in which you want to view the startup configuration.
5. Select Latest Startup Configuration from the popup menu.
   The most recent startup configuration file is displayed in the Configuration File Details page.

Stackable devices

For stackable devices, you must select the directory or location of the configuration file as follows:

1. Click the arrow keys to the right of the Source Device list, and select the unit you want to view.
2. To compare the startup file with the most recent backup version of the startup configuration file, click the Compare with Startup Configuration file of Latest Backup link located to the far right of the Configuration File Details page.
   The Compare Configuration File dialog box appears.
   The two startup configuration files are displayed in side-by-side windows with file details at the top of the dialog box.
   IMC provides a summary of all identical, changed, and unique lines at the bottom of the dialog box.
3. Do one of the following:
   - To view the entire contents of both configuration files, click the radio button to the left of Show All, or
   - To view only the differences between the two files, click the radio button to the left of Show Difference Only.
4. Do one of the following:
   - Click Next Diff to view, line-by-line, the configuration differences between the two files, or
4. Click Previous Diff to view the previous line that contains differences.
5. Click Close when you have finished viewing the configuration file comparison.

Viewing the latest running configuration

To view the latest running configuration for a device in the Configuration Center device list:

1. Navigate to Service→Configuration Center→Current Running Configuration File.
2. Click the Service tab from the tabular navigation system on the top.
3. Do one of the following:
   - Click the Configuration Center icon located under the Resource and Configuration Management section of the Service page, or
   - Click the Configuration Center link located on the left navigation tree.

   All devices that can be managed by IMC’s Configuration Center are displayed in the list in the bottom half of the Configuration Center page.
4. Click the icon in the Operation field of the device you want to view the running configuration for.
5. Select Latest Running Configuration from the popup menu.
   The most recent running configuration file is displayed in the Configuration File Details page.

Stackable devices

For stackable devices, you must select the directory or location of the configuration file as follows:
1. Click the arrow keys to the right of the Source Device list, and select the unit you want to view.
2. To compare the running configuration file with the most recent backup version of the running configuration file, click the Compare with Running Configuration file of Latest Backup link located to the far right of the Configuration File Details page.
   The Compare Configuration File dialog box appears.
   The two running configuration files are displayed in side-by-side windows with file details at the top of the dialog box.
   IMC provides a summary of all identical, changed, and unique lines at the bottom of the dialog box.
3. Do one of the following:
   - To view the entire contents of both configuration files, click the radio button to the left of Show All, or
   - To view only the differences between the two files, click the radio button to the left of Show Difference Only.
4. Do one of the following:
   - Click Next Diff to view, line-by-line, the configuration differences between the two files.
   - Click Previous Diff to view the previous line that contains differences, or
   
5. Click Close when you have finished viewing the configuration file comparison.

Configuration management page details

The Configuration Management option that can be found on the Operation popup menu provides you with many features for managing change and configuration for the selected device. At the top of this page, you can view configuration management summary details for the selected device. By using the features found in this section, you can initiate a manual backup of the startup and running configurations of the selected
device, configure a software baseline, set scheduled automatic backups and deploy operating system software to the selected device.

From the Configuration Backup History tab on the Configuration Management page, you can view a history of startup and running configuration backup files for the selected device. In addition, you can modify, restore, compare, establish a baseline and save configuration files.

Lastly, you can view the software update history for the selected device and deploy software from the Software Update History tab.

Configuration management summary

To view a summary of configuration management information for the selected device:

1. Navigate to Service→<Device Name>→Configuration Management.
2. Click the Service tab from the tabular navigation system on the top.
3. Do one of the following:
   - Click the Configuration Center icon located under the Resource and Configuration Management section of the Service page, or
   - Click the Configuration Center link located on the left navigation tree.

All devices that can be managed by the Configuration Center are displayed in the list in the bottom half of the Configuration Center page.

4. Click the icon in the Operation field of the device you want to view configuration information for.
5. Select Configuration Management from the popup menu.

The Configuration Management page is displayed and includes the following information:

- Device Name: Contains a link to the Device Details page for the associated device.
- Device Model: Contains device series and model information.
- Last Backup at: Contains a date and time stamp for the last backup of the configuration file. The [Backup] link to the right of this field initiates a manual backup of both the startup and running configuration files.
- Auto Backup Period: Contains information on the backup schedule for device configuration files. The [Set Attribute] link to the right of this field navigates you to the Add Auto Backup Plan page for scheduling regular configuration file backups. For more information on configuring an automatic backup plan, see "Managing automatic backup plans" (page 475).
- Current Software Version: Contains the current version of the operating system. The operating system name also serves as a link to the software library entry for the operating system, if it exists in the software library.
- Latest Available Version: Contains the latest version of the system software in the library for the associated device. The field is blank if there is no system software version that is newer than what is on the device and in the library. The [Deploy] link to the right of this field navigates you to the Deployment Guide configuration page for deploying software to selected devices. For more information of deploying software, see "Deploying configurations and software by using IMC’s deployment guide" (page 442).
- Baseline Software Version: Contains the baseline version of the operating system. This entry also serves as a link to the software library entry for the operating system, if it exists in the software library. A "-" in this field indicates that there is no configured baseline software version for the associated device. By using the [Configure] link to the right of this field enables you to select from the software list the operating system versions for performing a baseline on the selected device. For
more information on establishing a software version baseline, see "Establishing a software baseline" (page 417).

Configuration backup history

From the Configuration Backup History tab on the Configuration Management page, you can view a history of startup and running configuration backup files for the selected device. In addition, you can modify, restore, compare, establish a baseline or save configuration files.

To navigate to the Configuration Backup History list:
1. Navigate to Service→<Device Name>→Configuration Management.
2. Click the Service tab from the tabular navigation system on the top.
3. Do one of the following:
   - Click the Configuration Center icon located under the Resource and Configuration Management section of the Service page, or
   - Click the Configuration Center link located on the left navigation tree.

All devices that can be managed by the Configuration Center are displayed in the list in the bottom half of the Configuration Center page.
4. Click the icon in the Operation field of the device you in which you want to view the backup history.
5. Select Configuration Management from the popup menu.
   The Configuration Management page for the selected device appears.
6. Click the Configuration Backup History tab.
   The Configuration Backup History list appears.

Configuration backup history list

- **Version**: identifies the type of backup that was performed, a standard or common backup or a baseline backup.
- **File Name**: Contains the name of the backup file.
- **Type**: identifies what kind of configuration file was backed up, a startup or a running configuration file.
- **Backup Time**: Contains the date and time stamp for the associated backup of the configuration file.
- **Modify**: Contains a link for modifying the associated configuration file.
- **Restore**: Contains a link for restoring the associated configuration file.
- **Compare**: Contains a link for comparing the associated configuration file. IMC provides five options for comparing, including:
  - **Compare with Baseline Configuration**: Compares the selected backup history configuration file with the established baseline configuration file.
  - **Compare with Current Startup Configuration**: Compares the selected backup history configuration file with the device’s current startup configuration file.
  - **Compare with Current Running Configuration**: Compares the selected backup history configuration file with the device’s running startup configuration file.
  - **Compare with Current Startup and Running Configurations**: Compares the selected backup history configuration file with the device’s startup and running startup configuration file.
- **Compare with Other Configuration**: Compares the selected backup history configuration file with another startup, running, or backup history file for the same or another device.

- **Make Baseline**: Contains a link for establishing a baseline by using the associated file.

- **Save As**: Contains a link for saving the associated file.

If the **Configuration Backup History** list is long enough, the following navigational aids are displayed.

- Click to page forward in the **Configuration Backup History** list.
- Click to page forward to the end of the **Configuration Backup History** list.
- Click to page backward in the **Configuration Backup History** list.
- Click to page backward to the front of the **Configuration Backup History** list.

7. Click 8, 15, 50, 100, or 200 from the right side of the main pane to configure how many items per page you want to view.

8. For **Configuration Backup History** list that have more than one page, click 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 … from the bottom right side of the main pane to jump to a particular page of the trap list.

   You can sort the **Configuration Backup History** list by the **Version**, **File Name**, **Type**, and **Backup Time** fields. Click the column label to sort the list by the selected field. The column label is a toggle switch that lets you toggle between the various sort options specific to each field.

9. To filter the **Configuration Backup History** list, choose the option you want to filter by from the **Configuration File Version** list located on the far right of the **Configuration Backup History** section.

### Modifying a backup configuration file

IMC offers you the ability to make changes to configuration files. These changes include adding or modifying a description and changing the source devices.

To modify a backup configuration file:

1. Navigate to **Service**→**<Device Name>**→**Configuration Management**.
2. Click the **Service** tab from the tabular navigation system on the top.
3. Do one of the following:
   - Click the **Configuration Center** icon located under the **Resource and Configuration Management** section of the **Service** page, or
   - Click the **Configuration Center** link located on the left navigation tree.
   All devices that can be managed by the Configuration Center are displayed in the list in the bottom half of the **Configuration Center** page.
4. Click the icon in the **Operation** field of the device you want to view the backup history for.
5. Select **Configuration Management** from the popup menu.
   The **Configuration Management** page for the selected device appears.
6. Click on the **Configuration Backup History** tab.
   The **Configuration Backup History** list appears.
7. Click the icon in the **Modify** field of the backup configuration file you want to modify.
8. If prompted, select the device unit from the **Source Device** list.
9. Enter a description for this configuration backup file in the **Description** field.
10. To save the source device and description changes you made, click **Modify Description**.
11. To save your changes to a new file, click **Save As**.
   The **Save File As** dialog box appears.

12. Enter the name for the configuration file in the **File Name** field. The characters listed in Table 18 are invalid and cannot be used.

**Table 18 Invalid characters**

<table>
<thead>
<tr>
<th>Character</th>
<th>Name</th>
<th>Character</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>0-9</td>
<td>Numbers</td>
<td>'</td>
<td>Apostrophe or single quotation</td>
</tr>
<tr>
<td>_</td>
<td>Underscore</td>
<td>*</td>
<td>Asterisk</td>
</tr>
<tr>
<td></td>
<td>Vertical bars</td>
<td>:</td>
<td>Colon</td>
</tr>
<tr>
<td>\</td>
<td>Backslash</td>
<td>&quot;</td>
<td>Double quotation</td>
</tr>
<tr>
<td>/</td>
<td>Forward slash</td>
<td>&lt; &gt;</td>
<td>Angle brackets</td>
</tr>
<tr>
<td>?</td>
<td>Question mark</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

13. Click **OK**.

**Restoring a configuration file**

The **Restore** option on the **Configuration Management** page provides you with a link to the **Deployment Guide** for restoring a configuration file. For information on restoring software in IMC, see "Deploying configurations and software by using IMC’s deployment guide" (page 442) and "Restoring a device configuration" (page 445).

**Comparing configuration files**

The **Configuration Management** page under the **Operation** link for a selected device contains a link for comparing the contents of configuration files. You can compare backup startup or running configuration files with the current startup or running configuration files. IMC also provides a line-by-line comparison of the two files with changes highlighted. In addition, IMC provides a summary of identical, changes, and unique lines.

To compare the contents of a backup configuration file with another file:

1. Navigate to **Service→<Device Name>→Configuration Management**.
2. Click the **Service** tab from the tabular navigation system on the top.
3. Do one of the following:
   o Click the **Configuration Center** icon located under the **Resource and Configuration Management** section of the **Service** page, or
   o Click the **Configuration Center** link located on the left navigation tree.
All devices that can be managed by the Configuration Center is displayed in the list in the bottom half of the **Configuration Center** page.

4. Click the icon in the **Operation** field of the device in which you want to view the startup configuration.

5. Select **Configuration Management** from the popup menu.
   The **Configuration Management** page for the selected device appears.
6. Click the **Configuration Backup History** tab.
   The **Configuration Backup History** list appears.
7. Click the icon 📂 in the Compare field of the backup configuration file you want to compare.
The Select Target File dialog box listing file comparison options appears.
8. Click the radio button ☐ to the left of the file you want to compare:
   - Choose Compare with Baseline Configuration if you want to compare the selected file with the configuration file that has been designated as the Baseline Configuration for this device.
   - Choose Compare with Current Startup Configuration if you want to compare the selected file with the current startup configuration of the selected device.
   - Choose Compare with Current Running Configuration if you want to compare the selected file with the current running configuration of the selected device.
   - Choose Compare with Current Startup and Running Configurations if you want to compare the selected backup history configuration file with the device’s startup and running startup configuration file.
   - Choose Compare with Other Configuration if you want to compare the selected file with another configuration file from the same or another device.
9. Click OK.
10. Do one of the following:
    - If you selected one of the first three options, skip to Step 11 in the next section, or
    - If you selected the option to Compare with Other Configuration, follow the instructions in the next section.

    The General Configuration Compare page is displayed, enabling you to configure the two files you want to compare.

Configuring the first or left configuration file

This General Configuration Compare page lets you configure the two files you want to compare. The first file is displayed on the left side of the results page and the second file is displayed on the right.

to configure the options for the first or left file:

1. To change your device selection, click Select to add a device by the View method in the Select Device Field.
   This field is populated with the pre-selected device.
2. From the Select Devices dialog box, click the By View tab.
3. Expand the view you want to select a device by clicking on the arrow icon to the left of the three view options, IP View, Device View, or Custom View.
4. Click the view you want to select devices from the navigation tree on the left.
   The devices from the group you click on appear in the Devices Found field to the right of the navigation tree.
5. Highlight the device you want to select from the Devices Found list and click Add selected 🔖 to add it to the selected device list.
6. Confirm that the device you have found has been added by reviewing the Selected Devices list.
7. Click OK.
8. Confirm that the device now appears in the Select Device field of the General Configuration Compare page.
   If you are comparing configuration files for a stackable unit, the Stack Unit list appears.
9. Select the unit you want to use as a source for a configuration file from the Stack Unit list.
10. Select the type of configuration file you want to use for comparison from the File Type list.
11. If you selected Backup History as your file type, select the particular configuration file you want to compare from the Configuration File list.

### Configuring the second or right configuration file

Select the second configuration file that is displayed on the right.

To configure the options for the second or right configuration file:

1. Enter the device name or click Select to add a device by View or by the Advanced query method. See "Adding devices by View" (page 85) and "Adding devices by Advanced query" (page 85).
2. Confirm that the device now appears in the Select Device field of the General Configuration Compare page.
3. Select the type of configuration file you want to use for comparison from the File Type list.
4. Click OK.

   The Compare Configuration File dialog box is displayed with configuration files in side-by-side windows and file details at the top of the dialog box.

At the bottom of the page is a summary of all identical, changed, and unique lines.

5. Do one of the following:
   - To view the entire contents of both configuration files, click the radio button to the left of Show All, or
   - To view only the differences between the two files, click the radio button to the left of Show Difference Only.

6. Do one of the following:
   - Click Next Diff to view, line-by-line, the configuration differences between the two files, or
   - Click Previous Diff to view the previous line that contains differences.

7. Click Close when you have finished viewing the configuration file differences.

### Establishing a configuration file baseline

You can define a baseline from the Configuration Management page under the Operation link for a selected device. Establishing a baseline in IMC marks the selected file as the standard or basic configuration file for the selected device. Every device can have one configuration file defined as its baseline and it serves as a foundation upon which the device’s configuration is evaluated and audited.

In addition, once a baseline has been established, you can revert to the established baseline configuration file if any problems arise with the device’s configuration.

To establish a configuration file as a baseline configuration for the selected device:

1. Navigate to Service→<Device Name>→Configuration Management.
2. Click the Service tab from the tabular navigation system on the top.
3. Do one of the following:
   - Click the Configuration Center icon located under the Resource and Configuration Management section of the Service page, or
   - Click the Configuration Center link located on the left navigation tree.

   All devices that can be managed by the Configuration Center are displayed in the list in the bottom half of the Configuration Center page.
4. Click the icon 🗓️ in the **Operation** field of the device you want to view the startup configuration for.

5. Select 🛠️ **Configuration Management** from the popup menu.
   The **Configuration Management** page for the selected device appears.

6. Click the **Configuration Backup History** tab.
   The **Configuration Backup History** List appears.

7. Click the icon 📦 in the Make Baseline field of the backup configuration file you want to set as the baseline configuration.
   The **Configuration Management** page is updated to display the results of the baseline operation.

8. Review the results to ensure successful completion.

### Creating a configuration template by using Save As for configuration files

You can save a configuration file as a configuration template from the **Configuration Management** page. The **Save As** icon in the **Configuration Management Backup History** list serves as a link that navigates you to the **Configuration Templates** page for creating a configuration template. For more information on creating configuration templates in IMC, see "Creating a configuration template" (page 423).

### Software update history

The **Software Update History** tab of the **Configuration Management** page provides you with visibility into the history for system and other software updates for the selected device.

To view the software update history for the selected device:

1. Navigate to **Service → <Device Name> → Configuration Management**.

2. Click the **Service** tab from the tabular navigation system on the top.

3. Do one of the following:
   
   - Click the 🛠️ **Configuration Center** icon located under the **Resource and Configuration Management** section of the **Service** page, or
   
   - Click the 🛠️ **Configuration Center** link located on the left navigation tree.

   All devices that can be managed by IMC’s **Configuration Center** is displayed in the list in the bottom half of the **Configuration Center** page.

4. Click the icon 🗓️ in the **Operation** field of the device you want to view the startup configuration for.

5. Select 🛠️ **Configuration Management** from the popup menu.
   The **Configuration Management** page for the selected device appears.

6. Click the **Software Update History** tab.
   The **Software Update History** List appears.

### Software update history list

- **Update Result**: Contains the result of the software update task.
- **Start Time**: Contains a date and time stamp for the start time of the associated software update task.
- **Finished Time**: Contains a date and time stamp for the completion time of the associated software update task.
- **Update Type**: Identifies what type of software update task was performed. Possible values include Update and Rollback.
- **Old Version**: Contains the software file name of the old version of software, and whether the task was an update or a rollback.
- **New Version**: Contains the software file name of the new version of software.
- **Update Path**: Identifies to which directory on the selected device the software was written.
- **Restore**: Contains a link to the Deployment Guide for restoring the system software file. For information on restoring software in IMC, see "Deploying configurations and software by using IMC’s deployment guide" (page 442) and "Restoring device software" (page 445).

If the **Software Update History** list is long enough, the following navigational aids are displayed.

- Click to page forward in the **Software Update History** list.
- Click to page forward to the end of the **Software Update History** list.
- Click to page backward in the **Software Update History** list.
- Click to page backward to the front of the **Software Update History** list.

**Clean device space**

From the configuration management page, you can also remove system software, configuration files and other file types from the selected device by using the Clean Device Space option. IMC displays the contents of a device’s memory and with a few clicks you can remove unneeded files.

To remove files from the memory of a network device:

1. Navigate to Service→<Device Name>→Configuration Management.
2. Click the Service tab from the tabular navigation system on the top.
3. Do one of the following:
   - Click the **Configuration Center** icon located under the Resource and Configuration Management section of the Service page, or
   - Click the **Configuration Center** link located on the left navigation tree.

All devices that can be managed by the **Configuration Center** are displayed in the list in the bottom half of the **Configuration Center** page.

4. Click the icon in the Operation field of the device you want to view the startup configuration for.
5. Select **Clean Device Space** from the popup menu.

The **Device File List** dialog box for the selected device appears. This dialog box contains the **Device File List** for the selected device.

Total space and available space on the device is displayed at the top of the **Device File List** table.
Device file list

- **File Name**: Contains the name of the file.
- **File Location**: Contains the location of the file on the device.
- **File Size (Byte)**: Contains the size of the file in bytes.
- **File Type**: identifies the type of file – system or operating system software, configuration file, or other.
- **File State**: identifies whether or not the associated file is valid (usable) or invalid.
- **Image File Type**: If an image exists, the type of image is displayed in this field.
- **Running Image File**: identifies whether or not the associated file is also the current or running image for the device.
- **Startup Configuration**: identifies whether or not the associated file is the startup configuration file for the device.

If the Device File List is long enough, the following navigational aids appears.

- Click ➡️ to page forward in the Device File List.
- Click ⇡️ to page forward to the end of the Device File List.
- Click ◀️ to page backward in the Device File List.
- Click ◄️ to page backward to the front of the Device File List.

6. Click 8, 15, 50, 100, or 200 from the right side of the main pane to configure how many items per page you want to view.

7. For Device File List that have more than one page, click on 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 … from the bottom right side of the main pane to jump to a particular page of the Device File List.

8. To delete one or more files from the device, click the checkbox ☑️ to the left of each file you want to remove.

9. Click Delete File.

10. Click OK to confirm deletion of the selected files.

11. Click Refresh to refresh the Device File List and to confirm removal of the selected files.

**Establishing a software baseline**

By using the Set Baseline Software option available from the Operation popup menu, you can define the baseline or standard software configuration for the selected device. Once a software baseline has been established, you can easily revert to the established baseline if any problems arise with the device.

To set a software baseline for the selected device:

1. Navigate to Service→<Device Name>→Configuration Management.
2. Click the Service tab from the tabular navigation system on the top.
3. Do one of the following:
   - Click the 📝 Configuration Center icon located under the Resource and Configuration Management section of the Service page, or
   - Click the 📝 Configuration Center link located on the left navigation tree.

All devices that can be managed by the Configuration Center are displayed in the list in the bottom half of the Configuration Center page.

4. Click the icon 🐜 in the Operation field of the device you want to view the startup configuration for.
5. Select "Set Baseline Software" from the popup menu. The "Select Deployed Software" dialog box appears.

6. Click the radio button to the left of the file you want to set as the software baseline.

7. Click OK.
The results of the set baseline software task are displayed at the top of the Configuration Center page.

8. Review the results to ensure that the task was completed successfully.

**Comparing device configurations**

You can compare the contents of configuration files. You can compare backup startup or running configuration files with the current startup or running configuration files. IMC also provides a line-by-line comparison of the two files with changes highlighted.

In addition, IMC provides a summary of identical, changes, and unique lines. The "Compare with Other Device Configuration" option available from the Operations popup offers you a quick link to the Configuration Compare page. For more information on this feature, see "Comparing device configurations" (page 441).

1. Navigate to Service→<Device Name>→Configuration Management.

2. Click the Service tab from the tabular navigation system on the top.

3. Do one of the following:
   - Click the Configuration Center icon located under the Resource and Configuration Management section of the Service page, or
   - Click the Configuration Center link located on the left navigation tree.

   All devices that can be managed by the Configuration Center are displayed in the list in the bottom half of the Configuration Center page.

4. Click the icon in the Operation field of the device you want to view the startup configuration for.

5. Select "Compare with Other Device Configuration" from the popup menu.
The General Configuration Compare page appears.

   This page lets configure the two files you want to compare, the first file that is displayed on the left side of the results page and the second file that is displayed on the right.

**Configuring the first or left configuration file**

You configure the two files you want to compare. The first file is displayed on the left side of the results page and the second file is displayed on the right.

**Configuring the second or right configuration file**

You can configure the options for the second or right configuration file.

**Deploying software from the Configuration Center**

You can launch the Deployment Guide from the Configuration Center for deploying software to selected devices. The Deploy Software button on the Configuration Management page serves as a link that navigates you to the Deployment Guide for deploying software to the selected devices.

To use this feature, first click the checkbox to the left of the devices you want to deploy software to. Click Deploy Software to begin the deployment process for the selected devices. For more information on deploying software by using the Deployment Guide, see "Deploying configurations and software by using IMC’s deployment guide" (page 442).
Deploying configurations from the Configuration Center

You can launch the Deployment Guide from the Configuration Center for deploying configurations to selected devices. The Deploy Configuration button on the Configuration Management page serves as a link that navigates you to the Deployment Guide for deploying configurations to the selected devices.

To use this feature, click the checkbox  to the left of the devices in which you want to deploy software. Click Deploy Configuration to begin the deployment process for the selected devices. For more information on deploying software by using the Deployment Guide, see "Deploying configurations and software by using IMC’s deployment guide" (page 442).

Backing up configurations from the Configuration Center

You can back up the configuration files for one or more devices. The Configuration Center provides you with quick access to the backup configuration feature for one-time backups of selected devices. For scheduled backups, see "Managing automatic backup plans" (page 475) and "Automatic device configuration backups" (page 475).

To manually backup one or more devices from the Configuration Center:

1. Navigate to Service → Configuration Center.
2. Click the Service tab from the tabular navigation system on the top.
3. Do one of the following:
   o Click the Configuration Center icon located under the Resource and Configuration Management section of the Service page, or.
   o Click the Configuration Center link located on the left navigation tree.

All devices that can be managed by the Configuration Center are displayed in the list in the bottom half of the Configuration Center page.

4. Click the checkboxes  to the left of the devices for which you want to back up the configuration file.
5. Click Backup Configuration.

The page is updated to display the Configuration File Backup Result table. This results table displays the result for each configuration file that was backed up. The Configuration File Backup Result table provides descriptive information for the devices that were backed up including Device Name, Device Type, File Type, startup or running configuration file and the Time of the backup. Also included in this table are the results of each configuration file backup. The Results field contains information on whether or not the backup of configuration files for each device succeeded or failed.

Additionally, the icon in the Detail field associated with every configuration file navigates to a new dialog box that provides information on where backup succeeded or failed in each step of the backup process. Review the results for each entry in this table and in the Results and Detail fields in particular to ensure that all configuration files were backed up successfully or to identify where problems occurred that prevented a successful backup.

The Backup History Report option in the Configuration Center provides you with visibility into the results of both manual and automatic backup tasks. For more information on using the Backup History Report option, see "Backup history reporting" (page 479).

Restoring a configuration from the Configuration Center

The Restore button on the Configuration Management page provides a link to the Deployment Guide for restoring configurations or software by using IMC’s Deployment Guide. For information on restoring software or configurations in IMC, see "Deploying configurations and software by using IMC’s deployment guide" (page 442).
Deploying a file from the Configuration Center

You can launch the Deployment Guide from the Configuration Center for deploying files to selected devices. The Deploy File button on the Configuration Management page serves as a link that navigates you to the Deployment Guide for deploying files to the selected devices.

To use this feature, first click the checkbox to the left of the devices you want to deploy software to. Then, click Deploy Configuration to begin the deployment process for the selected devices. For more information on deploying software by using the Deployment Guide, see "Deploying configurations and software by using IMC’s deployment guide" (page 442).

Managing device configurations with templates

IMC uses configuration templates for standardizing the configuration of network device. Through the use of configuration templates, you can create and save device configurations and determine which device series or models to apply the configuration template. When you deploy the configuration template, IMC filters out all devices that the configuration template cannot be deployed to. This simplifies the deployment of configuration templates and reduces errors that can arise from applying a configuration template to the wrong device.

You can create three types of configuration templates, File, Segment, and CLI Script templates. With a file template type, you can create and store an entire startup or running configuration template and apply it in its entirety to one or more devices. With file templates, the old configuration file is replaced by the contents of the template. With a segment template type, you create just a portion of a startup or running configuration. IMC applies just the segment to the existing startup or running configuration file.

IMC provides folders for managing the organization of configuration templates. This lets you quickly access configuration templates. As with most other features and modules, IMC provides a search method for quickly locating configuration templates.

Accessing configuration templates

To access configuration templates and template folders:

1. Navigate to Service→Configuration Templates.
2. Click the Service tab from the tabular navigation system on the top.
3. Click the Configuration Center on the navigation tree on the left.
4. Click the Configuration Templates under Configuration Center from the navigation system on the left.

All root configuration template folders and configuration templates stored at the template folder root level is displayed in the Configuration Templates list.

Configuration templates list

- **Template Name**: Contains the name of the template or the template folder. Templates have a template icon to the left of the template name. Folders have a folder icon to the left of the folder name.
- **Type**: Identifies whether or not the associated entry is a template file, segment, or folder.
- **Create Time**: Identifies by date and time stamp when the configuration file, segment, or folder was created.
- **Description**: Contains the description for the file, segment or folder that was configured by the operator when it was created.
o **Delete**: Contains a link ✗ for deleting the associated configuration template or folder.

o **Operation**: Contains an icon that displays links to operational tasks for the associated file, segment, or folder. Options include **Rename**, **Modify**, **Copy**, **Export**, and **Deploy**. For more information on using each of these operations, see the following sections of this chapter on renaming, modifying, copying, exporting, or deploying templates.

You can sort the **Configuration Templates** list by the **Template Name**, **Create Time**, and **Description** fields. Click the column label to sort the list by the selected field. The column label is a toggle switch that lets you toggle between the various sort options specific to each field.

If the **Configuration Templates** list contains enough entries, the following navigational aids are displayed.

- Click ➤ to page forward in the **Configuration Templates** list.
- Click ➙ to page forward to the end of the **Configuration Templates** list.
- Click ◀ to page backward in the **Configuration Templates** list.
- Click ⇑ to page backward to the front of the **Configuration Templates** list.

5. **Click 8, 15, 50, 100, or 200** from the right side of the main pane to configure how many items per page you want to view.

### Querying configuration templates

You can search for a particular configuration template file or folder and filter the current list. You can filter either by a partial or complete template file or folder name or by template type. IMC displays only those configuration template files and folders that match the search or filter criteria.

To filter the **Configuration Templates** list:

1. Navigate to **Service**→**Configuration Templates**.
2. Click the **Service** tab from the tabular navigation system on the top.
3. Click the **Configuration Center** on the navigation tree on the left.
4. Click the **Configuration Templates** under **Configuration Center** from the navigation system on the left.

   All root configuration template folders and configuration templates stored at the template folder root level display in the **Configuration Templates** list. The **Query Criteria** section of the templates page displays above the **Configuration Templates** list.

5. Enter one or more of the following search criteria in the **Query Criteria** dialog box:
   - **Folder**: Select which folder you want to search in or filter on from the **Folder** list.
   - **Template Name**: Enter some portion or all of the configuration template name you want to filter the configuration template list.
   - **Template Type**: Select the type of template by which you want to filter the configuration template list from the **Template Type** list.

6. **Click Query** to submit your filter criteria.

   The results of your filter or search query is displayed in the **Configuration Templates** list below.

7. **Click Reset** when you want to restore the full **Configuration Templates** list.
Organizing configuration templates

IMC offers you the ability to create as many configuration templates as needed to manage the ongoing task of network device configuration management. With the ability to create whole configuration files and sections of a configuration file called segments, you can easily create hundreds of configuration files.

You can create folders to organize configuration templates. Template configuration folders work exactly the same way as folder or directories in file systems, meaning you can create folders at the root level and nested within folders. You can also add templates at the root level and in subfolders. Ideas for template organization include grouping templates by device type, location, device function, just to name a few.

Template configuration subfolders are accessed by selecting the parent folder in the same way that subdirectories are accessed by double clicking on the parent directory.

Creating a template folder

To create a new template folder:

1. Navigate to Service→Configuration Templates.
2. Click the Service tab from the tabular navigation system on the top.
3. Click the Configuration Center on the navigation tree on the left.
4. Click the Configuration Templates under Configuration Center from the navigation system on the left.

All root configuration template folders and configuration templates stored at the template folder root level are displayed in the Configuration Templates list.
5. Navigate to the folder in which you want to add a folder.
6. Click the Add Folder link located to the far right of the Configuration Templates list.

The Add Folder dialog box appears.

Operators must have administrative level access to create configuration template folders.
7. Enter a name for the folder in the Name field.

Configuration template names cannot begin or end with a period (.). Spaces in the configuration template name are also not permitted. In addition, the characters in Table 19 (page 422) are not permitted in a configuration template file name.

Table 19 Invalid characters

<table>
<thead>
<tr>
<th>Character</th>
<th>Name</th>
<th>Character</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>Asterisk</td>
<td>'</td>
<td>Apostrophe or single quotation</td>
</tr>
<tr>
<td></td>
<td>Vertical bars</td>
<td>:</td>
<td>Colon</td>
</tr>
<tr>
<td>\</td>
<td>Backslash</td>
<td>&quot;</td>
<td>Double quotation</td>
</tr>
<tr>
<td>/</td>
<td>Forward slash</td>
<td>&lt; &gt;</td>
<td>Angle brackets</td>
</tr>
<tr>
<td>?</td>
<td>Question mark</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

8. Enter a description for the folder in the Description field.
9. Click OK.

Modifying a configuration template folder

To modify an existing configuration template folder:
1. Navigate to Service→Configuration Templates.
2. Click the Service tab from the tabular navigation system on the top.
3. Click the Configuration Center on the navigation tree on the left.
4. Click the Configuration Templates under Configuration Center from the navigation system on the left.
   All root configuration template folders and configuration templates stored at the template folder root level are displayed in the Configuration Templates list.
5. Navigate to the parent folder that contains the folder you want to modify.
6. From the Configuration Templates list, click the Operation icon associated with the configuration template folder you want to modify. Select Modify from the popup window.
7. Modify the description of the folder in Description field as needed.
8. Click OK to accept your changes.

Deleting a configuration template folder

To delete an existing configuration template folder:
1. Navigate to Service→Configuration Templates.
2. Click the Service tab from the tabular navigation system on the top.
3. Click the Configuration Center on the navigation tree on the left.
4. Click the Configuration Templates under Configuration Center from the navigation system on the left.
   All root configuration template folders and configuration templates stored at the template folder root level is displayed in the Configuration Templates list.
5. Navigate to the parent folder that contains the folder you want to delete.
6. From the Configuration Templates list, click the Delete icon associated with the configuration template folder you want to delete.
7. Click OK to confirm deletion of the configuration template folder.

Creating a configuration template

IMC provides you with these types of templates: File, Segment, and CLI Script.

File configuration templates include the entire contents of a startup or running configuration. File configuration templates are applied in their entirety and the operator determines which file (the existing startup or running configuration file) is replaced when a template is deployed.

Segment configuration templates contain only a portion of a configuration file. When they are deployed, the configuration segment is added to the existing startup or running configuration. Segment configuration templates let you modularize the process of template creation and therefore configuration file management.

IMC also provides three methods for creating device configuration templates. The recommended method for creating a template involves importing the contents of a template from a configuration file backed up by IMC. By using this method, you can leverage existing configurations and modify them as needed to create a template.

You can also create a configuration template from scratch by using the Manual Add option. By using this method, you begin with a blank file and build the configuration manually.
The third method for creating a configuration template is to import the contents from a file on the operator’s local computer.

**Adding a configuration template by using a backup file**

Creating a configuration template by using a backup file is the quickest and easiest way to build templates. By using this method, you can leverage an existing configuration file and make the modifications that are needed before saving it as a template. This method is effective both file and segment configuration template types and is the recommended method for building configuration templates quickly and easily.

To create a configuration template from a backup configuration file created by IMC:

1. Navigate to **Service → Configuration Templates**.
2. Click on the **Service** tab from the tabular navigation system on the top.
3. Click on the **Configuration Center** on the navigation tree on the left.
4. Click the **Configuration Templates** under **Configuration Center** from the navigation system on the left.
   
   All root configuration template folders and configuration templates stored at the template folder root level are displayed in the **Configuration Templates** list.

5. Navigate to the folder that you want to add a configuration template to.
6. Click **Add**.
7. Select **Import From Backup File** from the popup menu.
   
   A list displaying all backup configuration files in IMC is displayed in the **Select Backup History** list.

8. Locate the backup configuration file from the **Select Backup History** list.
9. Click the radio button  to the left of the configuration file you want to use.
   
   To use this feature, the configuration file must already exist in IMC. For more information on using IMC to back up the device configuration files, see "Managing automatic backup plans" (page 475).

10. Click **Next**.

    The **Add Configuration Template** page appears.

11. Enter a name for the template in the Template Name field.

    Configuration template names cannot begin or end with a period (.). Spaces in the configuration template name are also not permitted. In addition, the characters in Table 20 (page 424) are not permitted in a configuration template file name.

<table>
<thead>
<tr>
<th>Character</th>
<th>Name</th>
<th>Character</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>Asterisk</td>
<td>'</td>
<td>Apostrophe or single quotation</td>
</tr>
<tr>
<td></td>
<td>Vertical bars</td>
<td>:</td>
<td>Colon</td>
</tr>
<tr>
<td>\</td>
<td>Backslash</td>
<td>&quot;</td>
<td>Double quotation</td>
</tr>
<tr>
<td>/</td>
<td>Forward slash</td>
<td>&lt; &gt;</td>
<td>Angle brackets</td>
</tr>
<tr>
<td>?</td>
<td>Question mark</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

12. Select the type of template you want to create from the **Template Type** list. Template type options include **File** and **Segment**.
A file template type creates an entire configuration file that is then applied to the devices selected for deployment. A segment template type creates only a portion of a configuration field, which is then applied to the selected devices. For example, if your organization uses SNMP community strings that vary by location, you can create a configuration file by using a segment template type for just the SNMP community string configuration for each location and then deploy that configuration template to devices by location.

13. Select the configuration template folder you want to save this template to from the **Folder** list.

14. Select the device type you want to create this configuration template for by clicking the **Select Model** button to the right of the **Applicable Devices** field.

The **Device Type** dialog box appears.

The **Device Type** dialog box contains two sections. The **Series List** section contains a list of all vendor specific device series in IMC. The top section under **Device Type** provides two options for filtering the **Series List**.

15. Do one of the following:
   - To display the device series for a specific vendor, select the vendor from the **Vendor Name** list in the top section of the **Device Type** dialog box, or
   - To display a specific device series, enter a full or partial device series name in the **Series** field.

16. Click **Query** to apply your filter to the **Series List**.

17. Click the device series name you want to adapt this configuration template to. An expanded list of all device types under the device series name you selected appears.

18. Click the checkbox □ to the left of the devices you want to adapt this configuration template to.

19. Click **OK**.

20. Enter a description for the configuration template in the **Description** field.

Adding a description that uniquely identifies the function of the configuration template is a valuable aid that supports the correct deployment of configuration templates. Consider using the devices to which the template is applied and what the template contains, if using a segment template type. For segment configuration templates, consider naming the template by the type of function or commands contained within the template.

21. Modify the text in the **Content** field as needed.

22. If you are creating a segment template, delete all of the content that you do not want to apply to devices when this configuration template is deployed to devices in the infrastructure.

Variables are supported in configuration templates. If you use variables in a configuration template, you is prompted for the variable values when you deploy the configuration template.

The variable format is ${variable name}. For example ${ip address} is a valid variable where ip address is used as the variable name. When you deploy the configuration template, ${ip address} is replaced by the IP address you define.

Any blank spaces before or after variable names are omitted. For example, IMC converts ${paramName} to ${paramName}. A variable name cannot include spaces ( ), dollars signs ($) or curly braces ({}).

23. Click **OK**.

**Adding a configuration template by using file import**

You can also import the contents of a configuration file from your local computer for use in creating a configuration template as follows:

1. Navigate to **Service**→**Configuration Templates**.
2. Click the Service tab from the tabular navigation system on the top.
3. Click the Configuration Center on the navigation tree on the left.
4. Click the Configuration Templates under Configuration Center from the navigation system on the left.
   All root configuration template folders and configuration templates stored at the template folder root level is displayed in the Configuration Templates list.
5. Navigate to the folder in which you want to add a configuration template.
6. Click Add.
7. Select Import From File from the popup menu.
   The Import Configuration Template page appears.
8. Enter the file, including the full path you want to use for this configuration template in the Select file field.
10. Click Browse to locate the file on your local computer.
11. Click OK once you have selected the file and the filename including its full path is displayed in the Select File field.
12. Enter a name for the template in the Target File field.
   Configuration template names cannot begin or end with a period (.). Spaces in the configuration template name are also not permitted. In addition, the characters in Table 21 are not permitted in a configuration template file name.

### Table 21 Invalid characters

<table>
<thead>
<tr>
<th>Character</th>
<th>Name</th>
<th>Character</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>Asterisk</td>
<td>'</td>
<td>Apostrophe or single quotation</td>
</tr>
<tr>
<td></td>
<td>Vertical bars</td>
<td>:</td>
<td>Colon</td>
</tr>
<tr>
<td>\</td>
<td>Backslash</td>
<td>&quot;</td>
<td>Double quotation</td>
</tr>
<tr>
<td>/</td>
<td>Forward slash</td>
<td>&lt; &gt;</td>
<td>Angle brackets</td>
</tr>
<tr>
<td>?</td>
<td>Question mark</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

13. Select the type of template you want to create from the Template Type list. Template type options include File and Segment.
   A file template type creates an entire configuration file that is then applied to the device by using the deployment option. A segment template type creates only a portion of a configuration field, which is then applied to the device.
   For example, if your organization uses SNMP community strings that vary by location, you can create a configuration file by using a segment template type for just the SNMP community string configuration for each location and then deploy that configuration template to devices by location.
14. Select the configuration template folder you want to save this template to from the Folder list.
15. Select the device you want to adapt this configuration template to by clicking the Select Model button to the right of the Applicable Devices field.
   The Device Type dialog box appears.
The **Device Type** dialog box contains two sections. The **Series List** section contains a list of all vendor specific devices series in IMC. The top section under **Device Type** gives you two options for filtering the **Series List**.

16. Do one of the following:
   - To display devices series for a specific vendor, select the vendor from the **Vendor Name** list in the top section of the **Device Type** dialog box, or
   - To display a specific device series, enter a full or partial device series name in the **Series** field.

17. Click **Query** to apply your filter to the **Series List**.

18. Click the device series name you want to adapt this configuration template to.
   An expanded list of all device types under the device series name you selected appears.

19. Click the checkbox \(\square\) to the left of the devices you want to adapt this configuration template to.

20. Click **OK**.

21. Enter a description for the configuration template in the **Description** field.
   Adding a description that uniquely identifies the function of the configuration template is a valuable aid that supports the correct deployment of configuration templates. Consider using the devices to which the template is applied and what the template contains, if using a segment template type. For segment configuration templates, consider naming the template by the type of function or commands contained within the template.

22. Click **OK**.

**Manually adding a configuration template**

To manually create a configuration template:

1. Navigate to **Service**→**Configuration Templates**.
2. Click the **Service** tab from the tabular navigation system on the top.
3. Click the **Configuration Center** on the navigation tree on the left.
4. Click the **Configuration Templates** under **Configuration Center** from the navigation system on the left.
   All root configuration template folders and configuration templates stored at the template folder root level display in the **Configuration Templates** list.
5. Navigate to the folder that you want to add a configuration template to.
6. Click **Add**.
7. Select **Manual Add** from the popup menu.
8. Enter a name for the template in the **Template Name** field.
   Configuration template names cannot begin or end with a period (.) Spaces in the configuration template name are also not permitted. In addition, the characters in Table 22 are not permitted in a configuration template file name.

<table>
<thead>
<tr>
<th>Character</th>
<th>Name</th>
<th>Character</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>Asterisk</td>
<td>'</td>
<td>Apostrophe or single quotation</td>
</tr>
<tr>
<td></td>
<td>Vertical bars</td>
<td>;</td>
<td>Colon</td>
</tr>
<tr>
<td>\</td>
<td>Backslash</td>
<td>&quot;</td>
<td>Double quotation</td>
</tr>
</tbody>
</table>

427
9. Select the type of template you want to create from the **Template Type** list. Template type options include **File**, **Segment** and **CLI Script**.

A file template type creates an entire configuration file that is then applied to the device by using the deployment option.

A segment template type creates only a portion of a configuration field, which is then applied to the device. For example, if your organization uses SNMP community strings that vary by location, you can create a configuration file by using a segment template type for just the SNMP community string configuration for each location and then deploy that configuration template to devices by location.

A CLI script template type creates a CLI configuration file, which is then applied to the device through telnet.

10. Select the configuration template folder you want to save this template to from the **Folder** list.

11. Select the device type you want to create this configuration template for by clicking the **Select Model** button to the right of the **Applicable Devices** field.

The **Device Type** dialog box appears.

The **Device Type** dialog box contains two sections. The **Series List** section contains a list of all vendor specific device series in IMC. The top section under **Device Type** provides two options for filtering the **Series List**.

12. Do one of the following:
   - To display the device series for a specific vendor, select the vendor from the **Vendor Name** list in the top section of the **Device Type** dialog box, or
   - To display a specific device series, enter a full or partial device series name in the **Series** field.

13. Click **Query** to apply your filter to the **Series List**.

14. Click the device series name you want to adapt this configuration template to.

An expanded list of all device types under the device series name you selected appears.

15. Click the checkbox box to the left of the devices you want to adapt this configuration template to.

16. Click **OK**.

17. Enter a description for the configuration template in the **Description** field.

Adding a description that uniquely identifies the function of the configuration template is a valuable aid that supports the correct deployment of configuration templates. Consider using the devices to which the template is applied and what the template contains, if using a segment template type. For segment configuration templates, consider naming the template by the type of function or commands contained within the template.

18. Enter the contents of your configuration template in the **Content** field.

Variables are supported in configuration templates. If you use variables in a configuration template, you are prompted for the variable values when you deploy the configuration template.

The variable format is `${variable name}`. For example `${ip address}` is a valid variable where ip address is used as the variable name. When you deploy the configuration template, `${ip address}` is replaced by the IP address you define.
19. If you select the **CLI Script** option from the **Template Type** list, you can add configuration template commands in the **Content** field by using a table.
   - **Command**: Enter the command to be configured.
   - **Response Prompt**: Response of the command lines.
   - **Prompt Condition**: Select the response type, ✗ Error Prompt or ✔ Successful Prompt.
   - **Action**: Click Add to enter another command, and click Delete to delete the corresponding command.

20. Click **Change to Advanced Mode** link to switch to the advanced mode, and enter the configuration template commands in the **Content** field.

Any blank spaces before or after variable names are omitted. For example, IMC converts `${paramName}` to `$(paramName)`. A variable name cannot include spaces ( ), dollars signs ($) or curly braces ({}).

21. Click **OK**.

If you click Add on the **Configuration Templates** page, and select Add CLI Script from the popup menu, you can also enter the **Add Configuration Template** page with the default **Template Type** as CLI Script.

### Modifying a configuration template

You can modify most of a configuration template’s parameters. Other configuration options such as renaming a template or moving it to another location are available through other **Operation** menu options.

To modify most of the parameters of a configuration template:

1. Navigate to **Service → Configuration Templates**:
   - Click the **Service** tab from the tabular navigation system on the top.
   - Click the **Configuration Center** on the navigation tree on the left.
   - Click the **Configuration Templates** under **Configuration Center** from the navigation system on the left.

   All root configuration template folders and configuration templates stored at the template folder root level is displayed in the **Configuration Templates** list.

2. Navigate to the folder that contains the configuration template you want to modify.

3. Click the icon 🏛 in the **Operation** field of the configuration template you want to modify.

4. Select **📝 Modify** from the popup menu.

   The **Modify Configuration Template** page appears.

   You cannot modify the name of a configuration template from the **Modify Configuration Template** page. To rename it, you must select the **Rename** option from the **Operation** popup menu. For more information on renaming a configuration template, see "Renaming a configuration template" (page 431).

5. To modify the template type, select the type from the **Template Type** list. Template type options include **File**, **Segment** and **CLI Script**.

   A file template type creates an entire configuration file that is then applied to the device by using the deployment option.

   A segment template type creates only a portion of a configuration field, which is then applied to the device. For example, if your organization uses SNMP community strings that vary by location, you can
create a configuration file by using a segment template type for just the SNMP community string configuration for each location and then deploy that configuration template to devices by location. A CLI script template type creates a CLI configuration file, which is then applied to the device through telnet.

You also cannot modify the folder in which a configuration template is saved once you have created it. To move a configuration file to a new folder, you can copy the configuration template and specify the new folder location from the Copy Configuration Template page. For more information on copying a configuration template, see “Copying a configuration template” (page 431).

6. You can remove devices in the Applicable Devices field by selecting the device you want to delete and clicking on Delete Model.

7. Select the device type you want to create this configuration template for by clicking the Select Model button to the right of the Applicable Devices field. The Device Type dialog box appears.

The Device Type dialog box contains two sections. The Series List section contains a list of all vendor specific devices series in IMC. The top section under Device Type gives you two options for filtering the Series List.

8. Do one of the following:
   - To display the devices series for a specific vendor, select the vendor from the Vendor Name list in the top section of the Device Type dialog box, or
   - To display a specific device series, enter a full or partial device series name in the Series field.

9. Click Query to apply your filter to the Series List.

10. Click the device series name you want to adapt this configuration template to. An expanded list of all device types under the device series name you selected appears.

11. Click the checkbox to the left of the devices in which you want to adapt this configuration template.

12. Click OK.

13. Modify the description for the configuration template in the Description field as needed.

14. Modify the contents of the configuration template in the Content field as needed.

Variables are supported in configuration templates. If you use variables in a configuration template, you are prompted for the variable values when you deploy the configuration template.

The variable format is ${variable name}. For example ${ip address} is a valid variable where ip address is used as the variable name. When you deploy the configuration template, ${ip address} is replaced by the IP address you define.

15. If you select the CLI Script option from the Template Type list, you can modify configuration template commands in the Content field by using a table.

   - Command: Enter the command to be configured.
   - Response Prompt: Response of the command lines.
   - Prompt Condition: Select the response type, ✗ Error Prompt or ✓ Successful Prompt.
   - Action: Click Add to enter another command, and click Delete to delete the corresponding command.

16. Click Change to Advanced Mode link to switch to the advanced mode, and modify the configuration template commands in the Content field.
Any blank spaces before or after variable names are omitted. For example, IMC converts \$\{ \text{paramName} \} to \$\{paramName\}. A variable name cannot include spaces ( ), dollars signs ($) or curly braces ({}).

17. Click OK.

**Renaming a configuration template**

To rename a configuration template

1. Navigate to **Service → Configuration Templates**.
2. Click the **Service** tab from the tabular navigation system on the top.
3. Click the **Configuration Center** on the navigation tree on the left.
4. Click the **Configuration Templates** under **Configuration Center** from the navigation system on the left.
   
   All root configuration template folders and configuration templates stored at the template folder root level is displayed in the **Configuration Templates** list.
5. Navigate to the folder that contains the configuration template you want to rename.
6. Click the icon in the **Operation** field of the configuration template you want to rename.
7. Select **Rename** from the popup menu.
   
   The **Rename** dialog box appears.
8. Enter the new name for the configuration template in the **New Name** field.
   
   Configuration template names cannot begin or end with a period (.). Spaces in the configuration template name are also not permitted. In addition, the characters in Table 23 are not permitted in a configuration template file name.

**Table 23 Invalid characters**

<table>
<thead>
<tr>
<th>Character</th>
<th>Name</th>
<th>Character</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>Asterisk</td>
<td>'</td>
<td>Apostrophe or single quotation</td>
</tr>
<tr>
<td></td>
<td>Vertical bars</td>
<td>:</td>
<td>Colon</td>
</tr>
<tr>
<td>\</td>
<td>Backslash</td>
<td>&quot;</td>
<td>Double quotation</td>
</tr>
<tr>
<td>/</td>
<td>Forward slash</td>
<td>&lt; &gt;</td>
<td>Angle brackets</td>
</tr>
<tr>
<td>?</td>
<td>Question mark</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

9. Click **OK**.

**Copying a configuration template**

Copying a configuration template allows you to re-use and modify an existing configuration template. In addition, the copy option also lets you move an existing configuration template to a new location.

To copy a configuration template:

1. Navigate to **Service → Configuration Templates**.
2. Click the **Service** tab from the tabular navigation system on the top.
3. Click the **Configuration Center** on the navigation tree on the left.
4. Click the **Configuration Templates** under **Configuration Center** from the navigation system on the left.

   All root configuration template folders and configuration templates stored at the template folder root level is displayed in the **Configuration Templates** list.

5. Navigate to the folder that contains the configuration template you want to copy.

6. Click the icon 🔄 in the **Operation** field of the configuration template you want to copy.

7. Select 📋 **Copy** from the popup menu.

   The **Copy Configuration Template** page appears.

8. Modify the name for the template in the **Template Name** field.

   You cannot modify the name of a configuration template from the **Modify Configuration Template** page. To rename it, you must select the **Rename** option from the **Operation** popup menu. For more information on renaming a configuration template, see "Renaming a configuration template" (page 431).

9. Select the type of template you want to create from the **Template Type** list. Template type options include **File**, **Segment** and **CLI Script**.

   A file template type creates an entire configuration file that is then applied to the device by using the deployment option.

   A segment template type creates only a portion of a configuration field, which is then applied to the device. For example, if your organization uses SNMP community strings that vary by location, you can create a configuration file by using a segment template type for just the SNMP community string configuration for each location and then deploy that configuration template to devices by location.

   A CLI script template type creates a CLI configuration file, which is then applied to the device through telnet.

10. To copy, delete, or add devices to a configuration template, do one of the following:

    o Select the folder you want to copy the configuration template to from the **Folder** list, or

    o Select the devices you want to remove in the **Applicable Devices** field and click **Delete Model**, or

    o Click **Select Model** to the right of the **Applicable Devices** field to add devices.

    The **Device Type** dialog box appears, containing two sections:

    The **Series List** section contains a list of all vendor specific device series in IMC.

    The top section under **Device Type** gives you two options for filtering the **Series List**.

11. Do one of the following:

    o To display the devices series for a specific vendor, select the vendor from the **Vendor Name** list in the top section of the **Device Type** dialog box, or

    o To display a specific device series, enter a full or partial device series name in the **Series** field.

12. Click **Query** to apply your filter to the **Series List**.

13. Click the device series name you want to adapt this configuration template to.

   An expanded list of all device types under the device series name you selected appears.

14. Click the checkbox ✅ to the left of the devices in which you want to adapt this configuration template.

15. Click **OK**.

16. Modify the description for the configuration template in the **Description** field as needed.
17. Modify the contents of the configuration template in the **Content** field.
   Variables are supported in configuration templates. If you use variables in a configuration template, you are prompted for the variable values when you deploy the configuration template.
   The variable format is $variable name$. For example ${ip address} is a valid variable where ip address is used as the variable name. When you deploy the configuration template, ${ip address} is replaced by the IP address you define.

18. If you select the **CLI Script** option from the **Template Type** list, you can modify configuration template commands in the **Content** field by using a table.
   - **Command**: Enter the command to be configured.
   - **Response Prompt**: Response of the command lines.
   - **Prompt Condition**: Select the response type, ✗ Error Prompt or ✔ Successful Prompt.
   - **Action**: Click Add to enter another command, and click Delete to delete the corresponding command.

19. Click **Change to Advanced Mode** link to switch to the advanced mode, and modify the configuration template commands in the **Content** field.
   Any blank spaces before or after a variable name is omitted. For example, IMC converts ${paramName} to ${paramName}. A variable name cannot include spaces ( ), dollars signs ($) or curly braces ({}).

20. Click OK.

### Exporting a configuration template

Exporting a configuration template lets you make the contents of an IMC configuration template available for other devices not managed by IMC. IMC exports templates into plain text, which can then be imported as configuration files to other devices.

To export the contents of a configuration template:
1. Navigate to **Service → Configuration Templates**.
2. Click the **Service** tab from the tabular navigation system on the top.
3. Click the **Configuration Center** on the navigation tree on the left.
4. Click the **Configuration Templates** under **Configuration Center** from the navigation system on the left.
   All root configuration template folders and configuration templates stored at the template folder root level is displayed in the **Configuration Templates** list.
5. Navigate to the folder that contains the configuration template you want to export.
6. Click the icon ![Export] in the **Operation** field of the configuration template you want to export.
7. Select ![Export] from the popup menu.
   The **Download Exported Device Configuration** page appears.
8. To save the exported file to your local computer, click the **Download Exported Device Configuration** link.
9. Follow your browser’s instructions for saving the file to your local computer.
Deploying a configuration template

You can launch the Deployment Guide from the Configuration Templates list for deploying the selected configuration template. For information on deploying configurations in IMC, see "Deploying configurations and software by using IMC’s deployment guide" (page 442).

Deleting a configuration template

To delete a configuration template:
1. Navigate to Service→Configuration Templates.
2. Click the Service tab from the tabular navigation system on the top.
3. Click the Configuration Center on the navigation tree on the left.
4. Click the Configuration Templates under Configuration Center from the navigation system on the left.
   
   All root configuration template folders and configuration templates stored at the template folder root level is displayed in the Configuration Templates list.
5. Navigate to the folder that contains the configuration template you want to delete.
6. Click the icon in the Delete field of the configuration template you want to delete.
7. Click OK to confirm deletion of the selected configuration template.

Managing the software library

You can store various system files in IMC for quick and reliable deployment. By using the Software Library feature, you can upload and annotate software, Boot ROM files, web files, OSM software or other file types to IMC. If the filename extension of the imported file complies with standard filename extension conventions (.bin, .web, .app, .zip…), IMC automatically resolves which software files can be downloaded to which devices in the infrastructure. This ensures a successful software deployment to selected devices.

IMC provides two ways to import software. The first method is to upload the software or other file from your local computer. The second method is to import software from a device in the network infrastructure. By using the second method, you can import the software from every device model in the network infrastructure to build a comprehensive software library. By using this in combination with the baseline feature lets you have critical software immediately available for restoration in the event of a failure.

Viewing the software library

To view the software you have imported into IMC’s software library:
1. Navigate to Service→Software Library.
2. Click the Service tab from the tabular navigation system on the top.
3. Click the Configuration Center on the navigation tree on the left.
4. Click the Software Library under Configuration Center from the navigation system on the left.
   
   All files in the software library are displayed in the Software Library list.

Software library list

- Software Name: Contains the name of the software file that has been imported. This field contains a link for navigating to the details for the associated software library entry or imported file.
- **Software Type**: Contains the type of software that the operator assigned to this file when the file was imported. Software type options include *Agent Software, Boot ROM, Web File, OSM Software*, and *Other*.

- **Software Size**: Contains the size in bytes of the associated file.

- **Applicable Devices**: Contains every device series and Object ID auto discovered by IMC that the associated software or other file can be deployed to.

- **Import Time**: Contains the date and time stamp for the successful import of the associated file.

- **Rename**: Contains a link for renaming the associated import file.

- **Modify**: Contains a link for modifying the associated import file entry.

- **Make Baseline**: Contains a link for creating a baseline for the associated import file.

- **Export**: Contains a link for exporting the associated import file.

5. If the **Software Library** list is long enough, the following navigational aids are displayed.

- Click ▶ to page forward in the **Software Library** list.

- Click ▶ to page forward to the end of the **Software Library** list.

- Click ◀ to page backward in the **Software Library** list.

- Click ◀ to page backward to the front of the **Software Library** list.

6. Click 8, 15, 50, 100, or 200 from the right side of the main pane to configure how many items per page you want to view.

7. For **Software Library** list that have more than one page, click 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 … from the bottom right side of the main pane to jump to a particular page of the trap list.

You can sort the **Software Library** by the **Software Name**, **Software Type**, **Software Size**, and **Import Time** fields. Click the column label to sort the list by the selected field. The column label is a toggle switch that lets you toggle between the various sort options specific to each field.

**Viewing the details of a software library entry**

To view the details for an individual software library entry:

1. Navigate to **Service**→**Software Library**→**Software Details**→**<Software Name>**.

2. Click the **Service** tab from the tabular navigation system on the top.

3. Click the **Configuration Center** on the navigation tree on the left.

4. Click the **Software Library** under **Configuration Center** from the navigation system on the left.

   All files in the software library are displayed in the **Software Library** list.

5. Click the link in the **Software Name** field for the import file you want to view details for.

   The **Software Details** page appears.

**Software details**

- **Software Name**: Contains the name of the software file that has been imported.

- **Software Size**: Contains the size in bytes of the associated file.

- **Software Type**: Contains the type of software that the operator assigned to this file when the file was imported. Software type options include *Agent Software, Boot ROM, Web File, OSM Software*, and *Other*.

- **Software Version**: Contains the version of the associated import file or software, if available.
- **Import Time**: Contains the date and time stamp for the successful import of the associated file.
- **Applicable Devices**: Contains every device series auto discovered by IMC that the associated import file can be deployed to.
- **Description**: Contains the description provided by the operator when the file was imported.

**Searching for a software library entry**

You can search for a particular file in the software library. You can search either by a partial or complete file name. IMC displays only those files that match the search criteria.

To search the **Software Library** list:

1. Navigate to **Service → Software Library**.
2. Click the **Service** tab from the tabular navigation system on the top.
3. Click the **Configuration Center** on the navigation tree on the left.
4. Click the **Software Library** under **Configuration Center** from the navigation system on the left.
   
   All files in the software library are displayed in the **Software Library** list.
5. Enter either a portion or the entire software file name you want to locate in the **Software Name** field of the **Query Condition** section.
6. Click **Query** to submit your filter criteria.
   
   The results of your filter or search query is displayed in the **Software Library** list below.
7. Click **Reset** when you want to restore the full **Software Library** list.

**Importing software into the software library from a file**

IMC provides two methods for importing software into the **Software Library**. Software can be uploaded to IMC from a file on your local computer. Or, software can be downloaded from devices in the network infrastructure.

To import software into your software library from a file on your local computer:

1. Navigate to **Service → Software Library**.
2. Click the **Service** tab from the tabular navigation system on the top.
3. Click the **Configuration Center** on the navigation tree on the left.
4. Click the **Software Library** under **Configuration Center** from the navigation system on the left.
   
   All files in the software library are displayed in the **Software Library** list.
5. Click **Add**.
6. Select **Import Software** from the popup menu.
7. Click on the radio button ○ to the left of **Import from File** to import software from your local computer.
8. Select the type of software to import from the **Software Type** list.
9. Enter the file to import, including the full path in the **Select File** field.
10. Optionally, you can browse the file system of your local computer for the file you want to import. To browse, click the **Browse** button to the right of the **Select File** field. Follow the instructions provided by your browser for locating the file.

   IMC auto populates the **Target File** field with the file name. However, you can override this by deleting the contents of the **Target File** field and entering your own file name.
Software file names cannot begin or end with a period (.). Spaces in the configuration template name are also not permitted. In addition, the characters in Table 24 are not permitted in a software file name.

Table 24 Invalid characters

<table>
<thead>
<tr>
<th>Character</th>
<th>Name</th>
<th>Character</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>Asterisk</td>
<td>'</td>
<td>Apostrophe or single quotation</td>
</tr>
<tr>
<td></td>
<td>Vertical bars</td>
<td>:</td>
<td>Colon</td>
</tr>
<tr>
<td>\</td>
<td>Backslash</td>
<td>&quot;</td>
<td>Double quotation</td>
</tr>
<tr>
<td>/</td>
<td>Forward slash</td>
<td>&lt; &gt;</td>
<td>Angle brackets</td>
</tr>
<tr>
<td>?</td>
<td>Question mark</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

11. Enter a description for this software file in the Description field.
12. Click OK to import the file.

**Importing software into the software library from a device**

To import software into your software library from a device:
1. Navigate to Service→Software Library.
2. Click the Service tab from the tabular navigation system on the top.
3. Click the Configuration Center on the navigation tree on the left.
4. Click the 🔄 Software Library under Configuration Center from the navigation system on the left. All files in the software library are displayed in the Software Library list.
5. Click Add.
6. Select Import Software from the popup menu.
7. Click the radio button 🌐 to the left of Import from Device to import software from your local computer.
8. Select the type of software to import from the Software Type list.
9. Select the devices you want to import the software file from by clicking Add Device.
10. Add devices either By View or by Advanced query.
    - You can add devices by using either the View or Advanced query option. See "Adding devices by View" (page 85) and "Adding devices by Advanced query" (page 85).

**Adding OSM software into the software library**

You can add OSM software into the Software Library.

To add OSM software into your software library from a file on your local computer:
1. Navigate to Service→Software Library.
2. Click the Service tab from the tabular navigation system on the top.
3. Click the Configuration Center on the navigation tree on the left.
4. Click the 🔄 Software Library under Configuration Center from the navigation system on the left. All files in the software library are displayed in the Software Library list.
5. Click Add.
6. Select **Add OSM Software** from the popup menu.
   The **Add OSM Software** page appears.

7. Enter a software name for this software file in the **Software Name** field.
   The **Software Name** field lets you set the name of the software file that has been added. Software file names cannot begin or end with a period (.). Spaces in the configuration template name are also not permitted. In addition, the characters in Table 25 are not permitted in a software file name.

**Table 25 Invalid characters**

<table>
<thead>
<tr>
<th>Character</th>
<th>Name</th>
<th>Character</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>Asterisk</td>
<td>'</td>
<td>Apostrophe or single quotation</td>
</tr>
<tr>
<td></td>
<td>Vertical bars</td>
<td>:</td>
<td>Colon</td>
</tr>
<tr>
<td>\</td>
<td>Backslash</td>
<td>&quot;</td>
<td>Double quotation</td>
</tr>
<tr>
<td>/</td>
<td>Forward slash</td>
<td>&lt; &gt;</td>
<td>Angle brackets</td>
</tr>
<tr>
<td>?</td>
<td>Question mark</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

8. Select the type of software you want to import from the **Software Type** list. **OSM Software** is selected by default.

9. Enter a description for this software file in the **Description** field.

10. Enter the IP address of the FTP server where the OSM software is located in the **FTP Server** field. Server name is not supported here.

11. Enter the file path of the OSM software on the FTP server in the **Software Path** field.

12. Enter the username for logging in to the FTP server in the **FTP User** field.

13. Enter the password for logging in to the FTP server in the **FTP User** field.

14. Click **OK** to add the OSM software.

**Renaming a software library entry**

To rename an entry in your software library:

1. Navigate to **Service→Software Library**.
2. Click the **Service** tab from the tabular navigation system on the top.
3. Click the **Configuration Center** on the navigation tree on the left.
4. Click the **Software Library** under **Configuration Center** from the navigation system on the left. All files in the software library are displayed in the **Software Library** list.
5. Click the icon in the **Rename** field of the software file you want to rename. The **Rename Software** dialog box appears.
6. Delete the existing name and enter the new name in the **New Name** field. Software file names cannot begin or end with a period (.). Spaces in the configuration template name are also not permitted. In addition, the characters in Table 26 are not permitted in a software file name.
Table 26 Invalid characters

<table>
<thead>
<tr>
<th>Character</th>
<th>Name</th>
<th>Character</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>Asterisk</td>
<td>'</td>
<td>Apostrophe or single quotation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>:</td>
<td>Colon</td>
</tr>
<tr>
<td>\</td>
<td>Backslash</td>
<td>&quot;</td>
<td>Double quotation</td>
</tr>
<tr>
<td>/</td>
<td>Forward slash</td>
<td>&lt; &gt;</td>
<td>Angle brackets</td>
</tr>
<tr>
<td>?</td>
<td>Question mark</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

7. Click OK.

Modifying a software library entry

To modify an existing entry in your software library:

1. Navigate to Service→Software Library→Modify Software Information→<Software Name>.
2. Click the Service tab from the tabular navigation system on the top.
3. Click the Configuration Center on the navigation tree on the left.
4. Click the Software Library under Configuration Center from the navigation system on the left. All files in the software library are displayed in the Software Library list.
5. Click the icon in the Modify field of the software file you want to modify.
6. The Software Details page appears.

To delete device series or models from the Applicable Devices field, click the device series you want to delete.

7. Click Delete Model.
8. To add new device series or models to the Applicable Devices list, click Select Model.

The Device Model dialog box appears.

The Device Model dialog box contains two sections. The Series List section contains a list of all vendor specific devices series in IMC.

The top section under Device Model gives you two options for filtering the Series List.

9. Do one of the following:
   - To display a device series for a specific vendor, select the vendor from the Vendor Name list in the top section of the Device Model dialog box, or
   - To display a specific device series, enter a full or partial device series name in the Series field.

10. Click Query to apply the filter to the Series List.
11. Click the device series name you want to add to the Applicable Devices list. An expanded list of all device types under the device series name you selected appears.
12. Click the checkbox to the left of the devices you want to add.
13. Modify the description in the Description field as needed.
14. Click OK.
Exporting a software library entry

To export an entry in your software library:

1. Navigate to Service→Software Library→Export Software→<Software Name>.
2. Click the Service tab from the tabular navigation system on the top.
3. Click the Configuration Center on the navigation tree on the left.
4. Click the Software Library under Configuration Center from the navigation system on the left. All files in the software library are displayed in the Software Library list.
5. Click the icon  in the Export field of the software file you want to export. The Download Exported Software page appears.
6. To save the exported file to your local computer, click the Download Exported Software link.
7. Follow your browser’s instructions for opening or saving the file to your local computer.

Deleting a software library entry

To delete one or more entries from your software library:

1. Navigate to Service→Software Library.
2. Click the Service tab from the tabular navigation system on the top.
3. Click Configuration Center on the navigation tree on the left.
4. Click Software Library under Configuration Center from the navigation system on the left. All files in the software library are displayed in the Software Library list.
5. Click the checkbox ☑ to the left of the software library entry you want to delete.
6. Click Delete.
7. Click OK to confirm the deletion of the selected software library entry.

Establishing baselines by using a software library entry

You can define an entry in the software library as the baseline for one or more devices or device models.

To establish a software file as a baseline for one or more devices:

1. Navigate to Service→Software Library.
2. Click the Service tab from the tabular navigation system on the top.
3. Click Configuration Center on the navigation tree on the left.
4. Click Software Library under Configuration Center from the navigation system on the left. All files in the software library are displayed in the Software Library list.
5. Click the icon  in the Make Baseline field of the software file you want to establish as a baseline, and select Single Device or Device Model.
6. If you want to define a software file as the baseline for one or more devices, select Single Device. The Select the baseline software and device page appears. Go to Step 8.
7. If you want to define a software file as the baseline for one or more device models, select Device Model. The Select the baseline software and device model page appears. Go to Step 5. The Device Software field is populated by the software file name you selected in Step 2.
8. Do one of the following:
   - If you want to select another software file, click Select located to the right of the Device Software field, or
   - If you want to use the current software file, go to Step 12.
9. After clicking Select, the Select Software dialog box appears.
10. Click the radio button ☐ to the left of the software file you want to establish as a baseline.
11. Click OK.
12. Select the devices on which you want to establish a baseline by using the software file you have selected.
13. Click Select Device. The Select Device dialog box appears.
14. Add devices by using either the View or Advanced query option. See "Adding devices by View" (page 85) and "Adding devices by Advanced query" (page 85).

Comparing device configurations

You can compare the contents of configuration files. You can compare backup startup or running configuration files with the current startup or running configuration files. IMC also provides a line-by-line comparison of the two files with the differences highlighted. In addition, IMC provides a summary of identical, changed, and unique lines. You can enter the page for comparing device configurations as explained in the following sections.

Configuration Center

To use the configuration center to compare device configurations:

1. Navigate to Service→Configuration Center.
2. Click the Service tab from the tabular navigation system on the top.
3. Click the Configuration Center on the navigation tree on the left.
4. Click the Configuration Center icon located under Configuration Center from the navigation system on the left.
   
   All devices that can be managed by the Configuration Center are displayed in the list in the bottom half of the Configuration Center page.
5. Click the icon in the Operation field of the device you want to compare a file with.
6. Select Compare with Other Device Configuration from the popup menu.
   
   The General Configuration Compare page appears. This page lets you configure the two files you want to compare. The first file is displayed on the left side of the results page and the second file is displayed on the right.

Configuring the first or left configuration file

- Left Device: Display the name of the device that you want to compare on the left of the page.
- Stack Unit: If prompted, select the unit you want to use as a source for a configuration file from the Stack Unit list.
- File Type: Select the type of configuration file you want to use for comparison from the File Type list.
Configuration File: If you selected Backup History as your file type, select the particular configuration file you want to compare from the Configuration File list.

Configuring the second or right configuration file

1. Select the second configuration file to display on the right by configuring the following:
   - Right Device: Display the name of the device that you want to compare on the right of the page. Click Select Device. The Select Device dialog box appears.

2. Add devices either By View or by Advanced query by using either the View or Advanced query option. See “Adding devices by View” (page 85) and “Adding devices by Advanced query” (page 85).

General configuration compare

To use the configuration compare to compare device configurations:

1. Navigate to Service→General Configuration Compare.
2. Click the Service tab from the tabular navigation system on the top.
3. Click the Configuration Center on the navigation tree on the left.
4. Click the Configuration Compare under Configuration Center from the navigation system on the left.
   The General Configuration Compare page appears. This page lets you configure the two files you want to compare. The first file is displayed on the left side of the results page and the second file is displayed on the right.
5. Select devices.
6. Click Select Device.
   The Select Device dialog box appears.
7. Add devices either By View or by Advanced query. "Adding devices by View" (page 85) and "Adding devices by Advanced query" (page 85).

Deploying configurations and software by using IMC’s deployment guide

IMC’s Deployment Guide is a step-by-step guide for successfully deploying device configurations and software. The Deployment Guide provides a facility for deploying device configurations by using the configuration templates you have created. When deploying configuration files, IMC evaluates the configuration template against every device selected for deployment to ensure that the template can be deployed successfully. IMC identifies when devices do not match the configuration template. By using the Deployment Guide you can also restore device configurations.

You can also deploy system software and other files uploaded to the software library. With the Deployment Guide, you can deploy software from the Software Library to one or more devices. With software deployments, IMC performs two checks. The first check evaluates whether or not the system software matches the devices current system software and identifies whether or not the software should be deployed to the devices. With the second check, IMC verifies that there is enough device space to deploy the selected software by using the deployment strategy that you have configured. By using the Deployment Guide you can also restore system software should the need arise.
Deploying a device configuration

The Deployment Guide lets you deploy the device configurations they have created by using configuration templates. IMC validates the viability of deploying configurations to every device selected for deployment and identifies when a configuration cannot be deployed to a device. In addition, you can run deployments immediately or schedule deployments for a later date.

To deploy device configuration to a selected device:

1. Navigate to Service → Deployment Guide.
2. Click the Service tab from the tabular navigation system on the top.
3. Click Configuration Center on the navigation tree on the left.
4. Click Deployment Guide under Configuration Center from the navigation system on the left.
5. Click the Deploy Configuration link from the Select a Deployment Task section of the Deployment Guide page.
6. Select the configuration template folder that contains the configuration file you want to deploy from the Folder list of the Select Configuration Template section of the Select Device for Update page.
7. Select the configuration template you want to deploy from the Template Name list.
8. Select the devices you want to update by using the selected configuration file by clicking Select Device.
9. Add devices By View or by Advanced query. See "Adding devices by View" (page 85) and "Adding devices by Advanced query" (page 85).

Deploying software

You can deploy system software to devices by using the Deployment Guide’s step-by-step software deployment wizard. This wizard includes several checkpoints to ensure the successful deployment of software to selected devices.

To deploy software by using IMC’s Deployment Guide, the software to be deployed must first exist in the software library. For more information on uploading files to IMC’s software library, see "Managing the software library" (page 434).

To deploy system software:

1. Navigate to Service → Deployment Guide.
2. Click the Service tab from the tabular navigation system on the top.
3. Click Configuration Center on the navigation tree on the left.
4. Click Deployment Guide under Configuration Center from the navigation system on the left.
5. Click the Deploy Software link from the Select a Deployment Task section of the Deployment Guide page.
6. To select the software you want to deploy, click Select to the right of the Software field in the Select Deployed Software section of the page.
   The Choose Software dialog box appears.
7. Select the software file you want to deploy by clicking the radio button to the left of the software filename you want to deploy.
8. Click OK.

The software file must exist in IMC’s software library before you can deploy it. To upload files to the
software library, see "Managing the software library" (page 434).

The Applicable Devices field of the Software List displays all device models that are supported by the
associated file. Review the Applicable Devices information before selecting the devices in which you
plan to deploy the selected software.

9. To select the Boot ROM you want to deploy, click Select to the right of the Boot ROM field.

The Choose Boot ROM dialog box appears.

10. Select the Boot ROM version you want to deploy by clicking the radio button  to the left of the Boot
ROM file name you want to deploy.

11. Click OK.

12. To select the devices to which the software or Boot ROM file is deployed, click the Select Device
button located in the Devices for Deployment section of the page.

The Select Devices dialog box appears.

13. Add devices either By View or by using the Advanced query option. See "Adding devices by View"
(page 85) and "Adding devices by Advanced query" (page 85).

Deploying a file

You can deploy other file types to selected devices. As with deployments for system software, the Deployment
Guide provides a step-by-step wizard for configuring the deployment of the selected file. This wizard also
includes several checkpoints to ensure the successful deployment of the selected file.

To deploy files by using IMC’s Deployment Guide, the file to be deployed must already exist in the software
library. For more information on uploading files to IMC’s software library, see "Managing the software
library" (page 434).

1. Navigate to Service—Deployment Guide.
2. Click the Service tab from the tabular navigation system on the top.
3. Click Configuration Center on the navigation tree on the left.
4. Click Deployment Guide under Configuration Center from the navigation system on the left.
5. Click the Deploy File (Other Files) link from the Select a Deployment Task section of the Deployment
Guide page.
6. To select the file you want to deploy, click Select to the right of the Device Software field in the Select
the file and device section of the page.

The Select Software dialog box appears.
7. Select the software file you want to deploy by clicking the radio button  to the left of the software
filename you want to deploy.
8. Click OK.

The software file must exist in the software library before you can deploy it. To upload files to IMC’s
software library, see "Managing the software library" (page 434).
9. To select the devices to which the file is deployed, click the Select Device button located in the Device
List section of the page.

The Select Devices dialog box appears.
10. Add devices either By View or by using the Advanced query option. See "Adding devices by View" (page 85) and "Adding devices by Advanced query" (page 85).

Restoring a device configuration

IMC's Deployment Guide also provides a step-by-step wizard for restoring a device’s configuration.

To restore configuration files:
1. Navigate to Service→Deployment Guide.
2. Click the Service tab from the tabular navigation system on the top.
3. Click Configuration Center on the navigation tree on the left.
4. Click Deployment Guide under Configuration Center from the navigation system on the left.
5. Click the Restore Device Configuration link from the Select a Deployment Task section of the Deployment Guide page.
6. To select the devices you want to restore a configuration file to, click Select Device. The Select Devices dialog box appears.
7. Add devices either By View or by using the Advanced query option. See "Adding devices by View" (page 85) and "Adding devices by Advanced query" (page 85).

Restoring device software


To restore system software:
1. Navigate to Service→Deployment Guide.
2. Click the Service tab from the tabular navigation system on the top.
3. Click Configuration Center on the navigation tree on the left.
4. Click Deployment Guide under Configuration Center from the navigation system on the left.
5. Click the Restore Device Software link from the Select a Deployment Task section of the Deployment Guide page.
   The Select the Device for Update and the Software Version page of the deployment wizard appears.
6. To select the devices to which software is deployed, click on the Select Device located in the Devices for Deployment section of the page.
   The Select Devices dialog box appears.
7. Add devices either By View or by using the Advanced query option. See "Adding devices by View" (page 85) and "Adding devices by Advanced query" (page 85).

Deploying OSM software

You can deploy the OSM software to devices by using a step-by-step software deployment wizard of the Deployment Guide. This wizard includes several checkpoints to ensure the successful deployment of software to selected devices.

To deploy OSM software by using IMC's Deployment Guide, the OSM software to be deployed must first exist in IMC's software library. For more information on uploading files to IMC's software library, see "Managing the software library" (page 434).
To deploy OSM software to selected devices:

1. Navigate to Service→Deployment Guide.
2. Click the Service tab from the tabular navigation system on the top.
3. Click Configuration Center on the navigation tree on the left.
4. Click Deployment Guide under Configuration Center from the navigation system on the left.
5. Click the Deploy OSM Software link from the Select a Deployment Task section of the Deployment Guide page.
6. To select the software you want to deploy, click Select to the right of the OSM Software field in the Select Deployed Software section of the page.
   The Choose Software dialog box appears.
7. Select the software file you want to deploy by clicking the radio button to the left of the software filename you want to deploy.
8. Click OK.
   The OSM software file must exist in IMC’s software library before you can deploy it. To upload files to IMC’s software library, see “Managing the software library” (page 434).
   The Applicable Devices field of the Software List displays all device models that are supported by the associated file. Review the Applicable Devices information before selecting the devices that you plan to deploy the selected software to.
9. To select the devices to which the OSM software is deployed, click the Select Device button located in the Devices for Deployment section of the page.
   The Select Devices dialog box appears.
10. Add devices either By View or by using the Advanced query option. See “Adding devices by View” (page 85) and “Adding devices by Advanced query” (page 85).

Managing deployment tasks

The Deployment Task management feature provides visibility into the status of configuration and software deployment tasks in IMC. Through the Deployment Task portal, you can view the current status of configuration and software deployments submitted by using the Deployment Guide. From the Deployment Task portal, you can drill down into the step-by-step details for every device in a deployment task and identify which devices failed a deployment and why.

From the same portal, you can suspend and resume configuration and software deployments and re-run failed or partially successful deployment tasks. From the same Deployment Task page, you can also modify a failed or partially successful deployment task and re-run it.

Lastly, you can copy a deployment task, make changes to it and resubmit it to the deployment task list.

Accessing the deployment task list

To navigate to the Deployment Task List:

1. Navigate to Service→Deployment Task.
2. Click the Service tab from the tabular navigation system on the top.
3. Click Configuration tab on the navigation tree on the left.
4. Click Deployment Task under Configuration Center from the navigation system on the left.
The Deployment Task page appears. All deployment tasks are displayed in the list in the bottom half of the Deployment Task page.

Deployment task list

- **Status—Operation Result**: Contains the results of the deployment task. The contents of this field serve as a link to the View Execution Result page for the associated deployment task. For more information on the View Execution Result page, see the section describing the Execution Result Page in this manual.

- **Task Name**: Contains the name of the deployment task. The contents of this field serve as a link to the View Task Detail Information page. The View Task Detail Information page provides details for the associated deployment task including basic task information, the deployment strategy and the devices configured in the deployment task.

You can configure the task name when using the Deployment Guide to deploy a configuration or software file. Otherwise, IMC provides a default task name that includes a date and time stamp for uniquely identifying deployment tasks.

- **Task Sub Type**: Identifies what type of deployment task was executed. Options include Deploy Device Configuration, Deploy Software, Deploy File, Restore Device Configuration from NMS, Restore Device Configuration from Device, and Restore Software.

- **Schedule Type**: Identifies whether or not the deployment task is a recurring or cyclical task or a task that was run once.

- **Creator**: Identifies the creator of the deployment task.

- **Last Begin Time**: Contains the date and time stamp of the start time of the associated deployment task’s execution.

- **Next Begin Time**: Contains the date and time stamp of the start time of the associated deployment task’s next cycle of execution. This field is blank if the Schedule Type is Once.

- **Modify**. IMC lets you modify the attributes of a deployment task for those tasks that have the status “For Executing”. This field contains an icon for navigating to the page for modifying the associated task.

- **Copy**: Contains an icon for navigating to the page for copying the associated task.

You can sort the Deployment Task List by the Status—Operation Result, Task Name, Task Sub Type, Schedule Type, Creator, Last Begin Time, and Next Begin Time fields. Click the column label to sort the list by the selected field. The column label is a toggle switch that lets you toggle between the various sort options specific to each field.

If the Deployment Task List contains enough entries, the following navigational aids are displayed.

- Click to page forward in the Deployment Task List.

- Click to page forward to the end of the Deployment Task List.

- Click to page backward in the Deployment Task List.

- Click to page backward to the front of the Deployment Task List.

5. Click 8, 15, 50, 100, or 200 from the right side of the main pane to configure how many items per page you want to view.

**Searching for a deployment task**

IMC provides the ability to search for a particular deployment task from the Deployment Task page.
To search the Deployment Task List:

1. Navigate to Service→Deployment Task.
2. Click the Service tab from the tabular navigation system on the top.
3. Click the Configuration Center on the navigation tree on the left.
4. Click the Deployment Task under Configuration Center from the navigation system on the left.
   
The Deployment Task page appears. The query conditions for searching the Deployment Task List are displayed in the upper portion of this page.
5. Enter one or more of the following search criteria in the Query Condition section of the page:
   - Task Type: Select the task type from the Task Type list.
   - Task Sub Type: Select the task sub type from the Task Sub Type list.
   - Task Status: Select the task status from the Task Status list.
   - Operation Result: Select the operation result you want to search for from the Operation Result list.
6. Click Query to submit your filter criteria.
   
The results of your filter or search query are displayed in the Deployment Task List below.
7. Click Reset when you want to restore the full Deployment Task List.

Viewing execution result page

IMC displays the deployment task results for every device configured in the task in the Execution Result page. This page provides the cause of deployment failures and information for each step in the deployment process for every device.

To view the results for a deployment task:

1. Navigate to Service→Deployment Task.
2. Click the Service tab from the tabular navigation system on the top.
3. Click the Configuration Center on the navigation tree on the left.
4. Click the Deployment Task under Configuration Center from the navigation system on the left.
   
The Deployment Task page appears. All deployment tasks are displayed in the list in the bottom half of the Deployment Task page.
5. Click the Status--Operation Result link for the deployment task you want to view results for.
   
The View Execution Result page appears. All deployment tasks are displayed in the list in the bottom half of the Deployment Task page.

Execution Results

- Device Name: Contains the name of the device to which a deployment was executed.
- Start Time on Device: Contains the start time of the deployment task.
- End Time on Device: Contains the end time of the deployment task.
- Execution Status: Identifies whether or not the deployment task has been completed.
- Operation Result: Identifies whether or not the deployment to the associated device was successful.
- Details: Contains a link for viewing the details for every step in the deployment process for the associated device. The Details page provides information on failures in the deployment process.
- View Change: Contains a link for comparing the changes that were made to the associated device.
On the Select Device for Update page that is used to deploy device configurations, if you selected Running Configuration in the File Type to be Deployed field, the following options are displayed. Click the checkbox to the left of the View the change before and after deployment option. After the deployment task is complete, you see View Change in the View Execution Result page.

Modifying a deployment task

By using the Modify option of the Deployment Task page, you can change the parameters of failed or partially successful deployment task and resubmit it to the deployment task queue for processing.

To modify a deployment task:

1. Navigate to Service→Deployment Task.
2. Click the Service tab from the tabular navigation system on the top.
3. Click the Configuration Center on the navigation tree on the left.
4. Click the Deployment Task under Configuration Center from the navigation system on the left.
   The Deployment Task page appears. The query conditions for searching the Deployment Task List are displayed in the upper portion of this page.
5. Click the icon in the Modify field of the deployment task you want to modify.
6. Select the type of deployment schedule you want to apply to this task from the Schedule Type list. Options include Once and Cycle. Select Once if you want IMC to execute this task one time. Select Cycle if you want this configuration deployment task to be executed on a scheduled basis.
7. If you selected Once in the Schedule Type field, complete the following steps:
   a. Select the time you want IMC to execute this task from the Schedule Time list. Options include Immediately and Scheduled. If you selected Immediately, go to Step 18.
   b. If you selected Scheduled, click on the calendar icon to populate the date and time for the execution of this task. A popup calendar appears. Select the date from the calendar.
   c. Go to Step 18.
   d. If you selected Cycle from the Schedule Type list, complete the following steps.
   e. Select the frequency with which you want IMC to execute this task from the Operation Frequency list.
   f. If you selected Every Week from the Operation Frequency list, select the date of the week you want IMC to execute this task from the list to the right of the Operation Frequency list.
   g. If you selected Every Month from the Operation Frequency list, select the day of the month you want IMC to execute this task from the list to the right of the Operation Frequency list.
8. Enter the time you want IMC to execute this task in the Operation Frequency list. Enter the time in HH:MM:SS format where HH denotes a two digit hour value, MM denotes a two digit minute value and SS denotes a two digit second value.
9. Enter the beginning date and time you want IMC to execute this task in the Start Time field. Click the calendar icon to populate the date and time for the execution of this task. A popup calendar appears. Select the start date from the calendar.
10. Enter the ending date and time you want IMC to execute this task in the End Time field. Click the calendar icon to populate the date and time for the execution of this task. A popup calendar appears. Select the end date from the calendar.
11. Select how you want IMC to execute the deployment of configuration files to every device in the deployment task from the Schedule Sequence list. Two options are available: Concurrent and
Sequential. If you select Concurrent, IMC executes the deployment to multiple devices simultaneously. If you select Sequential, IMC deploys the configuration file to one device at a time.

12. If you select Sequential from the Schedule Sequence list, you can also define the order in which IMC uses to deploy the selected configuration file or segment as follows.

13. Click Sort located to the right of the Schedule Sequence list. The Sort dialog box appears.

14. Click the checkbox ☐ to the left of the devices you want to move.

15. Do one of the following:
   - Click Up to move the devices up in the list, or
   - Click Down to move the devices down in the list.

16. Do one of the following:
   - Click Top to move the devices to the top of the list, or
   - Click Bottom to move the device to the bottom of the list.

17. Click OK when you have finished sorting the devices in the list.

18. If you selected Sequential from the Schedule Sequence list, you can also define how you want IMC to handle errors that arise in the deployment process. If you want IMC to abandon the deployment for all devices if an error arises during deployment, select Stop Deployments on All Devices from the Error Handling list. If you want IMC to abandon deployment for the device IMC is currently deploying the configuration file or segment to, select Stop Deployment on the Current Device from the Error Handling list.

19. Modify the description for this deployment task in the Task Description field.

20. Click OK to accept your changes to the deployment task.

The page is updated to display the Deployment Task page. The Deployment Task List displayed on this page contains the modified deployment task you just submitted.

Review the Status--Operation Result field for a status update on the deployment task you submitted. The contents of the Status--Operation Result field serve as a link to the View Execution Result page, which provides per device details.

The View Execution Result page contains details about the deployment task for every device. For deployment tasks that failed or were partially successful, click the Status--Operation Result link to view the View Execution Result details that include causes for deployment failures.

21. Click Refresh to refresh the page with a new status update.

Copying a deployment task

The copy option lets you leverage the existing configuration of a deployment task and make any changes to it through the Deployment Guide before resubmitting it to the Deployment Task List. For more information on using the Deployment Guide to configure deployment tasks, see “Deploying configurations and software by using IMC’s deployment guide” (page 442).

Running a deployment task

You can re-run deployment tasks that failed or have been suspended.

To re-run a failed or suspended deployment task:

1. Navigate to Service→Deployment Task.
2. Click the Service tab from the tabular navigation system on the top.
3. Click the **Configuration Center** on the navigation tree on the left.
4. Click the **Deployment Task** under **Configuration Center** from the navigation system on the left. The **Deployment Task** page appears. The query conditions for searching the **Deployment Task List** are displayed in the upper portion of this page.
5. Click the checkbox to the left of the deployment task you want to run.
6. Click **Run**.
   The **Deployment Task** page is updated to reflect the results of the deployment task.
7. Click **Refresh** to refresh the page with a new status update.
8. Review the **Status--Operation Result** field for a status update on the deployment task you submitted. The contents of the **Status--Operation Result** field serve as a link to the **View Execution Result** page. The **View Execution Result** page contains details about the deployment task for every device. For deployment tasks that failed or were partially successful, click the **Status-Operation Result** link to view the **View Execution Result** details that include causes for deployment failures.

### Suspending a deployment task

IMC provides you with the ability to suspend a deployment task that is in progress.

To suspend a deployment task that is in progress:
1. Navigate to **Service**→**Deployment Task**.
2. Click the **Service** tab from the tabular navigation system on the top.
3. Click the **Configuration Center** on the navigation tree on the left.
4. Click the **Deployment Task** under **Configuration Center** from the navigation system on the left. The **Deployment Task** page appears. The query conditions for searching the **Deployment Task List** are displayed in the upper portion of this page.
5. Click the checkbox to the left of the deployment task you want to suspend. Deployment tasks that are in progress contain the **Executing--Unknown** in the **Status--Operation Result** field.
6. Click **Suspend**.
   The **Status--Operation Result** field is updated to include the status **Suspended--Unknown**.
7. To complete the task, use the resume feature.

### Resuming a deployment task

IMC provides you with the ability to resume a suspended deployment task.

To resume a suspended deployment task:
1. Navigate to **Service**→**Deployment Task**.
2. Click the **Service** tab from the tabular navigation system on the top.
3. Click the **Configuration Center** on the navigation tree on the left.
4. Click the **Deployment Task** under **Configuration Center** from the navigation system on the left. The **Deployment Task** page appears. The query conditions for searching the **Deployment Task List** are displayed in the upper portion of this page.
5. Click the checkbox to the left of the deployment task you want to resume. Deployment tasks that have been suspended contain Suspended→Unknown in the Status→Operation Result field of the associated deployment task.

6. Click Resume.

   The Status→Operation Result field is updated to include the status Executing→Unknown.

7. Click Refresh to refresh the page with a new status update.

8. Review the Status→Operation Result field for a status update on the deployment task you submitted. The contents of the Status→Operation Result field serve as a link to the View Execution Result page.

   The View Execution Result page contains details about the deployment task for every device. For deployment tasks that failed or were partially successful, click the Status→Operation Result link to view the View Execution Results details that include causes for deployment failures.

Deleting a deployment task

You can also delete a task from the Deployment Task List.

To delete a deployment task from the Deployment Task List:

1. Navigate to Service→Deployment Task:
   a. Click the Service tab from the tabular navigation system on the top.
   b. Click the Configuration Center on the navigation tree on the left.
   c. Click the Deployment Task under Configuration Center from the navigation system on the left.

   The Deployment Task page appears. The query conditions for searching the Deployment Task List are displayed in the upper portion of this page.

2. Click the checkbox to the left of the deployment tasks you want to delete.

3. Click Delete.

4. Click OK to confirm deletion of the selected deployment tasks.

   The Deployment Task page is updated to reflect the status of the deletion request. Review the results to ensure the successful removal of deployment tasks.

Managing automatic deployment plans

IMC provides a facility for automatic executions of software upgrade, startup configuration deployment, CLI script execution, and configuration backup for devices with zero or simple configurations. With the Auto Deployment Plan feature, you can quickly configure devices in batch to operate properly without manual intervention.

An auto deployment plan is a set of automatic deployment operations that the network administrator defines for devices according to the network plan. IMC displays automatic deployment plans in a nested table. The external table shows information about each automatic deployment plan, including the plan name, creator, creation time, and the execution status of each device in the plan. The internal table shows information about automatic deployment devices, including the MAC address, current IP address, target IP address, mask, and operating status. As for automatic deployment plans,

IMC provides the functions of adding, deleting, modifying, and viewing automatic deployment plans. As for automatic deployment devices, IMC provides the functions of adding, deleting, modifying, viewing, and importing automatic deployment devices, triggering deployment, and viewing automatic deployment execution results.
An initial configuration file in IMC is deployed on a zero-configuration device through DHCP after the device is powered on. The initial configuration file must contain basic SNMP and Telnet parameters. After the zero-configuration device executes the initial configuration file, IMC automatically adds the device through auto discovery and apply a pre-configured automatic deployment plan to it.

Automatic deployment plans can be triggered for the following devices:

- Zero-configuration devices that are powered on and automatically added to IMC. Before powering on a zero-configuration device, the network administrator must configure on the DHCP server the address pool, gateway, DNS server, domain name, TFTP server for IMC, initial configuration file name, and timeout period.
- Simple-configuration devices that were not managed by IMC and are now added to IMC manually or through auto discovery.
- Simple-configuration devices that have been added to IMC.

**NOTE:**
Only operators with administrative level privileges can manage automatic deployment plans.

**Automatic deployment plan management**

With the Auto Deployment Plan feature, you can schedule configuration files and software to be automatically deployed on one or more devices.

**Accessing the automatic deployment plan page**

IMC provides a list of all automatic deployment plans in the Auto Deployment Plan page, in which you can add, view, modify, or delete automatic deployment tasks.

To access the page of automatic deployment plans:

1. Navigate to Service→Auto Deployment Plan.
2. Click the Service tab from the tabular navigation system on the top.
3. Click the Configuration Center on the navigation tree on the left.
4. Click the Auto Deployment Plan under Configuration Center from the navigation system on the left.

All existing automatic or scheduled deployment plans is displayed in the Auto Deployment Plan page.

**Auto Deployment Plan**

- **Created by:** Identifies person who created the deployment plan.
- **Created at:** Displays when the deployment plan was created.
- **Being Executed:** Displays the number of devices on which the deployment plan is being executed.
- **Not Executed:** Displays the number of devices on which the deployment plan has not been executed.
- **Successfully Deployed:** Displays the number of devices on which the deployment plan has been successfully executed.
- **Failures:** Displays the number of devices on which the deployment plan failed to be executed.
- **Operation:** Contains the following icons for managing the deployment plan:
  - This icon adds devices for the deployment plan.
  - This icon imports devices for the deployment plan.
This icon views the execution result of the deployment plan.
This icon modifies basic information for the deployment plan.
This icon deletes the deployment plan.

5. Click the icon with the deployment plan you want to expand.
   All existing devices in the deployment plan are displayed.

**Automatic deployment device list**
- **MAC Address**: displays the MAC address of the device.
- **Current IP Address**: displays the current IP address of the device.
- **Target IP Address/Mask**: displays the IP address and mask of the device after the deployment plan is successfully executed on it.
- **Running Status**: Contains the execution result of the deployment plan on the device.
- **Operation**: Contains the following icons for managing the deployment device:
  - This icon modifies the deployment information for the device.
  - This icon views detailed information about the deployment plan on the device.
  - This icon views the execution result of the deployment plan on the device.
  - This icon manually triggers a deployment plan on the device.
  - This icon deletes the device.

**Adding an automatic deployment plan**

To add an automatic deployment plan:
1. Navigate to **Service → Auto Deployment Plan**.
2. Click the **Service** tab from the tabular navigation system on the top.
3. Click the **Configuration Center** on the navigation tree on the left.
4. Click the **Auto Deployment Plan** under **Configuration Center** from the navigation system on the left.
   All existing automatic or scheduled deployment plans is displayed in the **Auto Deployment Plan** page.
5. Click **Add**.
   The **Auto Deployment Plan** dialog box appears.
6. Enter a unique name for this deployment plan in the **Name** field.
   Valid name length is 1–32 characters.
7. Enter a brief description for this deployment plan in the **Description** field.
   Valid description length is 0–128 characters.
8. Click **OK** to accept your deployment plan configuration.
   Review the results of the add operation in the **Auto Deployment Plan** page.

**Modifying an automatic deployment plan**

To modify an existing automatic deployment plan:
1. Navigate to **Service → Auto Deployment Plan**.
2. Click the **Service** tab from the tabular navigation system on the top.
3. Click **Configuration Center** on the navigation tree on the left.

4. Click **Auto Deployment Plan** under **Configuration Center** from the navigation system on the left. All existing automatic deployment plans is displayed in the **Auto Deployment Plan** page.

5. Click the icon **⪿** in the **Operation** field associated with the deployment plan you want to modify. The **Auto Deployment Plan** dialog box appears.

   You cannot modify the name of a deployment plan once you have created it. You must delete the existing deployment plan and create a new deployment plan with the new name.

6. Modify the description for this deployment plan in the **Description** field.

   Valid description length is 0–128 characters.

7. Click **OK** to accept your deployment plan configuration changes.

8. Review the results of the modify operation in the **Auto Deployment Plan** page.

### Deleting an automatic deployment plan

To delete an existing automatic deployment plan:

1. Navigate to **Service→Auto Deployment Plan**.
2. Click the **Service** tab from the tabular navigation system on the top.
3. Click the **Configuration Center** on the navigation tree on the left.
4. Click the **Auto Deployment Plan** under **Configuration Center** from the navigation system on the left. All existing automatic deployment plans is displayed in the **Auto Deployment Plan** page.
5. Click the icon **𝕏** in the **Operation** field associated with the deployment plan you want to delete.

   You cannot delete an automatic deployment plan containing devices on which automatic deployment is being executed.

6. Click **OK** to confirm deletion of the deployment plan.

7. Review the results of the delete operation in the **Auto Deployment Plan** page.

### Viewing detailed information about an automatic deployment device

To view detailed information about an automatic deployment device in the existing automatic deployment plan:

1. Navigate to **Service→Auto Deployment Plan**.
2. Click the **Service** tab from the tabular navigation system on the top.
3. Click the **Configuration Center** on the navigation tree on the left.
4. Click the **Auto Deployment Plan** under **Configuration Center** from the navigation system on the left. All existing automatic deployment plans are displayed in the **Auto Deployment Plan** page.
5. Click the icon **🗂** with the deployment plan you want to expand.

   All existing devices in the deployment plan appear.

6. Click the icon **🗂** in the **Operation** field associated with the device you want to view.

   The **Auto Deployment Device** dialog box is displayed, and shows detailed information about the automatic deployment device, including the configuration file to deploy, software to deploy, CLI script, device basic information, device information, and access parameters.
Adding an automatic deployment device

You can configure the following parameters on the device to which an automatic deployment device is deployed: configuration file to deploy, software to deploy, CLI script, device information, and access parameters.

After you add a device to an automatic deployment plan, the iCC module configures the device in the following workflow:

- Determines whether the device has been added to IMC and adds the device to IMC if not.
- Deploys the following items in the deployment plan to the device in turn: software (optional), configuration file, and CLI script (optional), and backs up the device configuration (optional).

To add a device to an automatic deployment plan:

1. Navigate to **Service→Auto Deployment Plan**.
2. Click the **Service** tab from the tabular navigation system on the top.
3. Click the **Configuration Center** on the navigation tree on the left.
4. Click the **Auto Deployment Plan** under **Configuration Center** from the navigation system on the left.
   All existing automatic deployment plans is displayed in the **Auto Deployment Plan** page.
5. Click the icon in the **Operation** field associated with the deployment plan you want to add a device.
   The **Add Auto Deployment Device** page appears.
6. Select the configuration file folder that contains the configuration file you want to deploy from the **Folder** list of the **Configuration File to Deploy** section.
7. Select the configuration file name you want to deploy from the **File Name** list of the **Configuration File to Deploy** section.
   You must add or import configuration files in the **Configuration Templates** list before selecting the configuration file name. Once you have added or imported the configuration files, they appear in the **File Name** list.
8. Do one of the following:
   - If you want IMC to back up the configurations of this device, click on the radio button to the left of **Yes** of the **Back Up Configuration File** field of the **Configuration File to Deploy** section, or
   - Click the radio button to the left of **No** if you do not.
9. Do one of the following:
   - If the configuration file content includes variables, input the parameters of the configuration file in the **Please input parameter** field of the **Configuration File to Deploy** section, or
   - If not, go to Step 10.
10. Do one of the following:
    - If you want to deploy software to this device, click the checkbox to the left of **Software to Deploy** of the **Software to Deploy** section, and then go to Step 11, or
    - If you do not, go to Step 13.
11. Select the software name you want to deploy from the **Software Name** list of the **Software to Deploy** section.
12. Configure the following settings as needed in the **Software Deployment Policy** section:
Set the Current Running Software as Backup Startup Software: Choose this option if you want to back up the current system software as startup software on this device.

Delete Current Running Software: Choose this option if you do not want to retain the current running software on this device. The current running software is deleted when the deployment plan begins. To choose this option, you must first deselect the first option, Set the Current Running Software as Backup Startup Software.

**WARNING:**
If you select the Delete Current Running Software option, IMC deletes the current running software of the device even if the deployment plan fails. If the deployment plan fails, the device might not restart. Exercise this option with caution.

Delete Current Backup Startup Software: Choose this option if you want to delete the current startup software backup from this device. The startup software backup is deleted when the deployment plan begins.

13. Do one of the following:
   - If you want to deploy the CLI script to this device, click on the checkbox to the left of CLI Script of the CLI Script section, and then go to Step 11, or
   - If you do not, go to Step 15.

14. Select the CLI script file folder that contains the CLI script file you want to deploy from the Folder list of the CLI Script section.

15. Select the CLI script file name you want to deploy from the File Name list of the CLI Script section.
    You must add CLI script files in the Configuration Templates list before selecting the CLI script file name. Once you have added the CLI script files, they appear in the File Name list.

16. Do one of the following:
   - If the CLI script file content includes variables, input the parameters of the CLI script file in the Please input parameter field of the CLI Script section, or
   - If not, go to Step 19.

17. Enter the MAC address for this device in the Match Criteria: MAC address field of the Device Basic Information section.
    - **Match Criteria: MAC address**: Enter the MAC address for this device.

18. Enter the current IP address for this device in the Match Criteria: Current IP address field of the Device Basic Information section.
    - **Match Criteria: Current IP Address**: Enter the current IP address for this device.
    You should input at least one of the match criteria. To match a zero-configuration device, enter the MAC address. To match a device that has been added to IMC, enter its MAC address, current IP address, or both.

19. Enter the target IP address for this device in the Target IP Address field of the Device Basic Information section.

20. Do one of the following:
    - If you want to assign a stack member ID to a zero-configuration device, click the checkbox to the left of Stack Member ID, and enter the stack member ID, or
    - If you do not, go to Step 24.
WARNING:
You can assign stack member IDs only to the zero-configuration devices. Otherwise, automatic deployment can fail.

21. Do one of the following:
   o If you want to configure device information, click the checkbox to the left of Configure Device Information of the Configure Device Information section, and then go to Step 19, or
   o If you do not, go to Step 27.

22. Enter a device label for this device in the Device Label field of the Configure Device Information section.
   o Device Label: Enter the name for the device you want to add.

23. Select the device group to which you want to add this device from the Device Group list of the Configure Device Information section.
   You must create device groups before you can add devices to them. Once you have created the device groups, they appear in the Device Group list.

24. Select the login type for this device from the Login Type list of the Configure Device Information section.
   o Login Type: Select the type that IMC uses to log in to the device from the Login Type list. Options include Telnet, SSH, and None.
   This parameter does not take effect on a device that has been added to IMC.

25. If you want IMC to process traps sent by this device for alarming and notification purposes, verify that the checkbox to the left of Automatically register to receive SNMP traps from supported devices is checked.

WARNING:
If the Automatically register to receive SNMP traps from supported devices checkbox is not checked, IMC does not process, display, or alarm on traps sent by this device.

26. If this device to be added responds to ping requests for monitoring reachability, verify that the checkbox to the left of Support Ping Operation is checked. If this device does not respond to ping requests, verify that the checkbox is unchecked.

27. Do one of the following:
   o If you want to configure the SNMP parameters for this device, click the checkbox to the left of SNMP Settings of the Access Parameters section, and then go to Step 28, or
   o If you do not, go directly to Step 28.
   If the configuration file or CLI script to be deployed contains SNMP, Telnet, and SSH parameter modifications, modify the access parameters to keep them consistent with those in the configuration file or CLI script, so that IMC can access the device.

28. To configure the SNMP settings for this device, click the Configure link located at the SNMP Settings of the Access Parameters section.
   The SNMP Parameters dialog box appears.
   You can either enter the SNMP settings in this dialog box or select an existing SNMP template that contains the SNMP settings for this device. SNMP templates are particularly useful when SNMP configurations are standardized. For more information on creating SNMP templates, see "SNMP templates" (page 74).
**Editing SNMP settings manually**

To edit the SNMP parameters:

1. Verify that the radio button  to the left of **Edit SNMP Parameters** is selected.
2. Select the version of SNMP (v1 or v2c) that is configured on the device to be added from the **Parameter Type** list.
   
   You can only add devices that are configured with SNMPv3 using SNMP templates. Therefore, you must create an SNMP template with the SNMPv3 parameters for this device before adding this device. For more information on creating SNMP templates, see "SNMP templates" (page 74).
3. Enter the read-only community string in the **Read-Only Community String** field.
4. Enter the read-write community string in the **Read-Write Community String** field.
5. Enter the SNMP timeout value (1–60 seconds) in the **Timeout** field. This parameter determines how long IMC waits for an SNMP reply from the managed device before declaring that the request has timed out. The default is 4.
6. Enter the number of SNMP retries (1–20) in the **Retries** field. The retries parameter defines how many times the management system (IMC) sends SNMP retries in an attempt to communicate with the managed device before reporting a failure. The default is 3.

**Using existing SNMP templates**

To configure the SNMP settings for this device using an SNMP template:

1. Click the radio button  to the left of **Select an Existing Template**.
2. Click the radio button  to the left of the SNMP template you want to use.
3. Click **OK** to apply the SNMP parameters for this device.
4. If you want to configure the telnet parameters for this device, click the checkbox  to the left of **Telnet Settings** of the **Access Parameters** section, and then go to Step 6.
5. To configure the Telnet settings for this device, click the **Configure** link located at the **Telnet Settings** of the **Access Parameters** section.

   The **Telnet Parameters** dialog box appears.

   You can either enter the Telnet settings in this dialog box or select an existing Telnet template that contains the Telnet settings for this device. Telnet templates are particularly useful when Telnet configurations are standardized. For more information on creating Telnet templates, see "Telnet templates" (page 77).

**Editing Telnet settings manually**

To edit the telnet parameters manually, verify that the radio button  to the left of **Edit Telnet Parameters** is selected.

Select the Telnet authentication mode from the **Authentication Mode** list.

- **Username**: Enter the Telnet username in the **Username** field, if prompted.
- **Password**: Enter the Telnet password in the **Password** field, if prompted.
- **Super Password**: Enter the Telnet super password in the **Super Password** field, if prompted.
- **Timeout**: Enter the Telnet timeout value configured on the managed device in the **Timeout** field. Valid range is 1–60 seconds.
Using existing Telnet templates

To configure the Telnet settings for this device using Telnet templates, click on the radio button to the left of **Select an Existing Template**.

1. Click the radio button to the left of the Telnet template you want to use.
2. Click **OK** to apply the Telnet configuration settings to this device.
3. If you want to configure the SSH parameters for this device, click the checkbox to the left of **SSH Settings** of the **Access Parameters** section.
4. To configure the SSH settings for this device, click the **Configure** link located at the **SSH Settings** of the **Access Parameters** section.

The SSH Parameters dialog box appears.

You can either enter the SSH settings in this dialog box or select an existing SSH template that contains the SSH settings for this device. SSH templates are useful when SSH configurations are standardized. For more information on creating SSH templates, see "SSH templates" (page 80).

Editing SSH settings manually

To edit the SSH parameters, verify that the radio button to the left of **Edit SSH Parameters** is selected.

- **Authentication Mode**: Select the authentication mode from the **Authentication Mode** list. The authentication mode selected must match the configuration on the managed devices.
- **User Name**: Enter username in the **User Name** field.
- **Password**: Enter the password in the **Password** field, if prompted.
- **Private Key File**: Enter the path and filename of the private key file that contains the key that enables login, if prompted.
- **Private Key Password**: Enter the private key password for the private key file, if prompted.
- **Port**: Enter the TCP port for SSH in the **Port** field. The default TCP port is 22.
- **Timeout**: Enter the SSH timeout value (1–120 seconds). The timeout parameter defines how long the system waits for the device to respond in seconds before declaring that the response has timed out. The default setting is 10 seconds.
- **Retries**: Enter the number of SSH retries (1–5). The retries parameter defines how many times the management system (IMC) sends SSH retries in an attempt to communicate with the managed device before reporting a failure. The default setting is 3.

Using existing SSH templates

To configure the SSH settings for this device using SSH templates:

1. Click the radio button to the left of **Select an Existing Template**.
2. Click the radio button to the left of the SSH template you want to use.
3. Click **OK** to apply the SSH configuration settings to this device.
4. Click **OK** to apply this device configuration.
5. Review the results of the add operation in the **Auto Deployment Plan** page.

Modifying an automatic deployment device

To modify an existing automatic deployment device:

1. Navigate to **Service→Auto Deployment Plan**.
2. Click the **Service** tab from the tabular navigation system on the top.
3. Click the **Configuration Center** on the navigation tree on the left.

4. Click the **Auto Deployment Plan** under **Configuration Center** from the navigation system on the left.

   All existing automatic deployment plans are displayed in the **Auto Deployment Plan** page.

5. Click the icon 📀 with the deployment plan you want to expand.

   All existing devices in the deployment plan appear.

6. Click the icon 📊 in the **Operation** field associated with the deployment device you want to modify.

   The **Modify Auto Deployment Device** page appears.

7. Do one of the following:

   - If you want to modify the **Configuration File to Deploy** information, click the **Modify** link to the left of the **Configuration File to Deploy** section, and then go to **Step 9**.
   - If you do not, go to **Step 12**.

8. Select the configuration file folder that contains the configuration file you want to deploy from the **Folder** list of the **Configuration File to Deploy** section.

9. Select the configuration file name you want to deploy from the **File Name** list of the **Configuration File to Deploy** section.

10. Do one of the following:

    - If you want IMC to back up the configurations of this device, click the radio button ☑ to the left of **Yes** of the **Back Up Configuration File** field of the **Configuration File to Deploy** section, or
    - Click the radio button ☑ to the left of **No** if you do not.

11. If the configuration file content includes variables, input the parameters of the configuration file in the **Please input parameter** field of the **Configuration File to Deploy** section.

12. If not, go to "Modifying the software to deploy information" section.

**Modifying the software to deploy information**

To modify the **Software to Deploy** information:

1. Do one of the following:

   - If you clicked the checkbox ☑ to the left of **Software to Deploy** when this device was added, go to **Step 4**, or
   - If you want to deploy software to this device, click the checkbox ☑ to the left of **Software to Deploy**, and then go to **Step 4**.

2. If you do not want to deploy software to this device, click the checkbox ☑ to the left of **Software to Deploy**, and then go to **Step 6**.

3. Select the software name you want to deploy from the **Software Name** list of the **Software to Deploy** section.

4. Configure the following settings as needed in the **Software Deployment Policy** section:

   - **Set the Current Running Software as Backup Startup Software**: Choose this option if you want to back up the current system software as startup software on this device.
   - **Delete Current Running Software**: Choose this option if you do not want to retain the current running software on this device. The current running software is deleted when the deployment plan begins. To choose this option, you must first deselect the first option, **Set the Current Running Software as Backup Startup Software**.
WARNING:
If you select the **Delete Current Running Software** option, IMC deletes the current running software of the device even if the deployment plan fails. If the deployment plan fails, the device might not restart. Exercise this option with caution.

- **Delete Current Backup Startup Software**: Choose this option if you want to delete the current startup software backup from this device. The startup software backup is deleted when the deployment plan begins.

5. Do one of the following:
   - If you want to modify the **CLI Script** information, click the **Modify** link to the left of the **CLI Script** section, and then go to **Step 8**, or
   - If you do not, go to **Step 18**.

6. To modify the **CLI Script** information:
   - If you clicked the checkbox to the left of **CLI Script** when this device was added, go to **Step 9**.
   - If you want to deploy the CLI script to this device, click the checkbox to the left of **CLI Script**, and then go to **Step 9**.
   - If you do not want to deploy the CLI script to this device, click the checkbox to the left of **CLI Script**, and then go to **Step 13**.

7. Select the CLI script file folder that contains the CLI script file you want to deploy from the **Folder** list of the **CLI Script** section.

8. Select the CLI script file name you want to deploy from the **File Name** list of the **CLI Script** section.

9. Do one of the following:
   - If the CLI script file content includes variables, input the parameters of the CLI script file in the Please input parameter field of the **CLI Script** section, or
   - If not, go to **Step 13**.

10. Modify the MAC address for this device as needed in the **Match Criteria: MAC address** field of the **Device Basic Information** section.

11. Modify the current IP address for this device as needed in the **Match Criteria: Current IP address** field of the **Device Basic Information** section.
    
    You should input at least one of the match criteria. To match a zero-configuration device, enter the MAC address. To match a device that has been added to IMC, enter its MAC address, current IP address, or both.

12. Modify the target IP address for this device as needed in the **Target IP Address** field of the **Device Basic Information** section.

13. If you want to modify the stack member ID for this device, enter the new stack member ID in the **Stack Member ID** field.

**WARNING:**
You can assign stack member IDs only to the zero-configuration devices. Otherwise, auto deployment can fail.

14. If you want to modify the **Configure Device Information**, see "Modifying the configure device information" section (page 463).
Modifying the configure device information

To modify the configure device information:

1. Do one of the following:
   - If you clicked the checkbox □ to the left of Configure Device Information when this device was added, go to Step 2, or
   - If you want to configure this device information, click the checkbox □ to the left of Configure Device Information, and then go to Step 2, or
   - If you do not want to configure this device information, click the checkbox ✓ to the left of Configure Device Information, and then go to Step 7.

2. Modify the device label for this device in the Device Label field of the Configure Device Information section.

3. Select the device group to which you want to modify this device from the Device Group list of the Configure Device Information section.
   You must create device groups before you can modify devices in them. Once you have created the device groups, they appear in the Device Group list.

4. Select the login type for this device from the Login Type list of the Configure Device Information section.
   This parameter does not take effect on a device that has been added to IMC.

5. If you want IMC to process traps sent by this device for alarming and notification purposes, verify that the checkbox to the left of Automatically register to receive SNMP traps from supported devices is checked.

   ▲ WARNING:

   If the Automatically register to receive SNMP traps from supported devices checkbox is not checked, IMC cannot process, display, or alarm on traps sent by this device.

6. If this device to be modified responds to ping requests for monitoring reachability, verify that the checkbox □ to the left of Support Ping Operation is checked.
   If this device does not respond to ping requests, verify that the checkbox is unchecked □.

7. Do one of the following:
   - If you want to modify the SNMP Settings information, click the Modify link to the left of the Device SNMP Settings section, and then go to Step 8, or
   - If you do not, go to Step 33.

8. Do one of the following:
   - If you clicked the checkbox □ to the left of SNMP Settings when this automatic deployment device was added, go to Step 9, or
   - If you want to configure the SNMP parameters for this automatic deployment device, click the checkbox □ to the left of SNMP Settings, and then go to Step 9, or
   - If you do not want to configure the SNMP parameters for this automatic deployment device, click the checkbox ✓ to the left of SNMP Settings, and then go to "Editing SNMP settings manually" (page 155).

   If the configuration file or CLI script to be deployed contains SNMP, Telnet, and SSH parameter modifications, modify the access parameters to keep them consistent with those in the configuration file or CLI script, so that IMC can access the device.
To configure the SNMP settings for this device, click the Configure link located at the SNMP Settings of the Access Parameters section.

The SNMP Parameters dialog box appears.

You can either enter the SNMP settings in this dialog box or select an existing SNMP template that contains the SNMP settings for this device. SNMP templates are particularly useful when SNMP configurations are standardized. For more information on creating SNMP templates, see "SNMP templates" (page 74).

**Editing SNMP settings manually**

To edit the SNMP parameters:

1. Verify that the radio button □ to the left of Edit SNMP Parameters is selected.
2. Select the version of SNMP (v1 or v2c) that is configured on the device to be modified from the Parameter Type list.
3. Enter the read-only community string in the Read-Only Community String field.
4. Enter the read-write community string in the Read-Write Community String field.
5. Enter the SNMP timeout value (1–60 seconds) in the Timeout field.
   
   This parameter determines how long IMC waits for an SNMP reply from the managed device before declaring that the request has timed out. The default is 4.
6. Enter the number of SNMP retries (1–20) in the Retries field. The retries parameter defines how many times the management system (IMC) sends SNMP retries in an attempt to communicate with the managed device before reporting a failure. The default is 3.

**Using existing SNMP templates**

To configure the SNMP settings for this device using an SNMP template:

1. Click the radio button □ to the left of Select an Existing Template.
2. Click the radio button □ to the left of the SNMP template you want to use.
3. Click OK to apply the SNMP parameters for this device.
4. If you clicked the checkbox □ to the left of Telnet Settings when this device was added, go to Step 34.
5. If you want to configure the telnet parameters for this device, click the checkbox □ to the left of Telnet Settings, and then go to Step 34.
6. If you do not want to configure the telnet parameters for this device, click the checkbox □ to the left of Telnet Settings, and then go to Step 36.
7. To configure the Telnet settings for this device, click the Configure link located at the Telnet Settings of the Access Parameters section.

The Telnet Parameters dialog box appears.

You can either enter the Telnet settings in this dialog box or select an existing Telnet template that contains the Telnet settings for this device. Telnet templates are particularly useful when Telnet configurations are standardized. For more information on creating Telnet templates see "Telnet templates" (page 77).

**Editing Telnet settings manually**

To edit the telnet parameters manually, verify that the radio button □ to the left of Edit Telnet Parameters is selected.

Select the Telnet authentication mode from the Authentication Mode list.
- **Username**: Enter the Telnet username in the **Username** field, if prompted.
- **Password**: Enter the Telnet password in the **Password** field, if prompted.
- **Super Password**: Enter the Telnet super password in the **Super Password** field, if prompted.
- **Timeout**: Enter the Telnet timeout value configured on the managed device in the **Timeout** field. Valid range is 1–60 seconds.

**Using existing Telnet templates**

To configure the Telnet settings for this device using Telnet templates:

1. Click the radio button to the left of **Select an Existing Template**.
2. Click the radio button to the left of the Telnet template you want to use.
3. Click OK to apply the Telnet configuration settings to this device.
4. If you clicked the checkbox to the left of **SSH Settings** when this device was added, go to Step 7.
5. If you want to configure the SSH parameters for this device, click the checkbox to the left of **SSH Settings**, and then go to Step 7.
6. If you do not want to configure the SSH parameters for this device, click the checkbox to the left of **SSH Settings**.
7. To configure the SSH settings for this device, click the **Configure** link located at the **SSH Settings** of the **Access Parameters** section.

The **SSH Parameters** dialog box appears.

You can either enter the SSH settings in this dialog box or select an existing SSH template that contains the SSH settings for this device. SSH templates are particularly useful when SSH configurations are standardized. For more information on creating SSH templates, see "SSH templates" (page 80).

**Editing SSH settings manually**

To edit the SSH parameters, verify that the radio button to the left of **Edit SSH Parameters** is selected.

- **Authentication Mode**: Select the authentication mode from the **Authentication Mode** list.

  The authentication mode selected must match the configuration on the managed devices.
  
  o **User Name**: Enter username in the **User Name** field.
  o **Password**: Enter the password in the **Password** field, if prompted.
  o **Private Key File**: Enter the path and filename of the private key file that contains the key that enables login, if prompted.
  o **Private Key Password**: Enter the private key password for the private key file, if prompted.
  o **Port**: Enter the TCP port for SSH in the **Port** field. The default TCP port is 22.
  o **Timeout**: Enter the SSH timeout value (1–120 seconds). The timeout parameter defines how long the system waits for the device to respond in seconds before declaring that the response has timed out. The default setting is 10 seconds.
  o **Retries**: Enter the number of SSH retries (1–5). The retries parameter defines how many times the management system (IMC) sends SSH retries in an attempt to communicate with the managed device before reporting a failure. The default setting is 3.

**Using existing SSH templates**

To configure the SSH settings for this device using SSH templates:

1. Click the radio button to the left of **Select an Existing Template**.
2. Click the radio button to the left of the SSH template you want to use.
3. Click **OK** to apply the SSH configuration settings to this device.
4. Click **OK** to apply this device configuration.

**Importing devices into an automatic deployment plan**

IMC provides you with the ability to batch import device information from a file to an automatic deployment plan.

The file must be in CSV format. The first line in the file is the column headings, and all the other lines are the corresponding values. The following table, shown in Table 27 (page 466) describes these columns.

**Table 27 Columns in a CSV file**

<table>
<thead>
<tr>
<th>Column heading</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>TargetIp</td>
<td>IP address of the device after the selected configuration file is deployed on the device.</td>
<td>Yes</td>
</tr>
<tr>
<td>ConfigFile</td>
<td>Name of the configuration file to be deployed on the device.</td>
<td>Yes</td>
</tr>
<tr>
<td>ConfigPara</td>
<td>Parameters in the configuration file to be deployed. The parameters are in the format of Parameter name1: Parameter value1; Parameter name2: Parameter value2; ...For example, ACLNumber: 3005.</td>
<td>No</td>
</tr>
<tr>
<td>CurrentDeviceIp</td>
<td>Current IP address of the device.</td>
<td>At least one of them is required.</td>
</tr>
<tr>
<td>MACAddress</td>
<td>MAC address of the device.</td>
<td></td>
</tr>
<tr>
<td>Unitld</td>
<td>Stack member ID, ranging from 1 to 9. A value of –1 indicates that the stack feature is disabled on the device.</td>
<td>No</td>
</tr>
<tr>
<td>changDeviceInfo</td>
<td>Indicates whether or not the device information is different from that in the existing configuration file on the device. The value can be: 0 for no 1 for yes</td>
<td>No</td>
</tr>
<tr>
<td>DeviceName</td>
<td>Device label.</td>
<td>No</td>
</tr>
<tr>
<td>DeviceGroup</td>
<td>Device group.</td>
<td>No</td>
</tr>
<tr>
<td>DeploySoft</td>
<td>Software to be deployed on the device.</td>
<td>No</td>
</tr>
<tr>
<td>CLIScript</td>
<td>Name of the CLI script to be deployed on the device.</td>
<td>No</td>
</tr>
<tr>
<td>CLIPara</td>
<td>Parameters in the CLI script file to be deployed. The parameters are in the format of Parameter name1: Parameter value1; Parameter name2: Parameter value2; ...For example, ACLNumber: 3005.</td>
<td>No</td>
</tr>
<tr>
<td>changSnmpPara</td>
<td>Indicates whether or not the device’s SNMP parameters are different from those in the existing configuration file on the device. The value can be: 0 for no 1 for yes</td>
<td>No</td>
</tr>
<tr>
<td>SnmpParaVersion</td>
<td>SNMP version. The value can be: 1 for SNMPv1 2 for SNMPv2c 3 for SNMPv3</td>
<td>No</td>
</tr>
<tr>
<td>Column heading</td>
<td>Description</td>
<td>Required</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>SnmpParaRead</td>
<td>Read-only community name, which is <strong>public</strong> by default and contains 32 characters at most.</td>
<td>No</td>
</tr>
<tr>
<td>SnmpParaWrite</td>
<td>Read and write community name, which is <strong>private</strong> by default and contains 32 characters at most.</td>
<td>No</td>
</tr>
<tr>
<td>SnmpParaSecurityUser</td>
<td>Username, which applies to only SNMPv3 and contains 32 characters at most. A username corresponds to a SNMPv3 template name.</td>
<td>No</td>
</tr>
<tr>
<td>SnmpParaContextName</td>
<td>SNMPv3 context name, which contains 32 characters at most.</td>
<td>No</td>
</tr>
<tr>
<td>SnmpParaSecuMode</td>
<td>Security mode. The value can be:</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>• 1 for no authentication and no encryption</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 2 for authentication and no encryption</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 3 for authentication and encryption</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The SnmpParaAuthScheme and SnmpParaPrivScheme columns must have the same value as this column.</td>
<td></td>
</tr>
<tr>
<td>SnmpParaAuthScheme</td>
<td>Authentication mode. The value can be:</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>• 1 for none</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 2 for MD5</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 3 for SHA</td>
<td></td>
</tr>
<tr>
<td>SnmpParaAuthPassword</td>
<td>Authentication password, which contains 32 characters at most.</td>
<td>No</td>
</tr>
<tr>
<td>SnmpParaPrivScheme</td>
<td>Encryption mode. The value can be:</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>• 1 for none</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 2 for DES</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 19 for AES128</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 21 for AES256</td>
<td></td>
</tr>
<tr>
<td>SnmpParaPrivPassword</td>
<td>Encryption password, which contains 32 characters at most.</td>
<td>No</td>
</tr>
<tr>
<td>SnmpParaTimeOut</td>
<td>Operation timeout period (in seconds), which is 4 by default.</td>
<td>No</td>
</tr>
<tr>
<td>SnmpParaRetry</td>
<td>Maximum number of SNMP retries allowed, which is 3 by default.</td>
<td>No</td>
</tr>
<tr>
<td>PingDevType</td>
<td>Indicates whether or not the ping operation is supported. The value can be:</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>• 1 for yes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 0 for no</td>
<td></td>
</tr>
<tr>
<td>changTelnet</td>
<td>Indicates whether or not the device's Telnet parameters are different from those in the existing configuration file on the device. The value can be:</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>• 0 for no</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 1 for yes</td>
<td></td>
</tr>
<tr>
<td>Column heading</td>
<td>Description</td>
<td>Required</td>
</tr>
<tr>
<td>----------------</td>
<td>-------------</td>
<td>----------</td>
</tr>
<tr>
<td>TelnetStyle</td>
<td>Telnet type. The value can be:</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>• 0 for password</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 1 for username+password</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 2 for super password</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 3 for password+super password</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 4 for username+password+super password</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 5 for no username+no password</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 6 for username+no password</td>
<td></td>
</tr>
<tr>
<td>TelnetUseName</td>
<td>Telnet username.</td>
<td>No</td>
</tr>
<tr>
<td>TelnetPassword</td>
<td>Telnet password.</td>
<td>No</td>
</tr>
<tr>
<td>TelnetSuperWord</td>
<td>Telnet super password.</td>
<td>No</td>
</tr>
<tr>
<td>TelnetTimeout</td>
<td>Telnet timeout period, ranging from 1 to 60 seconds.</td>
<td>No</td>
</tr>
<tr>
<td>changeSsh</td>
<td>Indicates whether or not the device’s SSH parameters are different from those in the existing configuration file on the device. The value can be:</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>• 0 for no</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 1 for yes</td>
<td></td>
</tr>
<tr>
<td>SshParaAuthType</td>
<td>SSH authentication mode. The value can be:</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>• 0 for password authentication.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Other authentication modes are not supported.</td>
<td></td>
</tr>
<tr>
<td>SshParaPort</td>
<td>SSH port number.</td>
<td>No</td>
</tr>
<tr>
<td>SshParaUserName</td>
<td>SSH username.</td>
<td>No</td>
</tr>
<tr>
<td>SshParaPassword</td>
<td>SSH password.</td>
<td>No</td>
</tr>
<tr>
<td>SshParaRetries</td>
<td>Maximum number of SSH retries allowed, ranging from 1 to 5.</td>
<td>No</td>
</tr>
<tr>
<td>SshParaTimeOut</td>
<td>SSH timeout period, ranging from 1–120 seconds.</td>
<td>No</td>
</tr>
<tr>
<td>LoginType</td>
<td>Login type. The value can be:</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>• 0 for none</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 1 for Telnet</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 2 for SSH</td>
<td></td>
</tr>
<tr>
<td>sendTrap</td>
<td>Indicates whether or not the device sends traps to IMC. The value can be:</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>• 0 for no</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 1 for yes</td>
<td></td>
</tr>
<tr>
<td>delBackupSoftFlag</td>
<td>Indicates whether or not the backup software is deleted. The value can be:</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>• 0 for no</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 1 for yes</td>
<td></td>
</tr>
<tr>
<td>delCurrSoftFlag</td>
<td>Indicates whether or not the current software is deleted. The value can be:</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>• 0 for no</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 1 for yes</td>
<td></td>
</tr>
<tr>
<td>Column heading</td>
<td>Description</td>
<td>Required</td>
</tr>
<tr>
<td>----------------</td>
<td>-------------</td>
<td>----------</td>
</tr>
<tr>
<td>mainToBackupFlag</td>
<td>Specifies whether or not the current software is backed up. The value can be:</td>
<td>No</td>
</tr>
<tr>
<td>Φ</td>
<td>0 for no</td>
<td>0 for no</td>
</tr>
<tr>
<td>Φ</td>
<td>1 for yes</td>
<td>1 for yes</td>
</tr>
</tbody>
</table>

To import devices into an automatic deployment plan from a file on your local computer:

1. Navigate to Service→Auto Deployment Plan.
2. Click the Service tab from the tabular navigation system on the top.
3. Click the Configuration Center on the navigation tree on the left.
4. Click the Auto Deployment Plan under Configuration Center from the navigation system on the left.
   All existing automatic deployment plans are displayed in the Auto Deployment Plan page.
5. Click the icon 📂 in the Operation field associated with the deployment plan to which you want to import devices.
   The Import Auto Deployment Devices dialog box appears.
6. Enter the file you want to import, including the full path in the Select Source File field.
7. Alternatively, you can browse the file system of your local computer for the file you want to import. To browse, click Browse to the right of the Select Source File field. Follow the instructions provided by your browser for locating the file.
8. Click Start Import to import the file.
9. After the file is imported, click Close.
10. Review the results of the import operation in the Auto Deployment Plan page.

Deleting a device from an automatic deployment plan

To delete a device from an automatic deployment plan

1. Navigate to Service→Auto Deployment Plan.
2. Click the Service tab from the tabular navigation system on the top.
3. Click the Configuration Center on the navigation tree on the left.
4. Click the Auto Deployment Plan under Configuration Center from the navigation system on the left.
   All existing automatic deployment plans are displayed in the Auto Deployment Plan page.
5. Click the icon 📂 with the deployment plan you want to expand.
   All existing devices in the deployment plan are displayed.
6. Click the icon ✗ in the Operation field associated with the deployment device you want to delete.
   You cannot delete an automatic deployment device on which automatic deployment is being executed.
7. Click OK to confirm deletion of the deployment device.
8. Review the results of the delete operation in the Auto Deployment Plan page.
Triggering automatic deployment on devices

You can trigger automatic deployment on devices that have not been deployed or failed to be deployed in the automatic deployment plan. This operation applies only to the simple-configuration devices that have been added to IMC.

To trigger automatic deployment on devices:

1. Navigate to Service→Auto Deployment Plan.
2. Click the Service tab from the tabular navigation system on the top.
3. Click the Configuration Center on the navigation tree on the left.
4. Click the Auto Deployment Plan under Configuration Center from the navigation system on the left.
   All existing automatic deployment plans is displayed in the Auto Deployment Plan page.
5. Click the icon with the deployment plan you want to expand.
   All existing devices in the deployment plan appears.
6. Click the icon in the Operation field associated with the device on which you want to trigger automatic deployment.
   The system displays that the deployment process is successfully triggered.

Viewing automatic deployment execution results

To view the execution result of an automatic deployment plan or device:

1. Navigate to Service→Auto Deployment Plan.
2. Click the Service tab from the tabular navigation system on the top.
3. Click the Configuration Center on the navigation tree on the left.
4. Click the Auto Deployment Plan under Configuration Center from the navigation system on the left.
   All existing automatic deployment plans are displayed in the Auto Deployment Plan page.
5. Do one of the following, to view the result of an automatic deployment plan or device, respectively:
   o If you want to view the execution result of an automatic deployment plan, go the Step 7, or
   o If you want to view the execution result of an automatic deployment device, go the Step 9.
6. Click the icon with the deployment plan for which you want to view the execution result in the Auto Deployment Plan page.
   The Auto Deployment Execution Result dialog box is displayed, showing the automatic deployment execution result of the plan.
7. Click the icon with the device information you want to view.
8. Click the icon with the deployment plan you want to expand in the Auto Deployment Plan page.
   All existing devices in the deployment plan appear.
9. Click the icon in the Operation field associated with the deployment device for which you want to view the execution result.
   The Auto Deployment Execution Result dialog box is displayed, showing the automatic deployment execution result of the device.
Initial configuration file management

You can manage the pre-defined and user-defined initial configuration files. An initial configuration file in IMC is deployed on a zero-configuration device through DHCP after the device is powered on. The initial configuration file must contain basic SNMP and Telnet parameters. After the zero-configuration device executes the initial configuration file, IMC automatically adds the device through auto discovery and apply a pre-configured automatic deployment plan to it.

Configuring the DHCP server

IMC provides you with the automatic initial configuration function for zero-configuration devices. When a zero-configuration device or a simple-configuration device is connected to IMC and started up, the DHCP server assigns an IP address to the device and sends the TFTP server address and initial configuration file name to the device. The device then downloads the initial configuration file from the TFTP server to complete automatic configuration.

Configure the address pool, network management system, DNS server, domain name, TFTP server address, initial configuration file name, and lease duration on the DHCP server.

The following guidelines apply to configuration file management:

- If the DHCP server and the device are not on the same network segment, configure a DHCP relay agent on the gateway that connects to the device.
- If the DHCP server does not support configuring the TFTP server address, configure the DNS server address and domain name on the DHCP server. The TFTP server must have an IMC iCC component installed.
- The initial configuration file configured on the DHCP server must be created in IMC and applies to the zero-configuration device to be deployed.

Accessing the initial configuration file

To access the page of initial configuration files:

1. Navigate to Service→Auto Deployment Plan→Initial Configuration File Management.
2. Click the Service tab from the tabular navigation system on the top.
3. Click the Configuration Center on the navigation tree on the left.
4. Click the Auto Deployment Plan under Configuration Center from the navigation system on the left.
5. Click the Initial Configuration File Management link located in the upper right corner of the Auto Deployment Plan page.

All existing initial configuration files are displayed in the Initial Configuration File Management page.

- File Name: Contains the name of the initial configuration file.
- File Type: Identifies the type of the initial configuration file. Options include Pre-Defined and Self-Defined.
- Creation Time: Contains a date and time stamp for the creation of the initial configuration file.
- Description: Contains a description for the initial configuration file.
- Modify: Contains a link for modifying the initial configuration file.
- Copy: Contains a link for copying the initial configuration file.
- Delete: Contains a link for deleting the initial configuration file.
You can sort the **Device Backup List** by the **File Name**, **File Type**, and **Creation Time** field. Click the column label to sort the list by the selected field. The column label is a toggle switch that lets you toggle between the various sort options specific to each field.

If the **Deployment Task List** contains enough entries, the following navigational aids are displayed.

- Click ▶️ to page forward in the **Initial Configuration File Management** list.
- Click ▶️ to page forward to the end of the **Initial Configuration File Management** list.
- Click ◀️ to page backward in the **Initial Configuration File Management** list.
- Click ◀️ to page backward to the front of the **Initial Configuration File Management** list.

6. Click 8, 15, 50, 100, or 200 from the right side of the main pane to configure how many items per page you want to view.

**Adding an initial configuration file**

To add an initial configuration file:

1. Navigate to **Service → Auto Deployment Plan → Initial Configuration File Management**.
2. Click the **Service** tab from the tabular navigation system on the top.
3. Click the **Configuration Center** on the navigation tree on the left.
4. Click the **Auto Deployment Plan** under **Configuration Center** from the navigation system on the left.
5. Click the **Initial Configuration File Management** link located in the upper right corner of the **Auto Deployment Plan** page.

All existing initial configuration files are displayed in the **Initial Configuration File Management** page.

6. Click **Add**.

The **Add Initial Configuration File** page appears.

7. Enter a unique name for this initial configuration file in the **File Name** field under the **Configuration File** section.

Valid name length is 1–32 characters.

8. Enter a brief description for this initial configuration file in the **Description** field under the **Configuration File** section.

Valid description length is 0–128 characters.

9. Do one of the following:
   - If you want to add this initial configuration file content in the **File Content** field, go to Step 10, or
   - If you want to add this initial configuration file content through an existing template, go to Step 11.

10. Enter the content for this initial configuration file in the **File Content** field under the **Configuration File** section, and then go to Step 14.

11. Click the **Select Template** link to the right of the **File Content** field under the **Configuration File** section.

    The **Select Template** dialog box appears.

12. Select a template in the left of the **Template Name** field, and click ▶️.

    The selected template content is displayed in the **Template Content** field.

13. Click **OK** to accept your template selected.
When you add an initial configuration file content through an existing template, IMC automatically replaces the \${snmpv1_community_read}, \${snmpv1_community_write}, \${telnet_user_name}, and \${telnet_password} variables in the template with the default settings in the Access Parameters section.

14. Click OK to accept your configuration.
15. Review the results of the add operation in the Initial Configuration File Management page.

Modifying an initial configuration file

To modify an existing initial configuration file:
1. Navigate to Service→Auto Deployment Plan→Initial Configuration File Management.
2. Click the Service tab from the tabular navigation system on the top.
3. Click the Configuration Center on the navigation tree on the left.
4. Click the Auto Deployment Plan under Configuration Center from the navigation system on the left.
5. Click the Initial Configuration File Management link located in the upper right corner of the Auto Deployment Plan page.
   All existing initial configuration files are displayed in the Initial Configuration File Management page.
6. Click the icon in the Modify field associated with the initial configuration file you want to modify.
   The Modify Initial Configuration File page appears. The pre-defined initial configuration file cannot be modified. You can modify the name of an initial configuration file once you have created it. You must delete the existing initial configuration file and create a new initial configuration file with the new name.
7. Modify the brief description for this initial configuration file as needed in the Description field under the Configuration File section.
   Valid description length is 0–128 characters.
8. Do one of the following:
   o If you want to modify this initial configuration file content in the File Content field, go to Step 10, or
   o If you want to modify this initial configuration file content through an existing template, go to Step 11.
9. Modify the content for this initial configuration file as needed in the File Content field under the Configuration File section, and then go to Step 14.
10. Click the Select Template link to the right of the File Content field under the Configuration File section.
   The Select Template dialog box appears.
11. Select a template in the left of the Template Name field, and click .
   The selected template content is displayed in the Template Content field.
12. Click OK to accept your template selected.
13. Click OK to accept your configuration.
14. Review the results of the modify operation in the Initial Configuration File Management page.

Copying an initial configuration file

Copying an initial configuration file allows you to re-use and modify an existing initial configuration file.

To copy an existing initial configuration file:
1. Navigate to Service→Auto Deployment Plan→Initial Configuration File Management.
2. Click the Service tab from the tabular navigation system on the top.
3. Click the Configuration Center on the navigation tree on the left.
4. Click the Auto Deployment Plan under Configuration Center from the navigation system on the left.
5. Click the Initial Configuration File Management link located in the upper right corner of the Auto Deployment Plan page.
   All existing initial configuration files are displayed in the Initial Configuration File Management page.
6. Click the icon in the Copy field associated with the initial configuration file you want to copy.
   The Copy Initial Configuration File page appears.
7. Rename the initial configuration file with a unique name in the File Name field.
8. Modify the brief description for this initial configuration file as needed in the Description field under the Configuration File section.
   Valid description length is 0–128 characters.
9. Do one of the following:
   o If you want to modify this initial configuration file content in the File Content field, go to Step 10, or
   o If you want to modify this initial configuration file content through an existing template, go to Step 11.
10. Modify the content for this initial configuration file in the File Content field under the Configuration File section, and then go to Step 14.
11. Click Select Template link to the right of File Content field under the Configuration File section.
    The Select Template dialog box appears.
12. Select a template in the left of Template Name field, click .
    The selected template content is displayed in the Template Content field.
13. Click OK to accept your template selected.
14. Click OK to accept your configuration.
15. Review the results of the copy operation in the Initial Configuration File Management page.

Deleting an initial configuration file

To delete an existing initial configuration file:
1. Navigate to Service→Auto Deployment Plan→Initial Configuration File Management.
2. Click the Service tab from the tabular navigation system on the top.
3. Click the Configuration Center on the navigation tree on the left.
4. Click the Auto Deployment Plan under Configuration Center from the navigation system on the left.
5. Click the Initial Configuration File Management link located in the upper right corner of the Auto Deployment Plan page.
   All existing initial configuration files are displayed in the Initial Configuration File Management page.
6. Do one of the following:
   o Click the checkbox to the left of the initial configuration files you want to delete, and click Delete, or
Click the icon ✗ in the Delete field associated with the initial configuration files you want to delete. The pre-defined initial configuration file cannot be deleted.

7. Click OK to confirm deletion of the initial configuration files.
8. Review the results of the delete operation in the Initial Configuration File Management page.

Viewing detailed information of an initial configuration file

To view detailed information of an existing initial configuration file:
1. Navigate to Service→Auto Deployment Plan→Initial Configuration File Management.
2. Click the Service tab from the tabular navigation system on the top.
3. Click the Configuration Center on the navigation tree on the left.
4. Click the Auto Deployment Plan under Configuration Center from the navigation system on the left.
5. Click the Initial Configuration File Management link located in the upper right corner of the Auto Deployment Plan page.
6. All existing initial configuration files are displayed in the Initial Configuration File Management page.
7. Click the file name link in the File Name field with the initial configuration file you want to view.

The View Initial Configuration File page is displayed, showing detailed information about the initial configuration file, including the file name, description, and file content.

Managing automatic backup plans

You can back up the configurations of network devices. With the Auto Backup Plan, you can schedule automated backups of configuration files for one or more devices. Backups can be scheduled to run every day, every week, or every month at a specified time. In addition, you can select one or more devices for automated backup. Or, with a single click of the mouse, you can configure a network-wide device configuration backup.

By using the Backup History Report you gain visibility into the backup results for all backup tasks, including backups initiated manually and backups initiated through an auto backup plan. Once a backup task has been initiated, whether manual or scheduled, you can view the results in the Backup History Report.

Automatic device configuration backups

IMC provides the ability to schedule daily, weekly, or monthly backups of one or more devices.

Accessing the automatic backup plan list

IMC provides you with a list of all auto backup plans in the Auto Backup Plan List. This list provides you with the ability to add, view, modify, or delete scheduled backup tasks.

To access the list of automatic or scheduled backup plans:
1. Navigate to Service→Auto Backup Plan.
2. Click the Service tab from the tabular navigation system on the top.
3. Click the Configuration Center on the navigation tree on the left.
4. Click the Auto Backup Plan under Configuration Center from the navigation system on the left.

All existing automatic or scheduled backup plans are displayed in the Auto Backup Plan List.

Auto backup plan list
- **Name**: Contains the operator defined name for this scheduled backup plan.
- **Description**: Contains the description for this backup plan provided by the creator.
- **Configuration Type**: Identifies whether or not the backup plan is a network wide backup plan or an auto backup plan that includes a list of one or more network devices for backup.
- **Backup History**: Contains a link for accessing a filtered view of the Backup History Report for the selected backup plan.
- **Status**: Identifies whether or not the associated backup plan is enabled or disabled.
- **Modify**: Contains an icon for navigating to the page for modifying the associated backup plan.

You can sort the **Auto Backup Plan List** by the **Name**, **Description**, **Configuration Type**, and **Status** fields. Click the column label to sort the list by the selected field. The column label is a toggle switch that allows you to toggle between the various sort options specific to each field.

If the **Auto Backup Plan List** contains enough entries, the following navigational aids are displayed.

- Click **Next** to page forward in the **Auto Backup Plan List**.
- Click **End** to page forward to the end of the **Auto Backup Plan List**.
- Click **Previous** to page backward in the **Auto Backup Plan List**.
- Click **First** to page backward to the front of the **Auto Backup Plan List**.

5. Click **8, 15, 50, 100, or 200** from the right side of the main pane to configure how many items per page you want to view.

**Adding an automatic backup plan**

To add a scheduled backup plan that runs automatically:

1. Navigate to **Service** → **Auto Backup Plan** → **Add Auto Backup Plan**.
2. Click the **Service** tab from the tabular navigation system on the top.
3. Click the **Configuration Center** on the navigation tree on the left.
4. Click the **Auto Backup Plan** under **Configuration Center** from the navigation system on the left. All existing automatic or scheduled backup plans are displayed in the **Auto Backup Plan List**.
5. Click **Add**.
   The **Set Auto Backup Attribute** page appears.
6. Enter a unique name for this backup plan in the **Name** field. Valid name length is 1-32 characters.
7. Select the frequency with which you want this backup to run from the **Operation Frequency** list. Options include **Every Day**, **Every Week**, and **Every Month**.
8. Enter the time of day that you want the backup to run in the field to the right of the **Operation Frequency** list. Valid time entry is HH:MM:SS where HH denotes the two digit hour value, MM denotes the two digit minute value and SS denotes the two digit second value.
9. Enter a brief description for this backup plan in the **Description** field. Valid description length is 0-128 characters.
10. If you want to include all devices in IMC in this backup plan, click the checkbox to the left of **Backup network-wide devices**.

476
Only one backup plan can be configured as a network-wide backup plan.

11. If you did not select the **Backup network-wide devices** option, click **Select Device** to select the devices for which you want configuration files to be backed up by using this backup plan.

12. Add devices either **By View** or by **Advanced** query. See "Adding devices by View" (page 85) and "Adding devices by Advanced query" (page 85).

**Modifying an existing automatic backup plan**

To modify an existing automatic backup plan:

1. Navigate to **Service**→**Auto Backup Plan**.
2. Click the **Service** tab from the tabular navigation system on the top.
3. Click the **Configuration Center** on the navigation tree on the left.
4. Click the **Auto Backup Plan** under **Configuration Center** from the navigation system on the left.
   
   All existing automatic or scheduled backup plan is displayed in the **Auto Backup Plan List**. You cannot modify the name of a backup plan once you have created it. You must delete the existing backup plan and create a new backup plan with the new name.
5. Click the icon in the modify field associated with the backup plan you want to modify.
   
   The **Set Auto Backup Attribute** page appears.
6. Modify the frequency with which you want this backup to run by selecting the new frequency from the **Operation Frequency** list.
   
   Options include **Every Day**, **Every Week**, and **Every Month**.
7. Modify the time of day that you want the backup to run in the field to the right of the **Operation Frequency** list.
   
   A valid time entry is HH:MM:SS where HH denotes the two digit hour value, MM denotes the two digit minute value and SS denotes the two digit second value.
8. Modify the description for this backup plan in the **Description** field.
   
   Valid description length is 0-128 characters.
9. Do one of the following to either include or remove devices from the backup plan:
   
   - If you want to include all devices in IMC in this backup plan, click the checkbox to the left of **Backup network-wide devices**, or
   - To remove this selection, click the checked box to remove the selection.
10. Do one of the following to either modify your plan or remove all devices from the Device List:
   
   - To modify your selection of devices for this backup plan, click **Select Device** to select the devices for which you want their configuration files to be backed up by using this backup plan or to remove devices on this list, or
   - To remove all devices from the Device List for this backup configuration, click **Delete All**.
11. Add or remove devices either **By View** or by **Advanced** query. See "Adding devices by View" (page 85) and "Adding devices by Advanced query" (page 85).

**Deleting an existing automatic backup plan**

To delete an existing automatic backup plan:

1. Navigate to **Service**→**Auto Backup Plan**.
2. Click the **Service** tab from the tabular navigation system on the top.
3. Click the Configuration Center on the navigation tree on the left.

4. Click the Auto Backup Plan under Configuration Center from the navigation system on the left.
   All existing automatic or scheduled backup plans is displayed in the Auto Backup Plan List.

5. Click the checkbox to the left of the backup plans you want to delete.

6. Click Delete.

7. Click OK to confirm deletion of the selected backup plans.

8. Review the results of the deletion operation in the Auto Backup Plan page.

Disabling an existing automatic backup plan

To disable an existing automatic backup plan:
1. Navigate to Service→Auto Backup Plan.
2. Click the Service tab from the tabular navigation system on the top.
3. Click the Configuration Center on the navigation tree on the left.
4. Click the Auto Backup Plan under Configuration Center from the navigation system on the left.
   All existing automatic or scheduled backup plans are displayed in the Auto Backup Plan List.
   The Status field contains the current status of the associated backup task.
   o ☑ Enabled indicates that the associated backup task is enabled.
   o ☒ Disabled indicates that the associated backup task is disabled.
5. Click ☑ Enabled in the Status field for the associated backup plan you want to disable.
6. Review the results of the operation in the Auto Backup Plan page to ensure that the backup plan now contains ☒ Disabled in the Status field of the Auto Backup Plan List.

Enabling an existing automatic backup plan

To enable an existing automatic backup plan:
1. Navigate to Service→Auto Backup Plan.
2. Click the Service tab from the tabular navigation system on the top.
3. Click the Configuration Center on the navigation tree on the left.
4. Click the Auto Backup Plan under Configuration Center from the navigation system on the left.
   All existing automatic or scheduled backup plans are displayed in the Auto Backup Plan List.
   The Status field contains the current status of the associated backup task.
   o ☑ Enabled indicates that the associated backup task is enabled.
   o ☒ Disabled indicates that the associated backup task is disabled.
5. To enable a check task, click the ☒ Disabled icon in the Status field.

The Backup History Report option in the Configuration Center provides you with visibility into the results of both manual and automatic backup tasks. For more information on using the Backup History Report option, see "Managing automatic backup plans" (page 475) and "Backup history reporting" (page 479).

Viewing backup history

By using the Backup History option in the Auto Backup Plan List, you can quickly access a filtered Backup History Report for the selected backup plan.
To view a filtered list:
1. Navigate to Service→Backup History Report.
2. Click the Service tab from the tabular navigation system on the top.
3. Click the Configuration Center on the navigation tree on the left.
4. Click the Auto Backup Plan under Configuration Center from the navigation system on the left. All existing automatic or scheduled backup plans are displayed in the Auto Backup Plan List.
5. Click the icon in the Backup History field for the associated backup plan you want to disable. The current page is updated to display the Backup History Report filtered for the selected backup plan. For more information on using the Backup History Report, see "Backup history reporting" (page 479).

Manual device configuration backups backups

By using the Configuration Center, you can perform manual backups of the configuration files for one or more devices.

To manually backup one or more devices from the Configuration Center:
1. Navigate to Service→<Device Name>→Configuration Management.
2. Click the Service tab from the tabular navigation system on the top.
3. Click the Configuration Center on the navigation tree on the left.
4. Click the Configuration Center icon located under Configuration Center from the navigation system on the left. All devices that can be managed by the Configuration Center are displayed in the list in the bottom half of the Configuration Center page.
5. Click the checkboxes to the left of the devices for which you want to backup the configuration files.
6. Click Backup Configuration.
   
   The page is updated to display the Configuration File Backup Result table. This results table displays the result for each configuration file that was backed up.
7. Review the results for each entry in this table to ensure that all configuration files were backed up successfully.

Backup history reporting

IMC provides a history of configuration file backup tasks for all backup tasks, including those initiated manually and scheduled backups. The Backup History Report list provides you with a view to the results of manual and automated backups.

Accessing the backup history report

To access the Backup History Report:
1. Navigate to Service→Backup History Report.
2. Click the Service tab from the tabular navigation system on the top.
3. Click on the Configuration Center on the navigation tree on the left.
4. Click the Backup History Report under Configuration Center from the navigation system on the left.

The Backup History Report page appears. A history of backups for all automatic and manual backups is displayed in the Backup History List.
Backup history list

- **Name**: Contains a name for the entry. If the backup type is automated or scheduled, this field contains the name of the automatic backup plan. If the backup type for the entry is manual, it contains a date and time stamp for the execution of the manual backup.

The contents of this field serve as a link to the Detailed Information page for the entry.

- **Description**: Contains the description configured for the backup plan if the entry is the result of an automated backup plan. This field is blank if the backup type is a manual backup.

- **Configuration Type**: Identifies whether or not the backup was a Network Wide Backup Plan, an Auto Backup Plan, or a Manual Backup.

- **Execution Time**: Contains a date and time stamp for the completion of the backup task.

- **Execution Result**: Identifies whether the backup Succeeded, Failed, or Partially Succeeded.

- **Operation**: Contains the following icons:
  - This icon initiates a backup of the configuration files for devices that failed on the first attempt.
  - This icon is a link to the Deployment Guide for deploying the associated backup configuration files. For more information on deploying configuration files, see “Deploying configurations and software by using IMC’s deployment guide” (page 442).

The Backup History List can be sorted by many fields. Click the column label to sort the list by the selected field. The column label is a toggle switch that lets you toggle between the various sort options specific to each field.

If the Backup History List contains enough entries, the following navigational aids are displayed.

- Click to page forward in the Backup History List.

- Click to page forward to the end of the Backup History List.

- Click to page backward in the Backup History List.

- Click to page backward to the front of the Backup History List.

5. Click 8, 15, 50, 100, or 200 from the right side of the main pane to configure how many items per page you want to view.

### Querying the backup history report

To query the Backup History Report:

1. Navigate to Service→Backup History Report.
2. Click the Service tab from the tabular navigation system on the top.
3. Click the Configuration Center on the navigation tree on the left.
4. Click the Backup History Report under Configuration Center from the navigation system on the left.

The Backup History Report page appears. A history of all automatic and manual backups is displayed in the Backup History List. To search for a manual backup, enter the date stamp to filter by using the YYYY-MM-DD format.

5. Enter one or more of the following search criteria in the Query Criteria dialog box:
   - **Name**: Enter a complete or partial name of the backup plan name you want to search for in the Name field.
   - **Type**: You can filter the Backup History List by selecting the type of backup you want to filter for from the Type list.
- **Start Time**: Enter the start time of the backup task in the **Start Time** field. You can also use the calendar function by clicking the calendar icon located to the right of the **Start Time** field. A popup calendar appears. Select the start date from the calendar.

- **End Time**: Enter the ending time of the backup task in the **End Time** field. You can also use the calendar function by clicking the calendar icon located to the right of the **End Time** field. A popup calendar appears. Select the end date from the calendar.

6. Click **Query** to submit your filter criteria.

The results of your filter or search query display in the **Backup History List** as explained in the next section.

7. Click **Reset** when you want to restore the full **Backup History List**.

### Backup history detailed information

The **Backup History Report** page provides drilldown capabilities to the details of an individual backup task. From the **Backup History Detailed Information** page, you can view backup details and navigate to the **Device Details** page for each device in the **Device Backup List**.

In addition, you can view the configuration file details, view the backup results for every device in the **Device List**, view the details for each backup task, and save the backup file as a configuration template.

To view backup history detailed information:

1. Navigate to **Service→Backup History Report→<Backup name>**.
2. Click the **Service** tab from the tabular navigation system on the top.
3. Click the **Configuration Center** on the navigation tree on the left.
4. Click the **Backup History Report** under **Configuration Center** from the navigation system on the left. The **Backup History Report** page appears. A history of backups for all automatic and manual backups is displayed in the **Backup History List**.
5. Click the link in the name field for the backup in which you want to view detailed information. The **Detailed Information** page appears. The **Detailed Information** page consists of two sections: the **Basic Information** section and the **Device Backup List**.

A list of all devices backed up is displayed in the **Device Backup List**.

### Device backup list

- **Device Name**: Contains the device label for the associated device. The contents of this field serve as a link to the **Device Details** page for the associated device.

- **Configuration File Name**: Contains the name of the backup file for the device’s configuration. The contents of this field serve as a link to view the details for the associated configuration file.

- **Configuration Type**: Identifies whether the configuration file that was backed up was a startup or running configuration file.

- **Result**: Identifies whether the backup **Succeeded**, or **Failed**. If failed, click the **Failed** link to view the cause for the backup failure.

- **Detail**: Contains an icon that displays the step-by-step detail for the configuration task.

- **Save As**: Contains an icon that opens the **Add Configuration Template** page for converting the backup configuration file into a configuration template. For more information on creating configuration templates, see "Managing device configurations with templates" (page 420).
You can sort the **Device Backup List** by every field with the exception of the **Operation** field. Click the column label to sort the list by the selected field. The column label is a toggle switch that lets you toggle between the various sort options specific to each field.

If the **Device Backup List** contains enough entries, the following navigational aids are displayed.

- Click the column label to sort the list by the selected field. The column label is a toggle switch that lets you toggle between the various sort options specific to each field.

6. **Click 8, 15, 50, 100, or 200 from the right side of the main pane to configure how many items per page you want to view.**

**Re-Executing a failed or partially successful backup**

To re-execute a failed or partially successful backup:

1. Navigate to **Service→Backup History Report.**
2. Click the **Service** tab from the tabular navigation system on the top.
3. Click the **Configuration Center** on the navigation tree on the left.
4. Click the **Backup History Report** under **Configuration Center** from the navigation system on the left.
   
   The **Backup History Report** page appears. A history of backups for all automatic and manual backups is displayed in the **Backup History List.**
5. Click the icon in the **Operation** field for the failed or partially successful backup you want to re-execute.
   
   The **Configuration File Backup Result** page is displayed and the result for each device entry is updated with the results of the backup.
6. Verify that all devices in the results page have been backed up successfully.

**Auditing configurations**

The **Configuration Audit** feature provides features for managing the task of auditing the configuration and software of network devices. The **Configuration Backup Report** provides you with a history of configuration file backups for all devices that are configured for backup. From this report, you can view the backup history of both the startup and running configuration file. IMC also provides you with a search/filter option for viewing by device name or file type or both. From the **Config Backup** page, you can also initiate a configuration file restore for one or more devices.

By using the **Configuration Baseline Report** feature, you can view IMC’s comparisons of the startup and running configuration files against the configured baseline files. If changes to the baseline exist, IMC acknowledges these changes and provides a link for the operator to manually compare the contents of the two files. From the **Config Baseline** page, you can launch the **Deployment Guide** to restore the baseline configuration to the device.

The **Software Update Report** provides you with software update histories for devices managed in IMC. With this software auditing feature, you can view the software update histories for all devices managed by IMC. From this page, you can also launch the **Deployment Guide** to restore selected software to the source device.

With the **Software Baseline Report**, you can compare the current system software against the configured baseline file. If differences exist between the baseline and the current system software, IMC acknowledges
these differences. From the Software Baseline page, you can launch the Deployment Guide to restore the baseline software to the device.

Configuration backup report

The Configuration Backup Report provides access to the backup history and files for all devices that IMC is configured to back up.

Accessing the configuration backup report

To access the Config Backup report:

1. Navigate to Service→Configuration Audit→Config Backup.
2. Click the Service tab from the tabular navigation system on the top.
3. Click the Configuration Center on the navigation tree on the left.
4. Click Config Backup under Configuration Audit on the left navigation tree.
5. To expand the section, click the expand button to the left of Configuration Audit. The Config Backup page appears.

Config Backup Report

- **Device Name**: Contains the device label or name.
- **Device Type**: Contains the model information for the associated device.
- **Latest Backup Time**: Contains the date and time stamp for the last backup of the configuration file type identified in the File Type field for the associated device.
- **File Name**: Contains the name of the backup file.
- **File Type**: Contains the type of configuration file that was backed up, startup or running configuration file.

You can sort the Config Backup report by every field. Click the column label to sort the list by the selected field. The column label is a toggle switch that lets you toggle between the various sort options specific to each field.

If the Configuration Backup Report has enough entries, the following navigational aids appear.

- Click to page forward in the Config Backup report.
- Click to page forward to the end of the Config Backup report.
- Click to page backward in the Config Backup report.
- Click to page backward to the front of the Config Backup report.

6. Click 8, 15, 50, 100, or 200 from the right side of the main pane to configure how many items per page you want to view.

Querying the configuration backup report

IMC provides the ability to search for a particular configuration backup report entry.

To search the Config Backup report:

1. Navigate to Service→Configuration Audit→Configuration Backup.
2. Click the Service tab from the tabular navigation system on the top.
3. Click the Configuration Center on the navigation tree on the left.
4. Click Config Backup under Configuration Audit on the left navigation tree.
To expand the section, click the expand button to the left of Configuration Audit. The Config Backup page appears.

5. Enter one or more of the following search criteria in the Device Query section of the page:
   - **Device Name**: To locate the configuration backup files for a particular device, enter a partial or complete device label or name in the Device Name field.
   - **File Type**: To filter the Configuration Backup Report for a particular configuration file type, select the type from the File Type list.

6. Click Query to submit your filter criteria.
   - The results of your filter or search query is displayed in the Config Backup list.

7. Click Reset when you want to restore the full Config Backup report.

### Restoring a configuration file from the configuration backup report page

The Restore button on the Config Backup page provides a link to the Deployment Guide wizard for restoring configuration files. For more information on using the Deployment Guide for updating or restoring device configurations, see "Restoring a device configuration" (page 445).

### Exporting a configuration file from the configuration backup report page

You can export the contents of a configuration file to a file on the operator’s local computer.

To export a configuration file to your local computer:

1. Navigate to Service→Configuration Audit→Config Backup.
2. Click the Service tab from the tabular navigation system on the top.
3. Click the Configuration Center on the navigation tree on the left.
4. Click Config Backup under Configuration Audit on the left navigation tree. Expand the section by clicking the expand button to the left of Configuration Audit.
   - The Config Backup page appears.
5. Click the checkbox to the left of the combination of device name and configuration file type you want to export.
6. Click Export.
   - The Download Exported Device Configuration page appears.
7. Click the Download Exported Device Configuration link to download the file to your local computer.
8. Follow your browser’s instructions for saving the file to your computer.

### Configuration baseline report

The Configuration Baseline Report provides the ability to view IMC’s comparison of a device’s most current startup and running configuration files against its configured baseline configuration files.

With this feature, IMC identifies when the last backed up configuration file does not match the configured baseline. IMC provides the ability to restore selected files from the Config Baseline page for those devices where running or startup configuration files do not match their baseline.

### Viewing the configuration baseline report

To access the Config Baseline report:

1. Navigate to Service→Configuration Audit→Config Baseline.
2. Click the **Service** tab from the tabular navigation system on the top.

3. Click the **Configuration Center** on the navigation tree on the left.

4. Click **Config Baseline** under **Configuration Audit** on the left navigation tree. Expand the section by clicking on the expand button [+ ] to the left of **Configuration Audit**.

   The **Config Baseline** page appears.

**Config baseline report**

- **Device Name**: Contains the device label or name.
- **Device Model**: Contains the model information for the associated device.
- **Last Backup Configuration**: Contains the filename of the last backed up configuration file for the file type identified in the **File Type** field.
- **Baseline Configuration**: Contains the name of the baseline configuration file.
- **File Type**: Contains the type of configuration file that was last backed up, startup or running configuration file.
- **Audit Result**: Contains the result of IMC’s comparison of the last backed up file and its configured baseline.

The value **Identical** indicates that the last backed up configuration file matches the configured baseline configuration file.

The value **Changed** indicates that the last backed configuration file does not match the configured baseline configuration file. The **Compare** link in this field launches the **Configuration Compare** feature for comparing the last backed up configuration file against the configured baseline configuration file. For more information on using this option, see “Comparing files in the configuration baseline report” (page XX).

The value **Unknown** indicates that IMC could not make a comparison between the last backed up configuration file and the configured baseline configuration file. You can sort the **Config Baseline** report by all fields. Click the column label to sort the list by the selected field. The column label is a toggle switch that lets you toggle between the various sort options specific to each field.

If the **Config Baseline** report has enough entries, the following navigational aids are displayed.

- Click [ ] to page forward in the **Configuration Baseline** report.
- Click [ ] to page forward to the end of the **Configuration Baseline** report.
- Click [ ] to page backward in the **Configuration Baseline** report.
- Click [ ] to page backward to the front of the **Configuration Baseline** report.

5. Click **8, 15, 50, 100, or 200** from the right side of the main pane to configure how many items per page you want to view.

**Querying the configuration baseline report**

IMC provides the ability to search for a particular **Configuration Baseline Report** entry.

To search the **Config Baseline** report:

1. Navigate to **Service**→**Configuration Audit**→**Config Baseline**.
2. Click the **Service** tab from the tabular navigation system on the top.
3. Click the **Configuration Center** on the navigation tree on the left.
4. Click **Config Baseline** under **Configuration Audit** on the left navigation tree. Expand the section by clicking the expand button [+ ] to the left of **Configuration Audit**.
The Config Baseline page appears.

5. Enter one or more of the following search criteria in the Device Query section of the page:
   - **Device Name**: To locate the configuration backup files for a particular device, enter a partial or complete device label or name in the Device Name field.
   - **Audit Result**: To filter the Configuration Baseline Report for a particular audit result, select the result from the Audit Result list.
   - **File Type**: To filter the Configuration Baseline Report for a particular configuration file type, select the type from the File Type list.

6. Click **Query** to submit your filter criteria.
   The results of your filter or search query is displayed in the **Config Baseline** list.

7. Click **Reset** when you want to restore the full **Config Baseline** report.

### Comparing files in the configuration baseline report

If **Changed** is displayed for the Audit Result field, you can click the **Compare** link to view the baseline configuration changes for the device. To compare the last backed up configuration file against the configured baseline file for the selected device:

1. Navigate to **Service→Configuration Audit→Config Baseline**.
2. Click the **Service** tab from the tabular navigation system on the top.
3. Click the **Configuration Center** on the navigation tree on the left.
4. Click **Config Baseline** under **Configuration Audit** on the left navigation tree. Expand the section by clicking the expand button + to the left of **Configuration Audit**.
   The **Config Baseline** page appears.
5. Click the **Compare** link in the Audit Result field for the device you want to compare files for.
   The **Compare Configuration File** dialog box appears.
   The two startup configuration files are displayed in side-by-side windows with file details at the top of the dialog box.
   IMC provides a summary of all identical, changed, and unique lines at the bottom of the dialog box.
6. Do one of the following:
   - To view the entire contents of both configuration files, click the radio button ○ to the left of **Show All**, or
   - To view only the differences between the two files, click the radio button ○ to the left of **Show Difference Only**.
7. Do one of the following:
   - Click **Next Diff** to view, line-by-line, the configuration differences between the two files, or
   - Click **Previous Diff** to view the previous line that contains differences.
8. Click **Close** when you have finished viewing the configuration file comparison.

### Restoring a configuration file from the configuration baseline report page

The **Restore** button on the **Config Baseline** page provides a link to the **Deployment Guide** wizard for restoring configuration files. For more information on using the **Deployment Guide** for updating or restoring device configurations, see “Restoring a device configuration” (page 445).
Software update report

The Software Update Report provides software update histories for devices managed in IMC. With this system software auditing feature, you can view the software update histories for devices managed by IMC. From this page, you can also launch the Deployment Guide to restore selected software to the source device.

Viewing the software update report

To access the Software Update report:
1. Navigate to Service→Configuration Audit→Software Update.
2. Click the Service tab from the tabular navigation system on the top.
3. Click the Configuration Center on the navigation tree on the left.
4. Click Software Update under Configuration Audit on the left navigation tree. Expand the section by clicking the expand button + to the left of Configuration Audit.

The Software Update page appears.

Software update report

- **Device Name**: Contains the device label or name.
- **Device Type**: Contains the model information for the associated device.
- **Latest Update Time**: Contains the date and time stamp for the last software update for the associated device.
- **Before Software Name**: Contains the file name of the system software that was replaced with the system software specified in the **After Software Name** field.
- **After Software Name**: Contains the file name of the system software that was used to update the system software specified in the **Before Software Name** field.

You can sort the Software Update report by all fields. Click the column label to sort the list by the selected field. The column label is a toggle switch that lets you toggle between the various sort options specific to each field.

If the Software Update report has enough entries, the following navigational aids are displayed.

- Click ➡️ to page forward in the Software Update report.
- Click ⬅️ to page backward to the end of the Software Update report.
- Click ⬅️ to page backward in the Software Update report.
- Click ⬅️ to page backward to the front of the Software Update report.
5. Click 8, 15, 50, 100, or 200 from the right side of the main pane to configure how many items per page you want to view.

Querying the software update report

You can search for a particular Software Update Report entry.

To search the Software Update report:
1. Navigate to Service→Configuration Audit→Software Update.
2. Click the Service tab from the tabular navigation system on the top.
3. Click the Configuration Center on the navigation tree on the left.
4. Click **Software Update** under **Configuration Audit** on the left navigation tree. Expand the section by clicking the expand button to the left of **Configuration Audit**.

The **Software Update** page appears.

5. Enter the following search criterion in the **Device Query** section of the page:
   - **Device Name**: To locate the configuration backup files for a particular device, enter a partial or complete device label or name in the **Device Name** field.

6. Click **Query** to submit your filter criterion.

   The results of your filter or search query are displayed in the **Software Update** list below.

7. Click **Reset** when you want to restore the full **Software Update** report.

**Restoring a software file from the software update report page**

The **Restore** button on the **Software Update** page provides quick link to the **Deployment Guide** wizard for updating or restoring system software. For more information on using the **Deployment Guide** for updating or restoring system software, see "Restoring device software" (page 445).

**Software baseline report**

The **Software Baseline Report** provides the ability to compare a device’s most current system software against its configured baseline system software file. IMC identifies when the current software file does not match the configured baseline software.

IMC also provides the ability to restore selected files from the **Software Baseline** page for those devices where current software does not match the baseline.

**Viewing the software baseline report**

To access the **Software Baseline** report:

1. Navigate to **Service**→**Configuration Audit**→**Software Baseline**.
2. Click the **Service** tab from the tabular navigation system on the top.
3. Click the **Configuration Center** on the navigation tree on the left.
4. Click **Software Baseline** under **Configuration Audit** on the left navigation tree. Expand the section by clicking the expand button to the left of **Configuration Audit**.

The **Software Baseline** page appears.

**Software baseline report**

- **Device Name**: Contains the device label or name.
- **Device Type**: Contains the model information for the associated device.
- **Current Software**: Contains the filename of the software currently running on the associated device.
- **Baseline Software**: Contains the name of the software file that is configured as the baseline software for the associated device.
- **Audit Result**: Contains the result of IMC’s comparison of the current software file and it’s configured baseline.

The value **Identical** indicates that the current software file matches the configured baseline software file.
The value **Changed** indicates that the current software file does not match the configured baseline file.

The value **Unknown** indicates that IMC could not make a comparison between the current software file and the configured baseline software file.

You can sort the **Software Baseline** report by all fields. Click the column label to sort the list by the selected field. The column label is a toggle switch that lets you toggle between the various sort options specific to each field.

If the **Software Baseline** report has enough entries, the following navigational aids appear.

- Click **»** to page forward in the **Software Baseline** report.
- Click **«** to page forward to the end of the **Software Baseline** report.
- Click **«** to page backward in the **Software Baseline** report.
- Click **»** to page backward to the front of the **Software Baseline** report.

5. Click 8, 15, 50, 100, or 200 from the right side of the main pane to configure how many items per page you want to view.

**Querying the software baseline report**

You can search for a particular software baseline report entry.

To search the **Software Baseline** report:

1. Navigate to **Service**→**Configuration Audit**→**Software Baseline**.
2. Click the **Service** tab from the tabular navigation system on the top.
3. Click the **Configuration Center** on the navigation tree on the left.
4. Click **Software Baseline** under **Configuration Audit** on the left navigation tree. Expand the section by clicking the expand button **»** to the left of **Configuration Audit**.

The **Software Baseline** page appears.

5. Enter one or more of the following search criteria in the **Device Query** section of the page:
   - **Device Name**: To locate the configuration backup files for a particular device, enter a partial or complete device label or name in the **Device Name** field.
   - **Audit Result**: To filter the **Software Baseline** report for a particular audit result, select the result from the **Audit Result** list.
   - **Custom View**: To filter the **Software Baseline** report for devices in a custom view, select the custom view from the Custom View list. You can also choose the blank option, which searches all custom views.

6. Click **Query** to submit your filter criteria.

   The results of your filter or search query are displayed in the **Software Baseline** list below.

7. Click **Reset** when you want to restore the full **Software Baseline** report.

**Restoring a software file from the software baseline report page**

The **Restore** button on the **Software Update** page provides a link to the **Deployment Guide** wizard for updating or restoring system software. For more information on using the **Deployment Guide** for updating or restoring system software, see "Restoring device software" (page 445).
Compliance check

Compliance check verifies whether configurations on devices are compliant with compliance policies and shows the check results in various forms. In addition, compliance check can fix incompliant configurations to make sure the network operates in a secure, stable environment.

To perform compliance check, you need to configure a check task, associate it to a compliance policy, and execute the check task immediately or periodically.

A compliance policy comprises multiple rules, and each rule corresponds to a violation severity level. IMC provides some system-defined compliance policies that cannot be modified. You can add, modify, and delete your own compliance policies and their rules as needed.

IMC shows the check results in policy view for analysis from the compliance policy’s perspective, in device view for analysis from the device’s perspective, and in the execution report for analysis from a comprehensive perspective.

Compliance check can also check whether the output of specific display commands is compliant with the associated compliance policy. You need to add the display commands in the rules of the compliance policy.

Compliance policy

IMC performs compliance check according to compliance policies. A compliance policy comprises a set of rules and each rule defines the violation severity level, check type, check target, vendor and product series under check, recovery commands, and the content to be checked. The following sections describe how to configure and maintain compliance policies and their rules.

Viewing the compliance policy list

To access the policy list:

1. Navigate to Service→Compliance Policy
2. Click the Service tab from the tabular navigation system on the top.
3. Click the Compliance Center on the navigation tree on the left.
4. Click Compliance Policy under Compliance Center on the left navigation tree.

The Policy List appears.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Contains the name of the compliance policy. The contents of this field serve as a link for navigating to the Compliance Policy Details page for the associated policy.</td>
</tr>
<tr>
<td>Description</td>
<td>Contains a description for the compliance policy.</td>
</tr>
<tr>
<td>Status</td>
<td>Shows the status of the compliance policy. ✗ means the policy is disabled and you can click it to enable the policy, ✔ means the policy is enabled and you can click it to disable the policy. Only enabled compliance policies can be associated with check tasks.</td>
</tr>
<tr>
<td>Type</td>
<td>Identifies whether the associated compliance policy is System Defined or User Defined.</td>
</tr>
<tr>
<td>Modify</td>
<td>Contains a link 📝 for modifying the associated compliance policy.</td>
</tr>
<tr>
<td>Delete</td>
<td>Contains a link ✗ for deleting the associated compliance policy. System defined policies cannot be modified or deleted. Only user defined policies can be modified and deleted.</td>
</tr>
</tbody>
</table>
You can sort the Policy List by the Name, Description, Status, and Type fields by clicking the column label to sort the list by the selected field. The column label is a toggle switch that allows you to toggle between the various sort options specific to each field.

If the Policy List contains enough entries, the following navigational aids are displayed.

- Click to page forward in the Policy List.
- Click to page forward to the end of the Policy List.
- Click to page backward in the Policy List.
- Click to page backward to the front of the Policy List.

5. Click 8, 15, 50, 100, or 200 from the right side of the main pane to configure how many items per page you want to view.

6. Click Start Check to enter the Add Check Task page.

**Viewing detailed information about a compliance policy**

To view detailed information about a compliance policy:

1. Navigate to Service→Compliance Policy
2. Click the Service tab from the tabular navigation system on the top.
3. Click the Compliance Center on the navigation tree on the left.
4. Click Compliance Policy under Compliance Center on the left navigation tree.
   The Policy List appears.
5. Click the name link of a compliance policy to enter the Compliance Policy Details page.

**Basic information**

- **Name**: Contains the name of the compliance policy.
- **Type**: Contains the type of the compliance policy, System Defined or User Defined.
- **Description**: Contains the description for the compliance policy.

**Rule list**

- **Name**: Contains the name of the rule. Click this link to view detailed information about the rule.
- **Type**: Contains the type of the rule, System Defined or User Defined.
- **Severity Level**: Contains the violation severity level of the rule.
- **Check Type**: Contains the object to be checked. Options include Device, Interface, Link, Aggregate Link, Configuration Segment, and Jython Script.
- **Test**: Click this link to enter the test page where you can perform a test to verify the function and validity of this rule.

Only the rules whose Check Type is Device, Interface, or Configuration Segment can be tested.

**Performing a test**

To perform a test:

1. Click the link to enter the Rule Test page.
2. Enter the test content in the text box under Test Content or import a configuration file from the configuration template database.
3. Click Test.
After the test is complete, the test results show whether the test content or configuration file matches the rule. You can judge whether the rule achieves your purpose according to the test results.

4. To clear the test content and result, click Reset.

Viewing detailed information about a rule

To view detailed information about a rule:

1. Navigate to Service→Compliance Policy.
2. Click the Service tab from the tabular navigation system on the top.
3. Click the Compliance Center on the navigation tree on the left.
4. Click Compliance Policy under Compliance Center on the left navigation tree. The Policy List appears.
5. Click the name link of a compliance policy to enter the Compliance Policy Details page.
6. Click the name link of a rule to enter the Rule Details page.

Basic information

- **Name**: Contains the name of the rule.
- **Type**: Contains the type of the rule, System Defined or User-Defined.
- **Severity Level**: Contains the violation severity level of the rule. Options include Informational, Warning, Minor, Major, and Critical.
- **Check Target**: Contains the check target of the rule. Options include Latest backup running configuration, Latest backup startup configuration, and Display command output.
- **Command**: Contains the display command. After IMC assigns this task, the target device executes this display command and checks whether the command output matches the rule. The Command field is available only when the Check Target is Display command output.
- **Vendor**: Contains the device vendor to be checked.
- **Device Series**: Contains the device series to be checked.
- **Check Type**: Contains the check type. Options include Device, Interface, Link, Aggregate Link, Configuration Segment, and Jython Script.
- **Start Identifier**: Contains the start identifier of the content to be checked when the check type is Link, Aggregate Link, or Configuration Segment.
- **End Identifier**: Contains the end identifier of the content to be checked when the check type is Link, Aggregate Link, or Configuration Segment.
- **Description**: Contains the description for the rule.
- **Rule Type**: This field is displayed only when the rule type is Advanced.
- **Operation**: Contains the operation mode of the rule, Check or Check and Get. The Check operation only checks the configuration file content. The Check and Get operation checks the configuration file content and gets relevant parameters according to the rule. When the check type is Link or Aggregate Link, the Check and Get operation gets relevant parameters according to the rule and compares the parameters to predefined values according to the comparison mode to check whether the device configuration matches the compliance policy. For other check types, the Check and Get operation only gets relevant parameters and displays them in the Configuration Retrieval Report.

The following describes the configuration items for basic and advanced rules respectively.
Basic
- **Rule Type**: Contains the rule type.
- **Match Mode**:
  - **Loose Match**: In this mode, a match occurs when the content in the configuration file or display command output contains the content in the rule.
  - **Negative Loose Match**: In this mode, a match occurs when the content in the configuration file or display command output does not contain the content in the rule.
  - **Strict Match**: In this mode, a match occurs only if the content in the configuration file or display command output appears in the same order as specified in the rule.
  - **Negative Strict Match**: In this mode, a match occurs only if the content in the configuration file or display command output does not appear in the same order as specified in the rule.
- **Match Patterns**: IMC compares the match patterns to the configuration content on the device, and determines whether the device violates the rule according to the match mode.

Advanced
When the rule contains only one match pattern, the following are displayed.
- **Rule Type**: Contains the type of the rule.
- **Operation**: Contains the operation mode of rule, **Check** or **Check and Get**.
- **Match Patterns**: Contains the content of the rule or regular expression.

When the rule contains multiple match patterns, the following are displayed.
- **Rule Relation**: **AND** or **OR**, displayed only when the rule type is Advanced. If the rule relation is **AND**, the two adjacent patterns must be found in the configuration file. If the rule relation is **OR**, only one of the two adjacent patterns must be found in the configuration file.
- **Rule Content Configuration**: **Included** or **Excluded**, displayed only when the check type is **Device**, **Interface**, or **Configuration Segment**.
  - **Included**: A match occurs if the device configuration contains the match patterns of the rule.
  - **Excluded**: A match occurs if the device configuration does not contain the match patterns of the rule.
- **Match Criteria**: Displayed when the check type is **Link** or **Aggregate Link**.
  - **Contain all**: A match occurs when both ends of a link have the match patterns of the rule in their configuration files.
  - **Contain none of them**: A match occurs when both ends of a link do not have the match patterns of the rule in their configuration files.
  - **Contain one of them**: A match occurs when at least one end of a link has the match patterns of the rule in its configuration file.
  - **Contain all but one**: A match occurs when at least one end of a link does not have the match patterns of the rule in its configuration file.
- **Match Patterns**: IMC compares the match patterns against the configuration content on the device.
- **Comparison Type**: IMC compares the values of the two interfaces according to the comparison type. Options include **All equal to**, **All not equal to**, **One of them equal to**, **One of them not equal to**, and **All Identical**. Configure the comparison type when the check type is **Link** or **Aggregate Link**, or when the check type is Advanced and the operation mode is **Check and Get**.
- **Value for Comparison**: IMC compares this value to the value obtained from the device. Use this item together with **Comparison Type**.
When the check type is **Jython Script**, the name information for the Jython script is displayed in the text box next to **Script Directory Information** in the **Jython Script** area.

7. Click **Back** to return to the **Compliance Policy List** page.

**Query a compliance policy**

To query a compliance policy:

1. Navigate to **Service→Compliance Policy**.
2. Click the **Service** tab from the tabular navigation system on the top.
3. Click the **Compliance Center** on the navigation tree on the left.
4. Click **Compliance Policy** under **Compliance Center** on the left navigation tree. The **Policy List** appears.
5. Enter a partial or complete name of a compliance policy in the **Name** box under **Query Condition**.
6. Click **Query**.

All matching compliancy policies are displayed in the **Policy List**.

**Create a compliance policy**

To create a compliance policy:

1. Navigate to **Service→Compliance Policy**.
2. Click the **Service** tab from the tabular navigation system on the top.
3. Click the **Compliance Center** on the navigation tree on the left.
4. Click **Compliance Policy** under **Compliance Center** on the left navigation tree. The **Policy List** appears.
5. Click **Add**.
6. Enter a name of the compliance policy, a string of 1 to 32 characters.
7. Enter a description for the compliance policy, a string of 0 to 128 characters.

You can add a new rule or import a rule from another compliance policy into the compliance policy.

**Add rule**

To add a rule:

1. Click **Add Rule** under **Rule List**.
2. Enter the name of the rule, a string of 1 to 32 characters.
3. Select the violation severity level for the rule by selecting the radio button to the left of **Severity Level**.

Options include: **Informational**, **Warning**, **Minor**, **Major**, and **Critical**.

4. Select the check type. Options include **Device**, **Interface**, **Link**, **Aggregate Link**, **Configuration Segment**, and **Jython Script**.
5. Do one of the following:
   - If you select **Interface** or **Configuration Segment**, go to **Step 6**.
   - If you select **Link** or **Aggregate Link**, go to **Step 10**.
   - If you select **Device**, go to **Step 3**.
   - If you select **Jython Script**, go to **Step 17**.
6. Set the start and end identifiers.
7. In the **Start Identifier** text box, enter the start identifier of the interface to be checked, for example, enter interface `*`.
8. In the **End Identifier** text box, enter the end identifier of the interface configuration, for example, enter `#` or `!`.
   The rule checks the configuration segment according to the start and end identifiers.
9. Go to **Step 13**.
10. Set the start and end identifiers.
11. In the **Start Identifier** text box, enter the start identifier of the target link and interface description.
    The actual start identifier comprises the value you entered and the interface description.
12. In the **End Identifier** text box, enter the end identifier of the link configuration.
    For example, enter `#` or `!`.
    The rule checks the configuration segment according to the start and end identifiers.
13. Select the check target from the **Check Target** list.
    Options include **Latest backup running configuration**, **Latest backup startup configuration**, and **Display command output**.
14. Do one of the following:
   o If you select **Latest backup running configuration** or **Latest backup startup configuration**, go to **Step 17**, or
   o If you select **Display command output**, go to **Step 15**.
15. Enter a **display** command in the text box next to **Command**, or select a **display** command as follows.
   a. Click **Select** next to the text box.
   b. In the window that displays, enter a partial or complete **display** command in the text box next to **Name of Display Command**, all qualified **display** commands are displayed in the **Command List**.
   c. Click the **radio button** of the desired **display** commands.
      The selected commands are displayed in the text box next to **Command**.
      The variables such as the dollar sign ($) are not supported. For example, a **display** command cannot contain ${ip address}.
16. Select a vendor from the **Vendor** list for the rule.
    The rule only checks the devices of the selected vendor.
17. Select the device series to be checked.
18. Click **Select** next to **Device Series**.
19. In the **Select Device Series** window that appears, enter the partial or complete name of the device series, and click **Query**.
    All the qualified device series are displayed in the **Device Series List**.
    If the device series contains enough entries, the following navigational aids are displayed.
   o Click **to page forward** in the **Device Series List**.
   o Click **to page forward** to the end of the **Device Series List**.
   o Click **to page backward** in the **Device Series List**.
   o Click **to page backward** to the front of the **Device Series List**.
20. Select the □ check box of the target device series, and click OK. The selected device series are displayed in the area next to Device Series.

21. To delete a device series, select it and click Delete.

22. Enter a description for the rule in the text box next to Description, a string of 1 to 128 characters.

23. If the check type selected in Step 4 is not Jython Script, go to Step 24.

24. Click Browse next to Jython Script, and select a local Jython script.

If you select Device, Interface, or Configuration Segment in Step 4, the Recover option appears.

Modifying incompliant settings

To modify the incompliant settings:

1. Select the ☐ radio button.

2. Click Yes, and enter the commands to be applied on the device. IMC uses the commands to modify the incompliant settings. If you click No, IMC does not modify the settings.

3. Select the rule type from the Rule Type list, Basic or Advanced. If you select Advanced, go to Step 6.

4. Select the match mode you want to use from the Match Mode list. Options include:
   - Loose Match: In this mode, a match occurs when the content in the configuration file or display command output contains the content in the rule.
   - Negative Loose Match: In this mode, a match occurs when the content in the configuration file or display command output does not contain the content in the rule.
   - Strict Match: In this mode, a match occurs only if the content in the configuration file or display command output appears in the same order as specified in the rule.
   - Negative Strict Match: In this mode, a match occurs only if the content in the configuration file or display command output does not appear in the same order as specified in the rule.

5. Enter the string you want IMC to search for in the Match Patterns field. Go to Step 42.

6. Select the operation mode from the Operation field, Check or Check and Get. The Check operation only checks the configuration file for selected devices. The Check and Get operation checks and retrieves the configuration settings for the selected devices. The check results are displayed in the Configuration Retrieval Report. For more information about the Configuration Retrieval Report, see “View configuration retrieval report” (page 521).

7. If you select Check and Get, go to Step 32. If the check type selected is Link or Aggregate Link, go to Step 10.

8. Select the match mode from the Match Mode list. This option is available when the check type is Device, Interface, or Configuration Segment. Two options provided for the advanced rule type are described below:
   - Included: A match occurs if the device configuration contains the match patterns of the rule.
   - Excluded: A match occurs if the device configuration does not contain the match patterns of the rule.

9. Go to Step 11.

10. Select the match criteria from the Match Criteria list. This option is available when the check type is Link or Aggregate Link. Four options provided for the advanced rule type are described below:
   - Contain all: A match occurs when both ends of a link have the match patterns of the rule in their configuration files.
- **Contain none of them**: A match occurs when both ends of a link do not have the match patterns of the rule in their configuration files.

- **Contain one of them**: A match occurs when at least one end of a link has the match patterns of the rule in its configuration file.

- **Contain all but one**: A match occurs when at least one end of a link does not have the match patterns of the rule in its configuration file.

11. Enter the pattern or regular expression in the **Match Patterns** field.

12. Click **Add** to add it to the rule.

13. To add a new pattern, select the logical operator from the **Rule Relation** list:
   Options include **AND** and **OR**.
   - If you choose **AND**, the two adjacent patterns must be found in the configuration file.
   - If you choose **OR**, only one of the two adjacent patterns must be found in the configuration file.

   IMC checks contents against the match patterns in sequence. You can have more than two patterns for one rule and use more than one logical operator in a given rule.

14. Select the match mode from the **Match Mode** list. If the check type is **Link** or **Aggregate Link**, select the match criteria from the **Match Criteria** list.

15. Enter the pattern or regular expression.

16. Click **Add** to add the pattern to the rule.

17. Repeat **Steps 8-16** to add more patterns to the rule in the **Match Patterns** field.

18. Enter a match pattern or regular expression for the rule in the text box next to **Match Patterns**. If the check type selected is not **Link** or **Aggregate Link**, go to **Step 28**.

19. Select a comparison type from the **Comparison Type** list. Options include the following.
   - **All equal to**: IMC uses the match pattern entered in **Step 18** to retrieve the target value from both devices on a link, and compares the retrieved value to the value entered in **Step 20**. If they match for both devices, both devices are matched; otherwise, both devices are violated.
   - **All not equal to**: IMC uses the match pattern entered in **Step 18** to retrieve the target value from both devices on a link, and compares the retrieved value to the value entered in **Step 20**. If no match is found for both devices, both devices are matched; otherwise, both devices are violated.
   - **One of them equal to**: IMC uses the match pattern entered in **Step 18** to retrieve the target value from both devices on a link, and compares the retrieved value to the value entered in **Step 20**. If they match for both devices, both devices are matched; otherwise, both devices are violated.
   - **One of them not equal to**: IMC uses the match pattern entered in **Step 18** to retrieve the target value from both devices on a link, and compares the retrieved value to the value entered in **Step 20**. If no match is found for both devices, both devices are matched; otherwise, both devices are violated.
   - **All Identical**: IMC uses the match pattern entered in **Step 18** to retrieve the target value from both devices on a link, and compares the values of the two devices. If they match, both devices are matched; otherwise, both devices are violated.

20. Enter a value in the **Value for Comparison** text box when the comparison type selected in **Step 19** is not **All Identical**.

   IMC compares the value with the value retrieved from devices.

21. Click **Add** next to **Value for Comparison** to add the match condition combination to the rule.

22. To add a new **Value for Comparison**, select a logical operator from the **Rule Relation** list.
   Options include **AND** and **OR**.
If you choose **AND**, the two adjacent values must be found in the configuration file.

If you choose **OR**, only one of the two adjacent values must be found in the configuration file.

IMC checks contents against the match patterns in sequence.

23. Select a comparison type from the **Comparison Type** list as described in **Step 19**.

24. Enter a value in the **Value for Comparison** text box if the comparison type selected in **Step 23** is not **All Identical**. IMC compares the entered value to the value retrieved from the devices.

25. Click **Add** next to **Value for Comparison** to add the match condition combination to the rule.

26. Repeat **Steps 18-25** to add more match conditions of the **Check and Get** type to the rule.

27. If the check type is **Link** or **Aggrerate Link**, repeat **Steps 6-26** to add more different types of match conditions to the rule.

28. Click **OK**.

29. The newly created rule is displayed in the **Rule List**.

**Import rule**

To import a rule from another compliance policy:

1. Click **Import Rule** under **Rule List**.

   The **Select Rules** window pops up. All compliance policies are displayed in the **Policy List**.

2. Click the name link of a compliance policy to show all rules.

3. Select a rule by selecting its □ check box, or select all rules by selecting the □ check box left to the compliance policy name.

4. Click **OK**.

   The selected rules are displayed in the **Rule List**.

5. Click the  button of a rule to modify the rule.

6. Click the  button of a rule to test the rule.

7. Enter the test content in the text box under **Test Content**, or import the test results from a configuration template.

8. Click **Test**.

   After the test is complete, IMC shows whether the test content or configuration file matches the rule. The test function is available only for rules whose check type is **Device**, **Interface**, or **Configuration Segment**. You can judge whether the rule achieves your purpose according to the test results.

9. To delete a rule, click the  link of that rule.

10. Click **OK**.

11. Verify that the added compliance policy is in the **Policy List**.

**Modifying a compliance policy**

To modify a compliance policy:

1. Navigate to **Service**→**Compliance Policy**.

2. Click the **Service** tab from the tabular navigation system on the top.

3. Click the **Compliance Center** on the navigation tree on the left.

4. Click  **Compliance Policy** under **Compliance Center** on the left navigation tree.

   The **Policy List** appears.
5. Click the link for the policy to enter the Modify Compliance Policy page. 
   System Defined configuration check rules cannot be modified. Only User Defined configuration check rules can be modified.
6. Delete the existing description, and enter a new description (0 to 128 characters) for the policy.
7. Add rules as required. For information on how to add a rule, see “Create a compliance policy” (page 494).
8. To modify a rule, click the link for the rule to enter the modification page. 
   You cannot change the rule name.
9. Select the severity level by clicking the radio button to the left of the severity level. 
   Options include Informational, Warning, Minor, Major, and Critical.
10. Select a check type from the Check Type list. 
    Options include Device, Interface, Link, Aggregate Link, Configuration Segment, and Jython Script. 
    These types are described respectively in the following steps.
11. Do one of the following: 
    o If you selected Interface or Configuration Segment, go to Step 12, or 
    o If you selected Link or Aggregate Link, go to Step 16, or 
    o If you selected Device, go to Step 19, or 
    o If you selected Jython Script, go to Step 23.
12. Set the start identifier and end identifier.
13. In the Start Identifier field, enter the start identifier, such as interface *.
14. In the End Identifier field, enter the end identifier, such as # or !. 
   The rule checks the configuration segment according to the start and end identifiers.
15. Go to Step 19.
16. Set the start identifier and end identifier for link configuration check 
17. In the Start Identifier field, enter the start identifier. The actual start identifier comprises the value you 
    entered and the interface description.
18. In the End Identifier field, enter the end identifier, such as # or !. 
    The rule checks the configuration segment according to the start and end identifiers.
19. Select the check target from the Check Target list. 
    Options include Latest backup running configuration, Latest backup startup configuration, and 
    Display command output.
20. If you selected Latest backup running configuration or Latest backup startup configuration, go to Step 29.
21. Type a display command in the field or select a display command from the command fragment.
22. Click Select to bring up the Select window.
23. In the Name of Display Command field, type the command or part of the command. 
    All commands matching your input is displayed in Command List.
24. Select a command and click OK. 
    The selected command displays in the command field. The variables such as $ are not supported. For 
    example, a display command cannot contain ${ip address}.
25. Select a vendor from the **Vendor** list.
26. Select a device series.
27. Click the **Select** button to the right of the device series area.
   The **Select Device Series** dialog box appears.
28. Type the device series name or part of the name in the **Device Series Name** field, and click **Query**. All matching device series are displayed in the **Device Series List**.
   If the query result contains enough entries, the following navigational aids are displayed.
   - Click **»** to page forward in the **Device Series List**.
   - Click **↓** to page forward to the end of the **Device Series List**.
   - Click **«** to page backward in the **Device Series List**.
   - Click **↑** to page backward to the front of the **Device Series List**.
   - Click a page number to display the entries on the page.
   - To select a device series, click the check box to the left of the device series and click **OK**. The selected device series is displayed in the area to the right of the **Device Series**.
   - To delete a device series, select a device series and click **Delete**.
29. Enter a new description (1 to 128 characters) for the rule in the **Description** field.
30. Click **Browse** to the right of the **Jython script** area to locate the Jython script.  
   If you selected **Device**, **Interface**, or **Configuration Segment**, the **Recover** option appears.
31. Click the radio button **☐** for **Yes** or **No** to the right of the **Recover** option:
   - If you select **Yes**, enter the fix command in the text box to the right of **Recovery Commands**. IMC uses this command to fix configuration files not compliant with the rule.
   - If you select **No**, IMC does nothing.
32. Select a rule type for the rule.
33. Select a rule type for the rule from the **Rule Type** list.
   Options include **Basic** and **Advanced**.
34. Select the match mode you want to use from the **Match Mode** list. Four options are provided for a basic configuration check file and each option as follows:
   - **Loose Match**: With this option, IMC matches on the presence of any words provided in the rule. If the configuration file or the display command results includes the rule content, IMC considers the device compliant with the policy.
   - **Negative Loose Match**: With this option, IMC matches on the presence of any words provided in the rule. If the configuration file or the display command result does not include the rule content, IMC considers the device compliant with the policy.
   - **Strict Match**: With this option, IMC considers the content in the rule a match with the content in the configuration file or display command result only if they appear in the same order as specified in the rule.
   - **Negative Strict Match**: With this option, IMC considers the content in the rule a match with the content in the configuration file or display command result only if they do not appear in the same order as specified in the rule.
35. Enter the pattern or regular expression in the **Match Patterns** field.
36. Select the type of rule check operation you want to perform with this rule from the **Operation** field: a configuration **Check** or a configuration **Check and Get**.
A configuration **Check** checks the configuration for all selected devices.

A configuration **Check and Get** checks and retrieves the configuration settings for the selected devices. **Check and Get** results are displayed in the Configuration Retrieval Report. For more information on the Configuration Retrieval Report, see “View configuration retrieval report” (page 521).

37. Select the pattern matching method you want to use from the **Match Mode** list. Two options are provided for an advanced configuration check file and each option is described below:
   - **Included**: If the configuration includes the rule content defined in the **Match Pattern**, the configuration is considered compliant with the policy.
   - **Excluded**: If the configuration does not include the rule content defined in the **Match Pattern**, the configuration is considered compliant with the policy.

38. Select the pattern matching method you want to use from the **Match Criteria** list. Four options provided for an advanced configuration check file and each option is described below:
   - **Contain all**: When the configuration files of the devices at the two ends of the link both include the rule content defined in the **Match Patterns**, the configurations are considered compliant with the policy.
   - **Contain none of them**: When neither of the configuration files of the devices at the two ends of the link includes the rule content defined in the **Match Patterns**, the configurations are considered compliant with the policy.
   - **Contain one of them**: When at least one of the configuration files of the devices at the two ends of the link includes the rule content defined in the **Match Patterns**, the configurations are considered compliant with the policy.
   - **Contain all but one**: When at least one of the configuration files of the devices at the two ends of the link do not include the rule content defined in the **Match Patterns**, the configurations are considered compliant with the policy.

39. Enter the pattern or regular expression you want IMC to search for in the **Match Patterns** field.

40. Click **Add** to the right of the **Match Patterns** field to add the match condition combination to the rule.

41. To add a new match condition, select the logical operator you want IMC to use to evaluate patterns and pattern matching from the **Rule Relation** list.

   Options include AND and OR.

   If you choose the logical operator **AND**, both patterns defined in the **Match Patterns** field on either side of the **AND** must be found in the configuration file for IMC to take the actions defined in the rule.

   If you choose the logical operator **OR**, only one of the patterns defined in the **Match Patterns** field on either side of the **OR** must be found in the configuration file for IMC to take the actions defined in the rule.

   You can have more than two **Match Pattern** regular expression values for one rule and therefore more than one logical operator in use in a given rule.

42. Select the pattern matching method you want to use from the **Match Mode** list as you did for the first match pattern in Step 39.

43. If the check type is **Link** or **Aggregate Link**, select the pattern matching method you want to use from the **Match Criteria** list as you did for the first match pattern in Step 40.

44. Enter the pattern or regular expression you want IMC to search for in the **Match Patterns** field.

45. Click **Add** to the right of the **Match Patterns** field to add the conditions to the rule.

46. Repeat Steps 39-47 for as many check type match patterns you want to add to the rule.
47. Enter the pattern or regular expression in the **Match Patterns** field. If what you selected in **Step 7** is not **Link** or **Aggregate Link**, go to **Step 40**.

48. Select the value comparison type from the **Comparison Type** list. Five options are provided:
   - **All equal to**: IMC retrieves values from the devices’ configuration files based on the rule content entered in **Step 49**, and compares them with the value you enter in **Step 51**. If the values match, the configuration files are compliant with the policy.
   - **All not equal to**: IMC retrieves values from the devices’ configuration files based on the rule content entered in **Step 49**, and compares them with the value you enter in **Step 51**. If none of the extracted values match the entered value, the configuration files are compliant with the policy.
   - **One of them equal to**: IMC retrieves values from the devices’ configuration files based on the match pattern entered in **Step 49**, and compares them with the value you enter in **Step 51**. If at least one of the extracted values matches the entered value, the configuration files are compliant with the policy.
   - **One of them not equal to**: IMC retrieves values from the devices’ configuration files based on the match pattern entered in **Step 49**, and compares them with the value you enter in **Step 51**. If at least one of the extracted values does not match the entered value, the configuration files are compliant with the policy.
   - **All Identical**: IMC retrieves values from the devices’ configuration files based on the match pattern entered in **Step 49**, and compares them. If the extracted values of the devices match, the configuration files are compliant with the policy.

49. If you selected is not **All Identical**, enter a value in the **Value for Comparison** field. IMC compares this value with the values retrieved from the devices.

50. Click **Add** to the right of the **Value for Comparison** field to add the match condition combination to the rule. If you selected the comparison type **All Identical** in **Step 50**, add the match pattern entered in **Step 49** to the rule.

51. To add a new **Value for Comparison**, select the logical operator you want IMC to use to evaluate patterns and pattern matching from the **Rule Relation** list. Options include **AND** and **OR**.
   - If you choose the logical operator **AND**, both patterns defined in the **Match Patterns** field on either side of the **AND** must be found in the configuration file for IMC to take the actions defined in the rule.
   - If you choose the logical operator **OR**, only one of the patterns defined in the **Match Patterns** field on either side of the **OR** must be found in the configuration file for IMC to take the actions defined in the rule.

52. Select a comparison type from the **Comparison Type** list.

53. If you selected is not **All Identical**, enter a value in the **Value for Comparison** field. IMC compares this value with the value retrieved from the device.

54. Click **Add** to the right of the **Value for Comparison** field to add the match condition combination to the rule.

55. Repeat the steps to add more **Check and Get type** match conditions to the rule.

56. If the check type is **Link** or **Aggregate Link**, repeat the necessary steps to add more match conditions to the rule and click **OK**.

57. Click the **link** of a rule to enter the rule test window.

58. Enter the test content in the text box under **Test Content**, or import a configuration file from the configuration template database, and click **Test**.
After the test is complete, the test results show whether the content or configuration file matches the rule. You can judge whether the rule achieves your purpose according to the test results. To clear the test content and result, click **Reset**.

59. To delete the rule, click the ✗ link of the rule and click **OK**.

**Deleting a compliance policy**

To delete a compliance policy:

1. Navigate to **Service**→**Compliance Policy**.
2. Click the **Service** tab from the tabular navigation system on the top.
3. Click the **Compliance Center** on the navigation tree on the left.
4. Click **Compliance Policy** under **Compliance Center** on the left navigation tree.
   The **Policy List** appears.
5. Click the ✗ link of the policy to be deleted. A dialog box appears.
6. Click **OK**.

*System Defined* compliance policy cannot be deleted. Only *User Defined* compliance policy can be deleted.

**Enabling a single compliance policy**

To enable a single compliance policy:

1. Navigate to **Service**→**Compliance Policy**.
2. Click the **Service** tab from the tabular navigation system on the top.
3. Click the **Compliance Center** on the navigation tree on the left.
4. Click **Compliance Policy** under **Compliance Center** on the left navigation tree.
   The **Policy List** appears.
5. Click the ✗Disabled link of the compliance policy to be enabled.

**Enabling all compliance policies**

To enable all compliance policies:

1. Navigate to **Service**→**Compliance Policy**.
2. Click the **Service** tab from the tabular navigation system on the top.
3. Click the **Compliance Center** on the navigation tree on the left.
4. Click **Compliance Policy** under **Compliance Center** on the left navigation tree.
   The **Policy List** appears.
5. Click the **Enable All** button.

**Disabling a single compliance policy**

To disable a single compliance policy:

1. Navigate **Service**→**Compliance Policy**.
2. Click the **Service** tab from the tabular navigation system on the top.
3. Click the **Compliance Center** on the navigation tree on the left.
4. Click **Compliance Policy** under **Compliance Center** on the left navigation tree.
The Policy List appears.

5. Click the Enabled link of the compliance policy to be disabled.

Disabling all compliance policies

To disable all compliance policies:

1. Navigate Service → Compliance Policy.
2. Click the Service tab from the tabular navigation system on the top.
3. Click the Compliance Center on the navigation tree on the left.
4. Click Compliance Policy under Compliance Center on the left navigation tree. The Policy List appears.
5. Click the Disable All button.

Rule examples

IMC predefines rules in a compliance policy. The following describes rules with the check type Device, Interface, Link, Aggregate Link, and Configuration Segment.

A Device rule checks the configuration file or display command outputs on the device. For example, if a rule checks the Latest backup running configuration file, it checks all the contents of the Latest backup running configuration file. (HPA)Syslog enabled is used as an example.

An Interface rule checks the configuration segments about interface in the configuration file or the configuration segments about interface in a display command output on the device. The start position and end position of the configuration segment are determined by Start Identifier and End Identifier in the rule. (Cisco) No delay an interface-CatOS is used as an example.

A Link rule checks the configuration segments about interface in the configuration file or the configuration segments about interface in a display command output on the devices on the two ends of a link. The start position and end position of the configuration segment are determined by Start Identifier and End Identifier in the rule. A Link rule checks devices by link rather than by device. (HPA) Duplex status is used as an example.

An Aggregate Link rule checks the configuration segments about interface in the configuration file or the configuration segments about interface in a display command output on the devices on the two ends of an Aggregate Link. The start position and end position of the configuration segment are determined by Start Identifier and End Identifier in the rule. An Aggregate Link rule checks devices by link rather than by device. (HPA) Speed status is used as an example.

A Configuration Segment rule checks any configuration segment in the configuration file on the device. The start position and end position of the configuration segment are determined by Start Identifier and End Identifier in the rule. (HPA) Remote login is used as an example.

Device

The (HPA)Syslog enabled rule belongs to the Syslog compliance policy. It checks whether the device is enabled with the Syslog function. If the device is not enabled with the Syslog function, a fixing command is executed to enable the function.

1. Navigate to Service → Compliance Policy.
2. Click the Service tab from the tabular navigation system on the top.
3. Click Compliance Center on the navigation tree on the left.
4. Click Compliance Policy under Compliance Center on the left navigation tree. The Policy List appears.

5. Input Syslog in the Name field, and click Query.

6. Click the name link of Syslog in the Policy List to enter the Compliance Policy Details page. For more information about the Compliance Policy Details page, see "Viewing detailed information about a compliance policy" (page 491).

7. Click the name link of (HPA)Syslog enabled in the Rule List to enter the Rule Details page. For more information about the Rule Details page, see "Error! Reference source not found." (page 492).

   a. Checks whether the device is a Hewlett Packard device. If not, the rule does not check the device. If yes, the rule goes to the next step.

   b. Checks whether the device series belongs to Device Series. If not, the rule does not check the device. If yes, the rule goes to the next step.

   c. Checks whether the Latest backup running configuration file contains the undo info-center enable string. If not, the device is enabled with the Syslog function and conforms to the Compliance Policy. If yes, the device violates the Compliance Policy, and the rule goes to the next step.

   d. Executes the info-center enable command to enable the Syslog function on the device and ends the check.

   e. Repeats the previous steps to check all the devices in the check task.

Interface

The (Cisco)No delay on interfaces-CatOS rule checks whether an interface delay is configured for an interface on the device. If yes, a fixing command is used to remove the interface delay configuration.


2. Click the Service tab from the tabular navigation system on the top.

3. Click Compliance Center on the navigation tree on the left.

4. Click Compliance Policy under Compliance Center on the left navigation tree. The Policy List appears.

5. Input Interface in the Name field, and click Query.

6. Click the name link of Interface delay in the Policy List to enter the Compliance Policy Details page. For more information about the Compliance Policy Details page, see "Viewing detailed information about a compliance policy" (page 491).

7. Click the name link of (Cisco)No delay on interfaces-CatOS in the Rule List to enter the Rule Details page. For more information about the Rule Details page, see "Error! Reference source not found." (page 492).

   a. Checks whether the device is a Cisco device. If not, the device is not checked. If yes, goes to the next step.

   b. Checks whether the device series belongs to Device Series. If not, the rule does not check the device. If yes, the rule goes to the next step.

   c. Reads the Latest backup running configuration file on the device to check the configuration segment starting with interface and ending with !. If the configuration segment does not contain
delay, the device conforms to the compliance policy. If the configuration segment contains delay, the rule goes to the next step.

d. Executes the no delay command to remove the interface delay configuration and ends the check.
e. Repeats the previous steps to check all the devices in the check task.

Links

The (HPA) Duplex status rule checks whether the duplex modes on the devices on the two ends of a link are the same. If not, the check result is displayed to notify the administrator.

2. Click the Service tab from the tabular navigation system on the top.
3. Click Compliance Center on the navigation tree on the left.
4. Click Compliance Policy under Compliance Center on the left navigation tree. The Policy List appears.
5. Input Link status in the Name field, and click Query.
6. Click the name link of Link status in the Policy List to enter the Compliance Policy Details page.
   For more information about the Compliance Policy Details page, see "Viewing detailed information about a compliance policy" (page 491).
7. Click the name link of (HPA)Duplex status in the Rule List to enter the Rule Details page.
   For more information about the Rule Details page, see "Error! Reference source not found." (page 492).
   a. Checks whether the device is a Hewlett Packard device. If not, the device is not checked. If yes, the rule goes to the next step.
   b. Checks whether the device series belongs to Device Series. If not, the rule does not check the device. If yes, the rule goes to the next step.
   c. Performs link calculation. If a device is not directly connected to any other device, the device is not checked. If only one device exists or no devices are directly connected, the rule ends the compliance check on all devices. Otherwise, the rule calculates links, reads description for interfaces connecting the two devices, and uses interface + interface description as a start identifier. Then the rule goes to the next step.
   d. Reads the Latest backup running configuration files on the devices on the two ends of a link, and checks whether the configuration segment starting with interface + interface description and ending with # contains duplex. If neither configuration segments contain duplex, the two devices use the auto negotiated duplex mode and conform to the compliance policy. Otherwise, the rule goes to the next step.
   e. Checks whether the configuration segments contain duplex auto. If at least one configuration segment contains duplex auto, at least one device adopts the auto negotiated duplex mode, and the two devices conform to the compliance policy. Otherwise, the rule goes to the next step.
   f. Reads the values of duplex according to the regular expression duplex <value> from the configuration segments on the two devices and compares the values. If the values are the same, the duplex modes for the two devices are the same, and the two devices conform to the compliance policy. Otherwise, the two devices violate the compliance policy. The check result is displayed to notify the administrator.
   g. Ends the check on the two devices and repeats the previous steps to check devices on other links.
Aggregate link

The **(HPA) Speed status** rule checks whether the flow control configurations on the devices on the two ends of a link are the same. If not, the check result is displayed to notify the administrator.

1. Navigation **Service→Compliance Policy**.
2. Click the **Service** tab from the tabular navigation system on the top.
3. Click **Compliance Center** on the navigation tree on the left.
4. Click **Compliance Policy** under **Compliance Center** on the left navigation tree. The **Policy List** appears.
5. Input **Aggregate Link status** in the **Name** field, and click **Query**.
6. Click the name link of **Aggregate Link status** in the **Policy List** to enter the **Compliance Policy Details** page.
   
   For more information about the **Compliance Policy Details** page, see “Viewing detailed information about a compliance policy” (page 491).
7. Click the name link of **(HPA) Speed status** in the **Rule List** to enter the **Rule Details** page.
   
   a. Checks whether the device is a Hewlett Packard device. If not, the device is not checked. If yes, the rule goes to the next step.
   
   b. Checks whether the device series belongs to **Device Series**. If not, the rule does not check the device. If yes, the rule goes to the next step.
   
   c. Performs link calculation. If a device is not directly connected to any other device, the device is not checked. If only one device exists or no devices are directly connected, the rule ends the compliance check on all devices. Otherwise, the rule calculates links, reads description for interfaces connecting the two devices, and uses **interface + interface description** as a start identifier. Then the rule goes to the next step.
   
   d. Reads the **Latest backup running configuration** files on the devices on the two ends of the link, and checks whether the configuration segment starting with **interface + interface description** and ending with # contains **speed**. If the configuration segments do not contain **speed**, the two devices do not restrict interface traffic and conform to the compliance policy. Otherwise, the rule goes to the next step.
   
   e. Reads the values of duplex according to the regular expression **speed ?<value>** from the configuration segments on the two devices and compares the values. If the values are the same, the two devices conform to the compliance policy. Otherwise, the rule goes to the next step.
   
   f. Checks whether the configuration segments contain **speed auto**. If at least one configuration segment contains **speed auto**, the two devices conform to the compliance policy. Otherwise, the two devices violate the compliance policy. The check result is displayed to notify the administrator.
   
   g. Ends the check on the two devices and repeats the previous steps to check devices on other links.

Configuration segment

The **(HPA)Remote login** rule checks whether the remote login mode is SSH.

1. Navigation **Service→Compliance Policy**.
2. Click the **Service** tab from the tabular navigation system on the top.
3. Click **Compliance Center** on the navigation tree on the left.
4. Click **Compliance Policy** under **Compliance Center** on the left navigation tree. The **Policy List** appears.
5. Input **Security** in the Name field, and click **Query**.

6. Click the name link of **Security** in the Policy List to enter the Compliance Policy Details page.

   For more information about the Compliance Policy Details page, see "Viewing detailed information about a compliance policy" (page 491).

7. Click the name link of **(HPA)Remote login** in the Rule List to enter the Rule Details page.
   a. Checks whether the device is a Hewlett Packard device. If not, the device is not checked. If yes, the rule goes to the next step.
   b. Checks whether the device series belongs to **Device Series**. If not, the rule does not check the device. If yes, the rule goes to the next step.
   c. Reads \(\text{(user-interface)[1]}\) \#1 in the latest backup running configuration file, and uses the read parameter as the end identifier. If no parameter is read, ends the check on the device. Otherwise, the rule goes to the next step.
   d. Checks the configuration segment starting with **user-interface vty** and ending with 1, 2, or 3, for example. If the configuration segment contains **protocol inbound ssh**, the device conforms to the compliance policy, and the rule ends the check on the device. If the configuration segment does not contain **protocol inbound ssh**, the device violates the compliance policy. The check result is displayed to notify the administrator that the device violates the compliance policy.
   e. Repeats the previous steps to check all the devices in the check task.

### Check tasks

A check task is used to check the policy compliance of a device based on the association between a compliance policy with the device and parameters such as the check severity level and execution period.

The following sections provide details about check tasks.

#### Viewing the check task list

To view the check task list:

1. Navigate to **Service**→**Check Task**.
2. Click the **Service** tab from the tabular navigation system on the top.
3. Click the **Compliance Center** on the navigation tree on the left.
4. Click **Check Task** under **Compliance Center** from the navigation system on the left.

The **Task List** appears.

**Task list**

- **Status**: Contains status of the check task, which can be **Finished**, **Enabled**, **Disabled**, or **Running**. If a task is finished, **Finished** appears. A task in **Enabled** state is executed automatically at an interval, and a task in **Disabled** state is not. Only periodic check tasks can be in **Enabled** or **Disabled** state. A task being executed is in **Running** state.
- **Task Name**: Contains name of the check task. Clicking on a check task name link, you enter the check task details page.
- **Execute Task**: Contains type of the check task, which can be **Periodically** or **Immediately**. A **Periodically** task is executed periodically as scheduled. An **Immediately** task is executed immediately, but only once.
- **Creation Time**: Contains time when the check task was created.
- **Operation**: Indicates whether the task is enabled (Disabled) or disabled (Enabled) when the task is periodic, and lets you disable or enable the task by clicking the status link. For a task in Running or Finished state, nothing is displayed in this field.

- **Check Results**: Highest violation level of the device. Violation levels are set when you create a rule. When you move the pointer over a violation level name, a popup window displays, showing the counts of each violation level. You can click the level name link to enter the Task Execution Results page.

- **Fix**: Click the link to enter the page for fixing violations. For more information about violation fixing, see Fixing violating devices.

- **Modify**: Contains a link for modifying the associated check task. This link is displayed when the value of the Execute Task field is Periodically.

- **History**: Contains a link for checking the execution results and history of the check task. When you click the link, a menu appears, providing three options: Task Check Results (Compliance Policy), Task Check Results (Device), and Task History. If the device is compliant with the policy, only the Task History option appears on the menu. The Task Check Results (Compliance Policy) option shows you the check results in policy view for analysis from the compliance policy’s perspective. The Task Check Results (Device) option shows you the check results in device view for analysis from the device’s perspective. For more information about the check result reports, see Task execution results, task execution report, and configuration retrieval report.

If the Task List contains enough entries, the following navigational aids appear.

- Click to page forward in the Task List.
- Click to page forward to the end of the Task List.
- Click to page backward in the Task List.
- Click to page backward to the front of the Task List.

5. Click 8, 15, 50, 100, or 200 from the right side of the main pane to configure how many items per page you want to view.

You can sort the Task List by the Status, Task Name, Execute Task, and Creation Time fields. Click the column label to sort the list by the selected field. The column label is a toggle switch that lets you toggle between the various sort options specific to each field.

### Viewing check task details

To view check task details:

1. Navigate to **Service**→**Check Task**.
2. Click the **Service** tab from the tabular navigation system on the top.
3. Click the **Compliance Center** on the navigation tree on the left.
4. Click **Check Task** under **Compliance Center** from the navigation system on the left. The Task List appears.
5. Click the **Task Name** link of the target check task to enter the Task Details page.

The Task Details page includes three parts: Task Attribute, Compliance Policy Information, and Device Information. The following describes these parts in detail.

### Task attribute

- **Task Name**: Contains the name of the check task.
- Severity: Controls which rules to execute. Only rules with a severity level equal to or higher than the value of this argument are executed.
- Execute Task: Contains the execution type of the check task, which can be Periodically or Immediately.
- Start Time: Start time of the check task. This argument is displayed only when the value of the Execute Task field is Periodically.
- Description: Contains a description of the check task.

Compliance policy information
- Name: Contains the name of the compliance policy added to the check task. Click on the compliance policy name link to enter the compliance policy details page. For more information about compliance policy details, see "Viewing detailed information about a compliance policy" (page 491).
- Description: Contains a description of the compliance policy.

Device information
- Status: Contains the alarm status of the device. If there are multiple alarms for the device, the status of the highest level appears.
- Device Name: Contains the name of the device. Click on the name link to enter the device details page. For more information about device details, see "Device details page" (page 212).
- IP Address: Contains the IP address of the device.
- Device Model: Contains the model of the device.

Adding a check task
To add a check task:
1. Navigate to Service→Check Task.
2. Click the Service tab from the tabular navigation system on the top.
3. Click the Compliance Center on the navigation tree on the left.
4. Click Check Task under Compliance Center from the navigation system on the left. The Task List appears.
5. Click the Add button to enter the Add Check Task page.
6. Enter a name in the Task Name field. The name can be a string of 1 to 32 characters.
7. Select a level from the Severity list. Options include All, Above Informational, Above Warning, Above Minor, and Above Major. This argument controls which rules to execute. Only rules with a severity level equal to or higher than the value of this argument are executed.
   - Configuration check tasks can be run immediately or they can be scheduled to run on a periodic basis: To run the task immediately, select Immediately from the Execute Task list, or To create a task that runs periodically, select Periodically from the Execute Task list.
   If you selected Periodically, the Task Attribute page of the Add Check Task wizard updates with fields to schedule the task.
8. Select the frequency with which you want to run this check task by selecting it from the Start Time list:
If you select **Every Week**, select the day of the week from the list to the right of the **Start Time** list, or

- If you select **Every Month**, select the day of the month from the list to the right of the **Start Time** list.

9. Enter the time of day that you want the check task to begin by entering it in the field to the right of the **Start Time** list.

   The valid format for time entry is HH:MM:SS where HH denotes the two digit hour, MM denotes the two digit minute, and SS denotes the two digit second.

10. Enter a brief description for this task in the **Description** field.

    A valid length for the description is 0-128 characters.

11. Click the link for a compliance policy to enter the policy’s details page.

12. To cancel the association of a compliance policy with the task, click the ✗ icon in the **Delete** column and click OK in the confirmation dialog box.

13. To select devices, you can do so from all devices, or select device models and then exclude the devices that you do not want to check:
   
   a. Select **Select Device** under **Select Device or Device Models** and then click **Select Device**. The **Select Devices** dialog box appears.
   
   b. Add devices by **View** or by the **Advanced** query method. See "Adding devices by View" (page 85) and "Adding devices by Advanced query" (page 85).

### Deleting a check task

To delete a check task:

1. Navigate to **Service→Check Task**.
2. Click the **Service** tab from the tabular navigation system on the top.
3. Click the **Compliance Center** on the navigation tree on the left.
4. Click **Check Task** under **Compliance Center** from the navigation system on the left. The **Task List** appears.
5. Select the check box ☑️ to the left of the target check task, or select the check box to the left of **Status** to select all check tasks.
6. Click the **Delete** button to delete the selected check tasks.

### Fixing violating devices

IMC provides the function of fixing the violating devices. The operator can enter a fix command, and set the execution time of the fix task. When the time is reached, IMC deploys the fix task to the device and executes the fix command on the device. This increases the fix task efficiency and reduces the operator workload.

1. Navigate to **Service→Check Task**.
2. Click the **Service** tab from the tabular navigation system on the top.
3. Click the **Compliance Center** on the navigation tree on the left.
4. Click **Check Task** under **Compliance Center** from the navigation system on the left. The **Task List** appears.
5. Click the corresponding ♻️ link of the target check task to enter the rule violation preview page.
The link is displayed only when the check task is completed and violating devices are detected. Stack devices do not support the fix task.

The rule violation preview is displayed in a tree structure of Device–Compliance Policy–Rule.

6. Do one of the following:
   - To clasped a compliance policy, click the link to the left of the device name, or
   - To expand a compliance policy, click the link to the left the compliance policy, or
   - To claspe rules, click the link to the left of the compliance policy, or
   - To expand rules, click on the link.
   - **Name**: Contains names of devices, compliance policies, and rules.
   - **Description**: Contains detailed information about the violations of the device and number of violations for each violation severity level for a device or compliance policy. You can know which check contents are not compliant with the rules and the match criteria for the rules.

7. Do one of the following:
   - To enter the rule information page, click a rule name link, or
   - To enter the check task detailed information page, click on the **Check Content** link.

8. Do one of the following:
   - To select the violation contents of a rule, select the checkbox to the left of the rule name, or
   - To select the violation contents of a compliance policy, select the checkbox to the left of the compliance policy, or
   - To select all the violation contents of a device, select the checkbox to the left of the device name, or
   - To select the violation contents of all devices on the current page, select the checkbox to the left of the **Name** field.

9. To select the violation contents for all devices, select the checkbox to the right of **Fix All Devices** on the upper right of the page.

10. Select 8, 15, or 50 from the right side of the main pane to configure how many items per page you want to view.

11. Click **Fix** to enter the **Fixing Commands** page.

12. Enter the command for fixing the device in the text box under the device name. The variables such as $ are not supported. For example, a fixing command cannot contain ${ip address}.

13. Select the checkbox to the right of the target device to cancel fixing the device.

14. Click **Next** to enter the **Set Task Attributes** page.

15. Enter a name for this task in the **Task Name** field.

16. Select the time you want IMC to execute this task from the **Schedule Time** list.
   Options include **Immediately** and **Scheduled**. If you selected **Immediately**, go to Step 27.

17. If you selected **Scheduled**, click the calendar icon to populate the date and time for the execution of this task. A popup calendar appears. Select the date from the calendar. Enter the start time in the box to the right of the **Time** field on the lower part of the calendar window, in the format of HH:MM.
Valid date and time format for this field is YYYY-MM-DD HH:MM:SS where YYYY denotes the four digit year, MM denotes the two digit month, DD denotes the two digit day and HH denotes the two digit hour, MM denotes the two digit minute and SS denotes the two digit second value.

18. Select the sequence to execute the fixing task from the Schedule Sequence list.
   Two options are available: Concurrent and Sequential. If you select Concurrent, IMC can fix multiple devices simultaneously. If you select Sequential, IMC can only fix one device at a time.
   If you select Sequential from the Schedule Sequence list, you need to set the sequence to fix the devices, and IMC fixes the devices based on the sequence you set.

19. Click Sort located to the right of the Schedule Sequence list. The Sort dialog box appears.

20. Click the checkbox ☐ to the left of the devices you want to move.

21. Do one of the following:
   o Click Up to move the devices up in the list, or
   o Click Down to move the devices down in the list.

22. Do one of the following:
   o Click Top to move the devices to the top of the list, or
   o Click Bottom to move the devices to the bottom of the list.

23. Click OK when you have finished sorting the devices in the list.

24. If you select Sequential from the Schedule Sequence list, you can define how you want IMC to handle errors that arise in the deployment process.

25. If errors occur in the fixing process and you want to stop the fixing task on all devices, select Stop Deployments on All Devices from the Error Handling list.

26. If errors occur in the fixing process and you want to skip the fixing task on the current device and continue with other devices, select Stop Deployment on the Current Device from the Error Handling list.

27. Enter the task description in the box to the right of Task Description.

28. Click Finish.

29. Go to the Service→Deployment Task page. The new fixing tasks are displayed in the deployment task list. For more information about task deployment, see “Accessing the deployment task list” (page XX)

Check task history

The check task execution results and violations are displayed in a report. Task check results (compliance policy), task check results (device), task execution report, and rule extract report are available. At the same time, the device violating results are sent to the network administrator in the form of alarms.

View check task history

To view check task history:
1. Navigate to Service→Task History.
2. Click the Service tab from the tabular navigation system on the top.
3. Click the Compliance Center on the navigation tree on the left.
4. Click ✅ Task History under Compliance Center from the navigation system on the left.
   The Task History List appears.

Task history list
Task Name: Contains name of the check task. You can enter the check task details page by clicking the task name link.

Description: Contains description for the check task.

Start Time: Contains the time when the check task starts to run.

End Time: Contains the time when the check task stops running.

Execution Result: Contains execution result of the check task. You can click on an execution result link to enter the View Execution Result page. The page displays all the devices concerned, start and end time, and execution result of the check task.

Operation: Contains Compliance Policy Check Results, Device Violating Results, Configuration Check Report, and Configuration Retrieval Report links. To enter the Compliance Policy Check Results page, click  . To enter the Device Violating Results page, click  . To enter the Configuration Check Report page, click  . To enter the Configuration Retrieval Report page, click  .

If the Task History List contains enough entries, the following navigational aids appear.

- Click  to page forward in the Task History List.
- Click  to page forward to the end of the Task History List.
- Click  to page backward in the Task History List.
- Click  to page backward to the front of the Task History List.

5. Click 8, 15, 50, 100, or 200 from the right side of the main pane to configure how many items per page you want to view.

You can sort the Policy List by the Task Name, Description, Start Time, End Time, and Execution Result fields. Click the column label to sort the list by the selected field. The column label is a toggle switch that lets you toggle between the various sort options specific to each field.

Query check task history

To query check task history:

1. Navigate to Service—Task History.
2. Click the Service tab from the tabular navigation system on the top.
3. Click the Compliance Center on the navigation tree on the left.
4. Click Task History under Compliance Center from the navigation system on the left. The Task History List appears.
5. Enter one or more of the following search criteria in the Query section of the page:
   - Task Name: To locate a check task name, enter a partial or complete name for the task in the Check Task Name field.
   - Time Range: To view tasks for a specific time range, enter the start of your time range in the From field. Valid date and time format for this field is YYYY-MM-DD HH:MM:SS where YYYY denotes the four digit year, MM denotes the two digit month, DD denotes the two digit day and HH denotes the two digit hour, MM denotes the two digit minute and SS denotes the two digit second value.
6. To auto populate the from field, click the calendar icon  located to the right of the from field. A popup calendar appears. Select the start date from the calendar. Enter the start time in the box to the right of the Time field on the lower part of the calendar window, in the format of HH:MM.
7. Enter the end time for the range in the to field. To auto populate the to field, click on the calendar icon located to the right of the to field. A popup calendar appears. Select the end date from the calendar. Enter the start time in the box to the right of the Time field on the lower part of the calendar window, in the format of HH:MM.

8. Valid date and time format for this field is YYYY-MM-DD HH:MM:SS where YYYY denotes the four digit year, MM denotes the two digit month, DD denotes the two digit day and HH denotes the two digit hour, MM denotes the two digit minute and SS denotes the two digit second value.

9. Click Query to submit your filter criteria. The results of your filter or search query display in the Task History List.

10. Click Reset when you want to restore the full Task History.

Delete check task history

To delete Check Task History:
1. Navigate to Service→Check History.
2. Click the Service tab from the tabular navigation system on the top.
3. Click the Compliance Center on the navigation tree on the left.
4. Click Task History under Compliance Center from the navigation system on the left. The Task History List appears.
5. Click the checkbox to the left of the target check task, or click the checkbox to the left of Task Name to select the history for all check tasks.
6. Click Delete. A confirmation dialog box appears. Click OK.

Task execution results, task execution report, and configuration retrieval report

The Task Execution Results are displayed in a report. The report shows the check task execution results and the device violating results. At the same time, the device violating results are sent to the network administrator in the form of alarms.

Compliance Policy Check Results lets you view the execution result of a check task in a policy compliance report, which shows the check result of the rules in each policy contained in the check task.

Device Violating Results lets you view the execution result of a check task in a device violation report, which shows the check result of the task on each device and information about the unchecked devices.

Configuration Check Report lets you view the execution report of a check task. The report shows the policy compliance and the check result of each rule.

Configuration Retrieval Report lets you view the get report after execution of a check task. The report shows the result of each rule on all devices associated with the check policy.

The following reports are described in detail:
- Task Execution Results
- Compliance Policy Check Results
- Device Violating Results
- Configuration Check Report
- Configuration Retrieval Report
View task execution results

To view task execution results:

1. Navigate to Service→Check Task.
2. Click the Service tab from the tabular navigation system on the top.
3. Click the Compliance Center on the navigation tree on the left.
4. Click Check Task under Compliance Center from the navigation system on the left.
   The Task List appears.
5. Click the violation level link in the Check Results column to enter the Task Execution Results page.
   The check task information is displayed on the upper left part of the report.
   - Task Name: Contains the name of the check task.
   - Creator: Contains the operator that created the check task.
   - Violating Devices: Contains the number of violating devices.
   - Vulnerability Sum: Contains the number of violations.
   - Task Description: Contains a description for the check task.

   The information is displayed on the upper right part of the report.

   The lower part of the report contains four areas: Device Check Information, Compliance Policy Check Information, Severity Level, and Level Description.

Device Check Information

Number of violations for each device and for each violation severity level is displayed in a form.

6. Click the device name link to enter the Device Violating Results page.
   - Task Name: Contains the name of the check task.
   - Check Time: Contains the time when the device violated the compliance policy.
   - Task Description: Contains a description for the check task.

   The Device Check Information area displays the detailed information about compliance policy violation by device:
   - Device Name: Contains the name of the device.
   - Description: Contains the detailed information about the violations of the device and number of violations for each violation severity level. You can click a rule name link to enter the Rule Content window and click the checked content link to enter the Check Content window.

7. Do one of the following:
   - To clasp the compliance policy, click to the left of the device name, or
   - To expand the compliance policy, click .

   If the Device Check Information List contains enough entries, the following navigational aids are displayed.
   - Click to page forward in the Device Check Information List.
   - Click to page forward to the end of the Device Check Information List.
   - Click to page backward in the Device Check Information List.
   - Click to page backward to the front of the Device Check Information List.
8. Select 8, 15, or 50 from the right side of the main pane to configure how many items per page you want to view.

9. Click the upper left corner to return to the Task Execution Results page.

Compliance policy check information

- **Policy Name**: Contains the name of the compliance policy. To enter the compliance policy check result page, click the target compliance policy.
- **Total Devices**: Contains the number of devices that violate the compliance policy.
- **Violating Devices**: Contains the name of each device that violates the compliance policy. To enter the Device Violating Results page, click the target device.

10. Click the target compliance policy to enter the Compliance Policy Check Results page.

   The check task information is displayed on the upper left part of the report.
   - **Task Name**: Contains the name of the check task.
   - **Check Name**: Contains the time when the device violated the compliance policy.
   - **Task Description**: Contains the description on the check task.

The Device Check Information area displays the detailed information about compliance policy violation by compliance policy:

- **Compliance Policy Name**: Contains the name of the compliance policy.
- **Rules**: Contains the number of rules contained in the compliance policy.
- **Check Result**: Contains the violation status of the device associated with the compliance policy.
  - ✅ means the device does not violate the compliance policy.
  - ❌ means the device violated the compliance policy.
- **Violations**: Contains the total number of violations for all devices.
- **Violating Devices**: Contains the number of violating devices.
- **Severity level**: For a compliance policy, this field displays the highest violation severity level among the rules. For a rule, this field displays the violation severity level for the rule.

11. Do one of the following:
   - To clasp the rules, click 🔗 to the left of the compliance policy, or
   - To expand the rules, click 🔍.

12. Do one of the following:
   - To clasp the devices, click 🔗 to the left of the rule name, or
   - To expand the devices, click 🔍.

If the Compliance Policy Check Information List contains enough entries, the following navigational aids are displayed.

- Click ⏯️ to page forward in the Compliance Policy Check Information List.
- Click ⏯️ to page forward to the end of the Compliance Policy Check Information List.
- Click ⏯️ to page backward in the Compliance Policy Check Information List.
- Click ⏯️ to page backward to the front of the Compliance Policy Check Information List.

13. Select 8, 15, or 50 from the right side of the main pane to configure how many items per page you want to view.
14. Click the upper left corner to return to the Task Execution Results page. The Severity level area displays the number of violating devices for each severity level and the names of the violating devices. The Level description area describes the impact of violations for each severity level to the network.

View compliance policy check results

To view compliance policy check results:

1. Navigate to Service→Task History.  
2. Click the Service tab from the tabular navigation system on the top.  
3. Click the Compliance Center on the navigation tree on the left.  
4. Click Task History under Compliance Center from the navigation system on the left. The Task History List appears.  
5. Click in the Operation column of the target check task to enter the Compliance Policy Check Results page.  

The check task information is displayed on the upper left part of the report.  

- **Task Name**: Contains the name of the check task.  
- **Creator**: Contains the username of the operator that created the check task.  
- **Violating Devices**: Contains the number of violating devices.  
- **Vulnerability Sum**: Contains the number of violations.  
- **Task Description**: Contains a description for the check task.  

The number of violations for each severity level is displayed in a form on the upper right part of the report.  

The Compliance Policy Check Information area displays the violation information by compliance policy:  

- **Compliance Policy Name**: Contains the name of the compliance policy.  
- **Rules**: Contains the number of rules contained in the compliance policy.  
- **Check Result**: Contains the violation status of the device associated with the compliance policy.  
  - ✓ means the device does not violate the compliance policy. ❌ means the device violated the compliance policy.  
- **Violations**: Contains the total number of violations for all devices.  
- **Violating Devices**: Contains the number of violating devices.  
- **Severity Level**: For a compliance policy, this field displays the highest violation severity level among the rules. For a rule, this field displays the violation severity level for the rule.  

6. Do one of the following:  
   - To clasp the rules, click to the left of the compliance policy name, or  
   - To expand the rules, click .  

7. Do one of the following:  
   - To clasp the devices, click to the left of the rule name, or  
   - To expand the devices, click .
If the **Compliance Policy Check Information List** contains enough entries, the following navigational aids are displayed:

- Click to page forward in the **Compliance Policy Check Information List**.
- Click to page forward to the end of the **Compliance Policy Check Information List**.
- Click to page backward in the **Compliance Policy Check Information List**.
- Click to page backward to the front of the **Compliance Policy Check Information List**.

8. Click 8, 15, or 50 from the right side of the main pane to configure how many items per page you want to view.

**View device violating results**

To view Device Violating Results:

1. Navigate to **Service→Task History**.
2. Click the **Service** tab from the tabular navigation system on the top.
3. Click the **Compliance Center** on the navigation tree on the left.
4. Click **Task History** under **Compliance Center** from the navigation system on the left. The **Task History List** appears.
5. Click in the **Operation** column of the target check task to enter the **Device Violating Results** page.

The check task information is displayed on the upper left part of the report, including:

- **Task Name**: Name of the check task.
- **Creator**: Username of the operator that created the check task.
- **Violating Devices**: Number of violating devices.
- **Vulnerability Sum**: Number of the violations for all devices associated with the compliance policy.
- **Task Description**: Description for the check task.
- **Number of violations for each severity level is displayed in a form on the upper right part of the report.**

The **Device Check Information** area displays the detailed violation information by device:

- **Device Name**: Name of the device.
- **Description**: For a device, this field displays the number of violations for each violation severity level. For a compliance policy, this field displays the name of the rule that the device violates and the violation content. To view the detailed rule information, click the rule name link. To view the configuration file on the device, click the **Checked Content** link.

6. Do one of the following:
   - To clasp the compliance policies, click to the left of the device name
   - To expand the compliance policies, click .

The **Check Failure Devices** area displays the check failure devices and check task execution results.

The **Skipped Devices** area displays information about the skipped devices and the reasons.

If the **Device Check Information List** contains enough entries, the following navigational aids appear:

- Click to page forward in the **Device Check Information List**.
- Click to page forward to the end of the **Device Check Information List**.
7. Click 8, 15, or 50 from the right side of the main pane to configure how many items per page you want to view.

**View configuration check report**

To view configuration check report:

1. Navigate to Service→Task History.
2. Click the Service tab from the tabular navigation system on the top.
3. Click the Compliance Center on the navigation tree on the left.
4. Click Task History under Compliance Center from the navigation system on the left. The Task History List appears.
5. Click in the Operation column of the target check task to enter the Configuration Check Report page.
   - Device Name: Contains the name of the device.
   - Match State: Whether the device matches the rules. If not, Breach appears. If yes, Match appears.
   - Breach Count: Contains the number of the violations for each violation level.
   - Match Count: Contains the number of rules that the device matches.
   - Check Time: Time when IMC applied the check task to the device.
   - Details: Contains the link for displaying detailed violation information for the device. You can click the Details link to enter the detailed information page. The Details link is displayed only when the device violates a compliance policy.
6. Click the Details link of the target device to enter the details page of the device.
   - Number of violations and number of matches for each violation severity level, and total number of violations and matches are displayed in a form on the upper part of the page.
   - The rule information and violation status of the device are displayed on the lower part of the page.
   - Rule Name: Contains the name of the rule.
   - Description: Contains a description on the rule.
   - Match State: Whether the device matches the rules. If not, Breach appears. If yes, Match appears.
   - Violation Level: Contains the violation severity level of the rule.
7. Export the execution result report.

**Exporting a report**

To export the report:

1. Click the export icon located on the toolbar on the top of the report.
2. Select the desired export file format from the File Format list.
   - Options include Crystal Reports (RPT), Adobe Acrobat (PDF), Microsoft Excel (97-2003), Microsoft Excel (97-2003) Data - Only, Microsoft Word (97-2003) – Editable, Rich Text Format (RTF), and Separated Values (CSV).
3. Select the desired page range from Page Range.
4. Click Export.
5. Print the execution result report to PDF.

**Printing a report**

To print the report to PDF:

1. Click the print icon located on the toolbar on the top of the report.
2. Select the desired page range from Page Range.
3. Click Export.
4. Input a text in the text box to the left of the icon located on the toolbar on the top of the report and click on the icon.

The page that contains the text pops up.

**View configuration retrieval report**

To view configuration retrieval report:

1. Navigate to Service → Task History.
2. Click the Service tab from the tabular navigation system on the top.
3. Click the Compliance Center on the navigation tree on the left.
4. Click Task History under Compliance Center from the navigation system on the left.

The Task History List appears.

5. Click in the Operation column of the target check task to enter the Rule Extract Report page.
   - **Rule Name**: Contains the name of the rule.
   - **Rule Description**: Contains a description for the rule.
   - **Extract Device Count**: Contains the number of devices from which values are extracted.
6. Export the execution result report.

**Exporting a report**

To export the report:

1. Click the export icon located on the toolbar on the top of the report.
2. Select the desired export file format from the File Format list.
   - Options include Crystal Reports (RPT), Adobe Acrobat (PDF), Microsoft Excel (97-2003), Microsoft Excel (97-2003) Data - Only, Microsoft Word (97-2003) – Editable, Rich Text Format (RTF), and Separated Values (CSV).
3. Select the desired page range from Page Range.
4. Click Export.
5. Print the execution result report to PDF.

**Printing a report**

To print the report to PDF:

1. Click the print icon located on the toolbar on the top of the report.
2. Select the desired page range from Page Range.
3. Click Export.
4. Input a text in the text box to the left of the icon located on the toolbar on the top of the report and click on the icon. The page that contains the text pops up.

Configuration check by using the display command

IMC provides a feature that lets you check the results of a device’s display command results against defined rules or groups of rules. You can create a display command configuration that contains the specific display command they want to test for. You then create a rule or group of rules to compare against the output of the display command. By using the Check Task feature, you create a configuration check task that tests the output of the display command against the rule or set of rules to identify any violations in the display commands output.

Accessing the configuration check display command list

To access the configuration check display command list:
1. Navigate to Service→Display Command.
2. Click the Service tab from the tabular navigation system on the top.
3. Click the Compliance Center on the navigation tree on the left.
4. Click Display Command under Compliance Center on the left navigation tree.
   The Display Command List appears.

Display command list

- **Name**: Contains the name of the display command. The contents of this field serve as a link for navigating to the Detail page for the associated display command.

  The Detail page provides you with basic display command information including name, description, and display command content.

- **Description**: Contains a description for the display command.

- **Creation Time**: Contains a date and time stamp for the creation of the associated display command.

- **Modify**: Contains an icon for modifying the associated configuration check rule.

- **Copy**: Contains an icon for copying the associated configuration check rule.

- **Delete**: Contains an icon for deleting the associated configuration check rule.

You can sort the Display Command List by the Name, Description, and Creation Time fields. Click the column label to sort the list by the selected field. The column label is a toggle switch that lets you toggle between the various sort options specific to each field.

If the Display Command List contains enough entries, the following navigational aids appear:

- **Click**: to page forward in the Display Command List.
- **Click**: to page forward to the end of the Display Command List.
- **Click**: to page backward in the Display Command List.
- **Click**: to page backward to the front of the Display Command List.

5. Click 8, 15, 50, 100, or 200 from the right side of the main pane to configure how many items per page you want to view.
Adding a configuration check display command

To add a configuration check display command:

1. Navigate to Service → Display Command.
2. Click the Service tab from the tabular navigation system on the top.
3. Click the Compliance Center on the navigation tree on the left.
4. Click Display Command under Compliance Center on the left navigation tree.
   The Display Command List appears.
5. Click Add.
6. Enter a name for the display command in the Name field.
   Display Command names cannot begin or end with a period (.). Spaces in the configuration template name are also not permitted. In addition, the characters in Table 28 are not permitted in a display command file name.

<table>
<thead>
<tr>
<th>Character</th>
<th>Name</th>
<th>Character</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>Asterisk</td>
<td>'</td>
<td>Apostrophe or single quotation</td>
</tr>
<tr>
<td></td>
<td>Vertical bars</td>
<td>:</td>
<td>Colon</td>
</tr>
</tbody>
</table>
| \
| Backslash   | "            | Double quotation         |
| /          | Forward slash    | < >       | Angle brackets            |
| ?          | Question mark    |            |                           |

7. Enter a description for the display command in the Description field.
8. Enter the display command in the Content field.
   For example, the following command displays the SNMP read community string on a 3Com switch.
   display snmp-agent community read
9. Click OK to create the display command.
   After you create a display command list, you can select a display command from the created display command list when you select Display command output from the Check Target list.

Modifying configuration display commands

To modify a configuration check display command:

1. Navigate to Service → Display Command.
2. Click the Service tab from the tabular navigation system on the top.
3. Click the Compliance Center on the navigation tree on the left.
4. Click Display Command under Compliance Center on the left navigation tree.
   The Display Command List appears.
5. Click the icon in the Modify field of the display command you want to modify.
   You cannot modify the name of a display command once you have created it.
   To rename it, you must delete the existing display command and re-create it.
6. Modify the description for the display command in the Description field.
7. Modify the display command in the Content field as needed.
8. Click **OK** to accept your modifications to the display command.

**Deleting configuration display commands**

To delete a configuration check display command:

1. Navigate to **Service→Display Command**.
2. Click the **Service** tab from the tabular navigation system on the top.
3. Click the **Compliance Center** on the navigation tree on the left.
4. Click **Display Command** under **Compliance Center** on the left navigation tree. The **Display Command List** appears.
5. Click the icon ≠ in the **Delete** field of the display command you want to delete.
6. Click **OK** to confirm the deletion of the display command.
8 Event and alarm management

IMC includes in its feature set the ability to manage events or faults and their resolutions in real time. This chapter explains traps and Syslog entries as sources of events in IMC that become alarms. It also covers browsing and filtering traps and Syslog events and the processes for defining which traps IMC processes.

This chapter also explains views that IMC offers for browsing the alarms generated by IMC. This includes how to query for alarms, and the processes for sending alarms into email and SMS text notifications and alarm forwarding to help desk and other management systems.

Event and alarm overview

In IMC, an event is an incident of interest in the network infrastructure. An event could indicate a failure or fault on a network device. An event could also indicate a resolution of fault in the network. Or an event can be informational. An alarm is an event that has been escalated in IMC for viewing by an IMC operator, network administrator or support team using one of the IMC alarm browser views.

IMC can receive SNMP traps and Syslog entries as real time alarm sources. You can configure all devices in the network infrastructure to send traps to IMC when issues arise and when issues are resolved. In addition, you can configure all devices to forward specified Syslog messages to IMC for notification of faults or their resolutions.

IMC can be a source of traps for events. IMC generates traps that are displayed in IMC when events arise for managed devices such as when performance thresholds are exceeded, when IP address conflicts arise, or when configuration management tasks do not complete. In addition, the IMC system is also a managed device and traps can also be generated by IMC when a condition arises within IMC such as high CPU utilization, disk space issues, or IMC process issues on the IMC server.

In addition, IMC has a built in engine for polling configured devices for performance metrics. System and user defined thresholds translate a polling result into an event, whether the event is a fault or its resolution.

IMC itself is a source of events. IMC generates events for IMC.

Each of these three sources of events (traps, Syslog events, performance polling) in the network infrastructure serves as inputs for alarms in IMC. System and user defined rules determine which of the events generated by these three sources become an alarm.

Alarms take the form of entries into alarm browser views in IMC. They also can be escalated into alarm notifications via email, SMS text messaging, or alarm forwarding to help desk and other management systems.

Once an event becomes an alarm, it is written to the alarm database. There are two ways to remove an alarm from IMC’s views and further notifications.

The first and preferred option for removing an alarm from the view and further notifications is to clear or recover the event. Clearing an event or removes the event from Real-Time Alarms and Root Alarms views though recovered alarms can still be viewed in the All Alarms view. Alarms that have been recovered are removed from the database according to the Data Export configuration. When an event is recovered, IMC includes the date and timestamp so that the duration of the event is recorded. This information can be valuable for measuring the duration of a fault or event. Therefore, clearing or recovering an event is the preferred method for removing an alarm from alarm views. However, clearing or recovering an alarm does not mean that the actual fault or error condition has been resolved.
When an alarm is cleared or recovered, IMC removes the alarm instance from the Real-Time Alarms and Root Alarms views. The alarm is visible in the All Alarms view until it is removed from the alarm database during the next Data Export, which is 2:00am daily by default.

The clearing or recovering of an event can occur manually as when an operator chooses the Recover action for an alarm. In addition, an alarm can be cleared automatically. Automatic clearing is done when an event is received by IMC and there is a rule, either system or user defined that distinguishes this event as the resolution for a specified alarm. In fact, many MIBs include resolution traps along with traps that indicate failures.

The second option is to delete it. HP does not recommend this option because deleting an alarm removes it from the alarm database and along with it the ability to report on it. Alarms are a valuable data source for performance management of the network infrastructure. You can schedule regular exports of the alarm database to retain alarm histories. Operators should consider carefully policies for retaining and for deleting alarms. For more information on the data export capabilities, see "Data export" (page 147).

Clearing or recovering alarms is an important function of IMC and incident management in IT organizations. Alarms can be cleared from the alarm Actions navigation tree located on the right of the Alarm Details page. This can be accessed from all of the alarm browse views that IMC offers. For more information on clearing alarms, "Alarm actions in the alarm details page" (page 569).

**Trap management**

An SNMP trap is a message that is generated by an SNMP network device and sent to a management system for processing. A trap can indicate an error condition and its resolution. Additionally, a trap can also be informational. Traps are a proactive source of real time information on the health and status of the network infrastructure. Traps are effective for monitoring failures in real time because SNMP traps are messages sent by managed devices to management systems such as IMC.

IMC lets you receive traps from all SNMP managed devices and to review, filter, and generate alarms and notifications based on the traps received.

Trap management is most effective when all devices in the network infrastructure are configured to forward traps to IMC and IMC is configured to manage all of the devices that are configured to forward traps to it. Traps that IMC receives from unmanaged devices are (by default) filtered out.

Therefore, to effectively use IMC as a trap destination and a source for managing and displaying trap information, you must first configure all devices to forward traps to IMC. Refer to each vendor’s support documentation for information on how to configure their devices to forward traps to a management system. You must also add all devices (trap sources) to IMC and configure IMC to receive traps from them using the IMC auto discovery feature.

For more information on adding and managing devices in IMC and specifically auto discovery, see "5 Resource management" (page 153). For information on the filtering out traps from unmanaged devices, see "Modifying the unmanaged devices trap filter rule" (page 534).

IMC simplifies the process of configuring SNMP settings in IMC when adding devices to IMC through the use of SNMP templates. SNMP templates lets you save one or more SNMP configurations, which can then be applied to devices during discovery or when adding devices manually. For more information on using SNMP templates, see "SNMP templates" (page 74).

**Browsing traps**

You can view traps. IMC trap views include the trap source, a description of the trap and the date and time the trap was received.
**Browsing traps**

To browse traps:

1. Navigate to **Browse Trap**.
2. Click the **Alarm** tab from the tabular navigation system on the top.
3. Click **Trap Management** on the navigation tree on the left.
4. Click **Browse Trap** under **Trap Management** from the navigation system on the left.

IMC displays all trap entries in the **Trap List** displayed in the main pane of the **Browse Trap** window.

**Trap list fields**

- **Device Name**: Contains the name of the device from which the trap was sent.
- **Device IP**: Contains the IP address of the device from which the trap was sent.

5. Click an individual entry in the **Device Name** or **Device IP** column to navigate to the **Device Details** page for the device that generated the trap.

For more information on the **Device Details** page, see "Managing one device via device details" (page 212).

- **Description**: provides the description that is contained within the trap itself.

6. Click an individual entry in the **Description** column to navigate to the **Trap Details** page that provides a view of all known trap details.

For more information on the **Trap Details** page, see "Trap details page" (page 527).

- **Trap at**: Contains the date and time stamp that the trap was either sent or received.

You can sort the **Trap List** by the **Device Name**, **Device IP**, **Description** or the **Trap at** fields. Click the column label to sort the list by the selected field. The column label is a toggle switch that lets you toggle between the various sort options specific to each field.

7. Click **8, 15, 50, 100, or 200** from the right side of the main pane to configure how many items per page you want to view.

   - Click **to page forward in the **Trap List**.
   - Click **to page forward to the end of the **Trap List**.
   - Click **to page backward in the **Trap List**.
   - Click **to page backward to the front of the **Trap List**.

8. For trap lists that have more than one page, click **1, 2, 3, 4, 5, 6, 7, 8, 9, 10 ...** from the bottom right side or on the top center of the main pane to jump to a particular page of the trap list.

You can configure devices to forward traps to IMC. IMC then receives and display all traps forwarded to it. However, IMC recognizes them and displays related information on the traps and the trap source only if the source of the trap is known and managed by IMC.

For unknown traps, the trap object identifier (OID) displays in the **Description** column to help locate the source of the trap.

Only the OID and the parameter value are displayed for unknown traps.

**Trap details page**

The **Trap Details** page lets you view into the details contained within individual traps. In addition, all traps for a particular device can be viewed from the **Trap Details** page.
To view trap details

To view the Trap Details page:
1. Navigate to Trap Details.
2. Click the Alarm tab from the tabular navigation system on the top.
3. Click Trap Management from the navigation tree on the left.
4. Click Browse Trap from the navigation tree on the left.
5. Click the Description under Trap List for the specific trap in which you want to view details.

Trap details fields

- **Name**: Contains the event name as defined in the source MIB.
- **OID**: Contains the object ID for the trap.
- **Trap At**: Contains the date and time stamp.
- **Trap Source**: Contains the name or IP address of the device that sent the trap. Clicking on Trap Source in this column navigates you to the Device Details page for the device that generated the trap. For more information on the Device Details page, see "Device details page" (page 212).
- **Description**: Contains the description for this event as defined in the source MIB.
- **Trap Cause**: Contains the cause for this event as defined in the source MIB.
- **Remediation Suggestion**: Contains the suggested remediation for this event as defined in the source MIB.
- **Trap Parameter**: Contains the parameters and parameter values for this particular trap.
- You can add trap filter rules for the selected trap by clicking on the Filter the Trap link located on the right Action navigation tree in the Trap Details page. This navigates you to the Add Filtering Rule page. For instructions on creating a trap filtering rule, see "Filtering traps with user-defined trap filter rules" (page 534).
- You can also escalate the selected trap to an alarm by clicking on the Escalate to alarms link located on the right Action navigation tree in the Trap Details page. This navigates you to the Trap to Alarm—Add Alarm Generation Settings page. For instructions on escalating a trap to an alarm, see "Generating alarms from traps" (page 538).

Trap query

You can query all received traps by Basic Query or by Advance Query.

To query for traps by basic query

To query traps by time or by source IP address:
1. Navigate to Browse Trap.
2. Click the Alarm tab from the tabular navigation system on the top.
3. Click Trap Management on the navigation tree on the left.
4. Click Browse Trap under Trap Management from the navigation system on the left.
If a Basic Query link appears at the upper right corner of the Trap Query section, the current query mode is Advanced Query.

5. To enter Basic Query mode, click the Basic Query link.
6. To query all traps by time, click the Time list, select the time range you want to query by, and click Query.
7. To query by device IP address, enter the IP address you want to view traps from in the Device IP field and click Query.

To query for traps by advanced query

To query traps by IP address in the advanced query mode:
1. Navigate to Browse Trap.
2. Click the Alarm tab from the tabular navigation system on the top.
3. Click Trap Management on the navigation tree on the left.
4. Click Browse Trap under Trap Management from the navigation system on the left.
   If an Advanced Query link appears at the upper right of the Trap Query section, the current query mode is Basic Query.
5. To enter the Advanced Query mode, click the Advanced Query link.
6. To query by device IP address, enter the IP address that you want to view traps from in the Device IP field.
7. Click Add, the device IP address is added to Selected Devices field.
8. Click Select located to the right of the Selected Devices field. The Select Devices dialog box appears.
9. Add devices either By View or using the Advanced query option. See "Adding devices by View" (page 85) and "Adding devices by Advanced query" (page 85).

Filtering traps with existing IMC Trap filter rules

Effective trap management requires careful consideration of which traps are useful to the organization and the consequent configuration of the network devices that send traps and the management station that receives them. More often than not though, some of these steps are skipped as network administrators and network management administrators rarely have time for this. Frequently, network devices are often configured either to send more traps than are useful or necessary or to send none at all.

You can more effectively manage the reception of traps for reporting incidents and their resolution in the network infrastructure through trap filtering. Trap filtering lets you distinguish between traps received by devices in the infrastructure that are useful from those that are not before traps are translated into alarms for viewing and notification.

You can create user defined trap filter rules and tmodify them in IMC.

Viewing IMC trap filter rules

To view existing IMC trap filter rules:
1. Navigate to Filtering Trap.
2. Click the Alarm tab from the tabular navigation system on the top.
3. Click Trap Management on the navigation tree on the left.
4. Click Filtering Trap under Trap Management from the navigation system on the left.
IMC is configured with the following trap filter rules.

- **Duplicate Trap Filter**: This filter rule reduces the possibility of event storms in IMC by filtering out duplicate traps from reporting and display when thresholds are met.

- **Intermittent Trap Filter**: This filter rule reduces the possibility of event storms by detecting when there is an intermittent problem in the network and setting thresholds when intermittent issues occur to eliminate the redundant alarming that occurs when intermittent issues arise.

- **Unknown Trap Filter**: Devices in the network infrastructure are often configured to send traps to management systems even when the management system is not configured to manage the source of the trap. Thus, these traps might be unknown and indecipherable to IMC. This filter rule lets you remove unknown traps from IMC views and reports.

- **Unmanaged Devices’ Trap Filter**: Devices in the network infrastructure are often configured to send traps to management systems even when the management system is not configured to manage these devices and receive traps from them. This filter rule lets you remove these traps from IMC views and reports.

Only administrators or operators who are members of a group with the ADMIN privilege level can add or modify trap filters.

**Modifying the duplicate trap filter rule**

This filter reduces the possibility of event storms in IMC by filtering out duplicate traps from reporting and display once thresholds are met.

To modify the **Duplicate Trap Filter** rule:

1. Navigate to **Filtering Trap**.
2. Click the **Alarm** tab from the tabular navigation system on the top.
3. Click **Trap Management** on the navigation tree on the left.
4. Click **Filtering Trap** under **Trap Management** from the navigation system on the left.
5. Click the **Modify** icon to the right of the **Duplicate Trap Filter**.
6. Click the **Escalate to alarms** checkbox [ ] if you want an alarm to be generated and displayed in IMC if the number of traps received for each duplicate trap type exceeds the value configured in the **Threshold** field.
   
   If you check this box, you need to define the threshold setting. Threshold determines how many duplicate traps are received before IMC generates an alarm. The default is 100.

   7. Click on the checked **Escalate to alarms** box [ ] if you do not want to receive any alarms in IMC notifying you that devices in the network infrastructure are sending duplicate alerts for the same error condition.

   8. Click the **Filter Repeated Traps** checkbox [ ] if you want IMC to use both the **Length of Trap Queue** and the length of time window defined below in the **Length of Time Window** field for escalating duplicate traps to alarms.

   9. Leave the **Filter Repeated Traps** checkbox unchecked [ ] if you only want to use the **Escalate to alarms** threshold for escalating duplicate traps to alarms.

   One of the two parameters listed in steps 3 and 4 must be checked to configure the remaining parameters of this trap filter rule.
Operators can remove specific traps from this trap filter rule so that all traps for the selected trap type are always reported. To remove specific trap types from being included in this rule and de-duplicated:

10. Click **Select** to the right of the **Unfiltered Duplicate Traps** field.

11. In the **Select Trap** dialog box, locate the MIB that contains the trap you want to exclude from this de-duplication rule.

12. To expand your view of the MIB, click the arrow key next to the MIB.

13. Click the **Expand all** icon located in the upper right corner of the **Select Trap** dialog box to expand your view to display all traps.

14. Use the query function located at the top of the **Select Trap** dialog box to locate a particular trap. As with most IMC search features, fuzzy matching is supported so partial and complete search criteria is acceptable.

15. Enter one or more of the following search criteria:
   - **Trap Name**: Enter a partial or complete object name for the trap you want to locate in the **Trap Name** field.
   - **Trap OID**: Enter a partial or complete Object ID for the trap in the **Trap OID** field.
   - **Enterprise Name**: Enter a partial or complete name for the Enterprise MIB you want to locate in the **Enterprise Name** field.
   - **Enterprise OID**: Enter a partial or complete Enterprise ID for the MIB you want to locate in the **Enterprise OID** field.

16. Click **Query** to submit your search criteria. The result of your query is displayed in the dialog box.

17. Click **Reset** to clear your query criteria and to restore the full list of MIBs and traps.

18. Click the checkbox to select a MIB object that you want to add to the filtering rule.

19. Click the checked box to remove a MIB object from the filtering rule.

20. Click **OK**.

   It can take a while for the **Select Trap** dialog box to close. When it does, it updates the **Unfiltered Duplicate Traps** field with the configured trap.

   You can click multiple checkboxes to select multiple traps to exclude from this de-duplication rule. Each trap is listed in the **Unfiltered Duplicate Traps** field.

   - **Length of Time Window**: Defines the length of time in minutes in which traps would be considered duplicate. Enter the time in minutes. The default is 10 minutes.
   - **Length of Trap Queue**: Defines the maximum number of traps that are kept by IMC. Traps in the trap queue are matched against incoming traps to determine if there is a duplicate trap match. A long trap queue length ensures that the filter catches more traps and a shorter trap queue length reduces the number of traps filtered by this filter. The default is 5000 trap entries. The minimum is 100 and the maximum is 10000.

21. Click the **Use Sliding Time Window** checkbox if you want a sliding window time counter applied to the length of time window for this filter rule.

22. Leave the box unchecked if you want to apply a fixed time window.

23. Click **OK**.
Modifying the intermittent trap filter rule

This filter reduces the possibility of event storms by detecting when there is an intermittent problem in the network and setting thresholds for reporting when intermittent issues occur and eliminating the redundant alarming that occurs when intermittent issues arise.

To modify the Intermittent Trap Filter
1. Navigate to Filtering Trap.
2. Click the Alarm tab from the tabular navigation system on the top.
3. Click Trap Management on the navigation tree on the left.
4. Click Filtering Trap under Trap Management from the navigation system on the left.
5. Click the Modify icon in the Modify field associated with the Intermittent Trap Filter rule.
6. Click the Escalate to alarms box if you want an alarm to be sent to and displayed in IMC if the number of traps received for each intermittent trap type exceeds the value configured in the Threshold field.
   If you check this box, you need to define the threshold setting. The threshold determines how many traps are received before IMC generates an alarm. The default is 3.
7. Click the checked Escalate to alarms box if you do not want to receive any alarms notifying you that devices in the network infrastructure are sending intermittent alerts for the same error condition.
   The Escalate to alarms box must be checked to configure the parameters of this trap filter rule.
   You can add specific traps to this trap filter rule so that all traps for the selected trap type are included in this intermittent trap filter.
8. To add specific trap types to this rule, do the following:
9. Click Select to the right of the field below the Threshold field.
10. In the Select Trap dialog box, locate the MIB that contains the trap you want to exclude from this de-duplication rule.
11. To expand your view of the MIB, click the arrow key next to the MIB that the trap that you want to exclude from this de-duplication rule.
12. To expand your view of the MIB, click the arrow key next to the MIB that contains the trap that you want to add.
13. Click the Expand all icon located in the upper right corner of the Select Trap dialog box to expand your view to display all traps.
   You can also use the query function located at the top of the Select Trap dialog box to locate the trap you want to add. Fuzzy matching is supported so partial and complete search criteria is acceptable.
14. Enter the following search criterion:
   o Enterprise ID/Name: Enter a partial or complete name/ID for the Enterprise MIB you want to locate in the Enterprise ID/Name field.
15. Click Query to submit your search criteria.
   The results of your query display in the dialog box.
16. Click Reset to clear your query criteria and to restore the full list of MIBs and traps.
17. Click the checkbox to select a MIB object that you want to add to the filtering rule.

18. Click the checked box to remove a MIB object from the filtering rule.

19. Click OK. It can take a while for the Select Trap dialog box to close. When it does, it updates the field with the configured trap.

20. Click multiple checkboxes to select multiple traps to exclude from this de-duplication rule. Each trap is listed in the field.
   - Length of Time Window: defines the duration in time that traps would be considered intermittent. Enter the time in seconds. The default is 1 second.
   - Length of Trap Queue: defines the maximum number of traps that are kept. Traps in the trap queue are matched against incoming traps to determine if there is a duplicate trap match. A long trap queue length ensures that the filter catches more traps and a shorter trap queue length reduces the number of traps filtered by this filter. The default is 5000 trap entries. The minimum is 100 and the maximum is 5000.

21. Click the Use Sliding Time Window box if you want a sliding window time counter applied to the Length of Time window for this filter rule.

22. Leave the box unchecked if you want to apply a fixed time window.

23. Click OK.

**Modifying the unknown trap filter rule**

Devices in the network infrastructure are often configured to send traps to management systems even when the management system is not configured to receive them. Thus, these traps are unknown and indecipherable to IMC. This filter allows you to remove unknown traps from IMC views and reports.

To modify the Unknown Trap Filter:

1. Navigate to Filtering Trap.
2. Click the Alarm tab from the tabular navigation system on the top.
3. Click Trap Management on the navigation tree on the left.
4. Click Filtering Trap under Trap Management from the navigation system on the left.
5. Click the Modify icon to the right of the Unknown Trap Filter.
6. Click the Escalate to alarms box if you want an alarm to be sent to and displayed in IMC if the number of traps received for unknown traps exceeds the value configured in the Threshold field. If you check this box, you need to define the threshold setting. Threshold determines how many traps are received before IMC generates an alarm. The default is 1000.
7. Click the checked Escalate to alarms box if you do not want to receive any alarms in IMC notifying you that devices in the network infrastructure are sending traps that are unknown to IMC. The Escalate to alarms box must be checked to have the ability to configure the parameters of this trap filter rule.
8. Click the Filter Unknown Traps box if you want IMC to discard all traps for which the trap type is unknown to IMC.
9. Click the checked box ✓ if you want IMC to receive and report unknown traps.
10. Click OK.

Modifying the unmanaged devices trap filter rule

Devices in the network infrastructure are often configured to send traps to management systems even when
the management system is not configured to manage these devices and receive traps from them. This filter lets
you discard traps from unmanaged devices.

To modify the unmanaged devices trap filter:
1. Navigate to Filtering Trap.
2. Click the Alarm tab from the tabular navigation system on the top.
3. Click Trap Management on the navigation tree on the left.
4. Click Filtering Trap under Trap Management from the navigation system on the left.
5. Click the Modify icon 📂 to the right of the Unmanaged Devices' Trap Filter.
6. Click the Escalate to alarms box ☑ if you want an alarm to be sent to and displayed in IMC if the
   number of traps received for unknown traps exceeds the value configured in the Threshold field.
   If you check this box, you need to define the threshold setting. Threshold determines how many traps
   are received before IMC generates an alarm. The default is 1000.
7. Click the Escalate to alarms checked box ☑ if you do not want to receive any alarms in IMC
   notifying you that devices in the network infrastructure are sending traps that are unknown to IMC.
   The Escalate to alarms box must be checked for you to configure the parameters of this trap filter rule.
8. Click the Filter Traps from unmanaged devices box ☑ if you want to discard traps sent from
   unmanaged devices.
9. Click the checked box ✓ if you want to receive traps from unmanaged devices.
10. Click OK.

Filtering traps with user-defined trap filter rules

Effective use and management of traps for reporting faults in the network infrastructure requires trap filtering.
User defined trap filtering lets you define your own trap filters to determine for your environments the traps
that are useful from those that are not.

Adding a user-defined trap filter rule

To add a user defined trap filter:
1. Navigate to Filtering Trap.
2. Click the Alarm tab from the tabular navigation system on the top.
3. Click Trap Management on the navigation tree on the left.
4. Click Filtering Trap under Trap Management from the navigation system on the left.
5. Click Add in Filtering Trap window.
6. Enter a unique name for this filtering rule in the Filtering Rule Name field.
7. Select the filter mode for this rule from the **Filter Mode** list:
   - **By Common Trap Group**: Select this option if you want to filter by the trap groups defined by IMC.

   There are two types of common trap groups in IMC. The first is the interface **UP/DOWN Trap Group**. This group provides filtering for interface UP and DOWN traps. Interface UP and DOWN traps are generated by two sources. The first UP/DOWN trap source is IMC through its device polling. The second source of UP/DOWN traps are the managed devices. For a managed device to send UP/DOWN traps, it must be configured to send them and it must be configured to forward them to IMC. In addition, IMC must be configured to receive them, which is done when a device is added to IMC.

   You must specify which interfaces on every device you want to filter UP/DOWN traps for. If you do not specify the device interfaces, IMC filters out UP/DOWN traps for all interfaces on all devices.

   The second type of common trap group is the **IMC Trap Group**. This option provides filtering for traps sent by IMC modules, including Sysmonitor and MPLS VPN monitor. Selecting this option filters out all traps generated by these IMC modules.

   - **By Trap**: Select this option if you want to define the trap that is used in this trap filtering rule. If you select the **By Trap** option, go to **Step 11**.

8. Select the trap group that you want to filter on from the **Common Trap Group** list if you selected **By Common Trap Group** from the **Filter Mod** list in **Step 7**.

9. Select **IMC Trap Group** if you want to filter traps for IMC Sysmonitor and MPLS VPN Monitor.

10. Select **UP/DOWN Trap Group** if you want to filter for interface UP/DOWN traps.

11. If you select **UP/DOWN Trap Group**, you must also select the devices and their interfaces in which this trap filter rule applies.

   **CAUTION:**

   If you select the **UP/DOWN Trap Group** in the **Common Trap Group** list without selecting the interfaces, the trap filtering rule is applied to all interfaces on all devices.

12. To select interfaces, click **Select** located to the right of the **Interfaces to Filter** field.

### Selecting Interfaces by View

1. From the **Select Interfaces** dialog box, click the **By View** tab.

2. Expand the view you want to select interfaces from by clicking the arrow icon to the left of the four view options, **IP View**, **Device View**, **Custom View**, or **Port Group**.

3. Click on the view you want to select interfaces from the navigation tree on the left. The devices from the group you click appears in the **Device List** tab to the right of the navigation tree. Highlighting a device from the **Device List** tab populates the **Interface List** tab with the highlighted device’s interfaces.

4. Highlight the interfaces you want to select from the **Interface List** tab and do one of the following:
   - Click the **Add selected** button to add them to the **Selected Interface** list, or
   - To select all of the interfaces displayed in the **Interface List** tab, click **Add all**,
   - To remove one or more interfaces, select them and click **Remove selected**,
   - To remove all of the selected interfaces, use **Remove all**.

5. Confirm that the interfaces you have found have been added by reviewing the **Selected Interfaces** list.

6. Click **OK**. Confirm that the interfaces now appear in the **Interfaces to Filter** field.

### Adding interfaces by advanced query
You can also select interfaces using the **Advanced** query option to search IMC using various criteria and use the results of the search to add devices.

1. Click **Select** located to the right of the **Interfaces to Filter** field.
2. From the **Select Interfaces** dialog box, click the **Advanced** tab.
3. Enter values in one or more of the search parameters as follows:
   - **Query By Filter**: Select the filter you want to filter interfaces by. A filter is a set of query criteria. Operators do not need to enter other query criteria if a filter is selected.
   - **Device IP**: Enter the IP address you want to query for. Click on the **Exact Query** checkbox if you want IMC to search for the full IP address you have entered. Leave **Exact Query** box unchecked if you want IMC to match only a certain portion of the IP address.
   - **Device IP List**: Configure multiple device IP addresses to be searched. Click the link. Then, the **Device IP List Configuration** window appears. Enter one or multiple device IP addresses in the **Input Device IP** field (if you enter multiple IP addresses, enter one IP address on each line), and then click **Add** to add the entered IP addresses to the **Device IP List** field below. Repeat the steps above to add all device IP addresses to be searched. To delete an IP address in the **Device IP List** field, select the IP address and then click **Delete**. Click **OK** to complete the operation. Make sure that the device IP addresses to be searched have been added to the **Device IP List** field. To clear the **Device IP List** field, click the link.
   - **Device Label**: Enter the name for the devices you want to add. IMC supports fuzzy matching for device labels. Therefore, you can enter the entire device label for the device you want to locate, or you can enter just a portion of it. IMC displays all matches that contain the portion you enter.
   - **Interface Alias**: Enter the alias for the interface you want to filter on.
   - **Interface Type**: Select an interface type from the **Interface Type** list.
   - **Interface IP**: Enter the IP address of the interface in which you want to filter. Click the **Exact Query** checkbox if you want IMC to search for the exact IP address you have entered.
   - **Status**: Select the current status of the interfaces you want to filter by.
4. Click **Query** to begin your search.
   The results of your search appear in the **Interface List**.
5. Highlight the interfaces you want to select and do one of the following:
   - Click **Add selected** to add them to the **Selected Interfaces** list, or
   - To select all of the interfaces displayed in the **Interface List**, click **Add all**, or
   - To remove one or more interfaces, select them and click **Remove selected**, or
   - To remove all of the selected interfaces, click **Remove all**.
6. Confirm that the interfaces you have found have been added.
7. Click **OK**. Confirm that the interfaces now appear in the **Interfaces to Filter** field.
8. If you selected **By Trap** in the **Filter Mode** list, you need to select the trap to be filtered for in this rule as follows
9. Click **Select** to the right of the **Alarm Trap Name** field.
10. Do one of the following:
    11. In the **Select Trap** dialog box, locate the MIB that contains the trap in which you want to filter.
        - To expand your view of the MIB, click on the arrow key next to the MIB that contains the trap that you want to add, or
Click the **Expand all** icon  located in the upper right corner of the **Select Trap** dialog box to expand your view to display all traps.

You can also use the query function located at the top of the **Select Trap** dialog box to locate the trap you want to add. Fuzzy matching is supported so partial and complete search criteria is acceptable. Enter one or more of the following search criteria:

- **Trap Name**: Enter a partial or complete object name for the trap you want to locate in the **Trap Name** field.
- **Trap OID**: Enter a partial or complete Object ID for the trap in the **Trap OID** field.
- **Enterprise Name**: Enter a partial or complete name for the Enterprise MIB you want to locate in the **Enterprise Name** field.
- **Enterprise OID**: Enter a partial or complete Enterprise ID for the MIB you want to locate in the **Enterprise OID** field.

12. Click **Query** to submit your search criteria. The results of your query display in the dialog box.
13. Click **Reset** to clear your query criteria and to restore the full list of MIBs and traps.
14. Click on the radio button  to select the trap that you want to add.
15. Click **OK**. It might take a while for the **Select Trap** dialog box to close. When it does, it updates the **Alarm Trap Name** field with the configured trap.
16. If you selected **By Trap** in the **Filter Mode** list, you also need to select the devices to apply this trap filter rule for.

**CAUTION:**
If you select **By Trap** as your **Filter Mode** without selecting the devices, then the trap filtering defined in the rule applies to all devices.

17. Click **Select** located to the right of the **Devices to Filter** field. The **Select Devices** dialog box appears.
18. Add devices either **By View** or using the Advanced query option. See "Adding devices by View" (page 85) and "Adding devices by Advanced query" (page 85).

**Modifying a user-defined trap filter rule**

To modify a user defined trap filter rule:

1. Navigate to **Filtering Trap**.
2. Click the **Alarm** tab from the tabular navigation system on the top.
3. Click **Trap Management** on the navigation tree on the left.
4. Click  **Filtering Trap** under **Trap Management** from the navigation system on the left.
5. Click the **Modify** icon  in the **Filtering Trap** main page associated with the trap filtering rule you want to modify.

**Rule name** entries in the **Filtering Trap** table that are displayed in blue denote user defined filtering rules.

You cannot modify the name of a trap filtering rule once you have created it.

6. Modify the filter mode for this rule from the **Filter Mode** list.
- **Common Trap Group**: Select this option if you want to filter by the trap groups defined by IMC.
- **By Trap**: Select this option if you want to define the trap that is used in this trap filtering rule. If you select the **By Trap** option, go to Step 5.

7. Modify the trap group that you want to filter on from the **Common Trap Group** list.
8. Select **IMC Trap Group** if you want to filter traps for IMC Sysmonitor and MPLS VPN Monitor.
9. Select **UP/DOWN Trap Group** if you want to filter traps for interface up/down traps.
10. If you select **UP/DOWN Trap Group**, you must also select the devices and their interfaces in which this trap filter rule applies.
11. Click **Select** located to the right of the **Interfaces to Filter** field.
12. Add devices either **By View** or using the **Advanced** query option. See "Adding devices by View" (page 85) and "Adding devices by Advanced query" (page 85).

### Deleting a user-defined trap filter rule

To delete a user defined trap filter rule:
1. Navigate to **Filtering Trap**.
2. Click the **Alarm** tab from the tabular navigation system on the top.
3. Click **Trap Management** on the navigation tree on the left.
4. Click **Filtering Trap** under **Trap Management** from the navigation system on the left.
5. Click the **Delete** icon in the **Filtering Trap** list associated with the user defined trap forwarding rule you want to delete.
6. Click **OK** to confirm deletion of the user defined trap-forwarding rule.

You can only delete user-defined trap forwarding rules. You cannot delete IMC generated trap forwarding rules.

### Generating alarms from traps

IMC relies on system and user defined rules to determine which traps generate alarms. IMC includes many system-defined rules that upon installation generate alarms based on traps received by IMC. You can also create user-defined rules that generate alarms based on traps received by IMC.

You can create these from scratch or you can copy an existing system defined rule and modify it to meet your needs. You also have the ability to enable and disable system and user defined rules and upgrade traps to alarms system wide. You can choose to escalate traps to alarms based on traps that match alarm rules or traps that do not match alarm rules. After you upgrade a trap to an alarm, the severity level does not change.

### Browsing trap to alarm rules

To view all **Trap to Alarm** rules:
1. Navigate to **Trap to Alarm**.
2. Click the **Alarm** tab from the tabular navigation system on the top.
3. Click **Trap Management** on the navigation tree on the left.
4. Click **Trap to Alarm** under **Trap Management** from the navigation system on the left.

IMC displays all trap to alarm entries in the **Trap to Alarm** list displayed in the main pane of the **Trap to Alarm** window. The following section describes each of the columns in this list.
Trap to alarm list fields

- **Rule Name**: Contains the trap to alarm rule name. Clicking on the link in this field navigates you to the Alarm Generation Setting Details page that displays the details of this alarm setting.
- **Rule Description**: Provides a general description of the rule. System generated rules contains the value "default rule" in this field while you can provide descriptions for user defined rules that lets you identify the purpose of rules you have created.
- **Type**: Identifies the creator of the rule - system defined or operator (user) defined.
- **Status**: Provides a current status of the rule and the ability to enable or disable a rule.
- **Modify**: Provides you with a link for modifying the associated rule.
- **Copy**: Provides you with a link for copying an existing rule to serve as a foundation for a user defined or operator defined rule.

You can sort the Trap to Alarm List by the Rule Name, Rule Description, Type, or Status fields. Click the column label to sort the list by the selected field. The column label is a toggle switch that lets you toggle between the various sort options specific to each field.

5. Click 8, 15, 50, 100, or 200 from the right side of the main pane to configure how many items per page you want to view.

6. For Trap to Alarm Lists that have more than one page, click 1, 2, 3, 4, 5, 6 from the bottom right side or the top center of the main pane to jump to a particular page of the trap list.

Creating a user-defined trap to alarm rule

To create a user defined trap to alarm rule:
1. Navigate to Trap to Alarm.
2. Click the Alarm tab from the tabular navigation system on the top.
3. Click Trap Management on the navigation tree on the left.
4. Click Trap to Alarm under Trap Management from the navigation tree on the left.
5. Click Add.
6. Enter a unique name in the Rule Name field.
7. Enter a description in the Rule Description field.
8. Click the checkbox to the left of Keywords if you want to add a keyword to this trap to alarm rule. Keywords can be any word found in the Selected Keywords field of a trap.
9. Select the logical operator you want to use for this rule from the Logical Combination list. If you select AND, an alarm is generated when all keywords in the Selected Keywords field are matched. If you select OR, an alarm is generated when any keyword in the Selected Keywords field is matched. Only one logical operator can be used in a rule. This parameter is meaningful only if you add more than one keyword.
10. Select the keyword condition from the **Keyword** list. Select **Yes** if you want the trap to contain the keyword. Select **No** if you want to alarm on traps that do not contain the keyword.

11. Enter the keyword you want to match on in the **Keyword** field to the right of the **Keyword** list. The total number of characters of all the keywords cannot exceed 256.

12. Click **Add** to add the keyword condition and keyword to the **Selected Keywords** for the trap to generate an alarm.
   If you want to remove any keyword condition and keyword, highlight the keyword condition and keyword and click **Delete** located to right of the **Selected Keywords** field.
   You can have more than one keyword and each keyword can use yes or no. However, you can only have one **AND/OR** logical operator in a rule.

13. Click the checkbox to the left of **Trap Source** if you want to define which devices in which this Trap to Alarm rule generate alarms.

⚠️ **CAUTION:**
If you do not specify a trap source, the Trap to Alarm rule applies to all devices.

14. Select **Yes** or **No** from the **Trap Source If Match** list:
   - Select **Yes** if you want the trap source to match one of the IP addresses specified in the **Selected Devices** fields, or
   - Select **No** if you do not want the trap source to match one of the IP addresses specified in the **Selected Devices** fields.
   You can select multiple IP addresses as the trap source but you can only have one **IF Match** condition for trap source in a rule.

15. Enter the IP address of the device you want to include or exclude in the **Device IP** field.

16. Click **Add**.

17. Add multiple devices by first selecting **Yes** or **No** in the **IF Match** field and then entering the IP address for every device you want to include in this Trap to Alarm rule.

18. Add devices by selecting devices by views that have already been discovered or managed in IMC.

19. Click **Select** located to the right of the **Selected Devices** field. The **Select Devices** dialog box appears.

20. Add devices either **By View** or using the **Advanced** query option. See "Adding devices by View" (page 85) and "Adding devices by Advanced query" (page 85).

**Trap to alarm upgrade strategy**
You can create user-defined rules that upgrade received traps to alarms either when the trap matches the rule or when a trap does not match the alarm rule conditions. To use this feature, you must first create the Trap to Alarm rule and then apply the upgrade strategy to the alarm rule. For more information on creating a user defined trap to alarm rule, see "Creating a user-defined trap to alarm rule" (page 539).

To modify the **Trap to Alarm** strategy:
1. Navigate to **Trap to Alarm**.
2. Click the **Alarm** tab from the tabular navigation system on the top.
3. Click **Trap Management** on the navigation tree on the left.
4. Click ** Trap to Alarm** under **Trap Management** from the navigation system on the left.
   IMC displays all trap to alarm entries in the **Trap to Alarm** List displayed in the main pane of the **Trap to Alarm** window.

540
The current upgrade strategy is displayed above the Trap to Alarm list.

5. Click the Modify link at right of the Upgrade Strategy, the upgrade strategy list appears.
6. Select the Trap to Alarm upgrade strategy you want to use from the Upgrade Strategy list.
7. Select Upgrade Traps matching the rules to alarm if you want IMC to escalate a trap to an alarm if the trap’s contents match the conditions defined in the Trap to Alarm rule list.
8. Select Upgrade Traps not matching the rules to alarm if you want IMC to escalate a trap to an alarm if the trap’s contents do not match the conditions defined in the Trap to Alarm rule list.
9. Click OK to accept the upgrade strategy for the alarms you have selected.

Modifying and copying trap to alarm rules

The Copy feature for Trap to Alarm rules lets you create a new rule by making a copy of an existing system or user-defined rule and make whatever modifications are necessary to the copy.

With this feature, you can make changes to a system-defined rule, as IMC does not allow modifications to system-defined rules. The Copy feature also provides you with the additional benefit of changing the name of a Trap to Alarm rule, which the Modify feature does not.

The process for copying a Trap to Alarm rule is similar to the process for modifying a rule.

1. Navigate to Trap to Alarm.
2. Click the Alarm tab from the tabular navigation system on the top.
3. Click Trap Management on the navigation tree on the left.
4. Click Trap to Alarm under Trap Management from the navigation tree on the left.
5. Do one of the following:
   - Click the Copy icon associated with the rule you want to copy, or
   - Click the Modify icon associated with the user-defined rule you want to modify.
6. If you are copying a rule, you can rename the rule by entering the new name in the Rule Name field. Rule names must be unique.
   You cannot modify the name of a rule once it has been created. To modify a rule name, you must use the Copy option to copy the contents of a system or user-defined rule to a new user-defined rule.
7. Enter a description in the Rule Description field.
8. Click the checkbox to the left of Keywords if you want to add or modify a keyword in this Trap to Alarm rule.
9. Change the logical operator for this rule as needed in the Logical Combination field.
   This parameter is meaningful only if you add more than one keyword.
10. Do one of the following:
    - If you choose the logical operator AND with multiple keywords, all keywords must be found in the description field of the trap for the trap to generate an alarm, or
    - If you select the logical operator OR, only one of the words must exist in the description field of the trap for an alarm to be generated. Only one logical operator can be used in a rule.
11. Add the keyword condition from the Keyword list.
12. Do one of the following:
    - Select Yes if you want the trap to contain the keyword, or
o Select **No** if you want to alarm on traps that do not contain the keyword.

13. Add the keywords you want to match on in the **Keyword** field to the right of the **Keyword** list. The total number of characters of all the keywords cannot exceed 256.

14. Delete keywords as necessary by using the **Delete** button to the right of the **Selected Keywords** field.

15. To modify the added keyword conditions, delete undesirable keyword conditions and then add new ones.

16. Click the checkbox □ to the left of **Trap Source** if you want to modify which devices in which this Trap to Alarm rule generate alarms.

17. Select **Yes** or **No** from the **Trap Source If Match** list:
   - o Select **Yes** if you want the trap source to match one of the IP addresses specified in the **Selected Devices** fields, or
   - o Select **No** if you do not want the trap source to match one of the IP addresses specified in the **Selected Devices** fields.

18. Modify or remove the IP address of the devices you want to include or exclude in this trap to alarm field in the **Device IP** field by highlighting the IP addresses you want to remove and click the **Delete** button to the right of the **Trap Source** field.

19. To add devices, refer to the step on adding devices in the previous section of this manual.

20. Click the checkbox □ to the left of **Trap Type** if you want to define the traps in which this Trap to Alarm rule generates alarms.

21. Select **Yes** or **No** from the **Trap Type If Match** list:
   - o Select **Yes** if you want the alarms to be generated for the trap type selected, or
   - o Select **No** if you want to do not want alarms to be generated for the trap type selected.

   You can select multiple traps as the trap type, but you can only have one **IF Match** condition for trap type in a rule.

22. Select the traps you want to add this trap to alarm rule by clicking **Select** to the right of the **Trap Name** field.

23. In the **Select Trap** dialog box, locate the MIB that contains the trap that you want.

24. Do one of the following:
   - o To expand your view of the MIB, click on the arrow key next to the MIB that contains the trap that you want to add, or
   - o Click the **Expand all** icon located in the upper right corner of the **Select Trap** dialog box to expand your view to display all traps.

   You can also use the query function located at the top of the **Select Trap** dialog box to locate the trap you want to add.

25. Enter one or more of the following search criteria:
   - o **Trap Name**: Enter the object name for the trap you want to locate in the **Trap Name** field.
   - o **Trap OID**: Enter the Object ID for the trap in the **Trap OID** field.
   - o **Enterprise Name**: Enter a partial or complete name for the Enterprise MIB you want to locate in the **Enterprise Name** field.
   - o **Enterprise OID**: Enter a partial or complete Enterprise ID for the MIB you want to locate in the **Enterprise OID** field.
26. Click **Query** to submit your search criteria.
   The results of your query display in the dialog box.
27. Click **Reset** to clear your query criteria and to restore the full list of MIBs and traps.
28. Click on the checkbox [ ] to select the trap that you want to include in this rule.
29. Click **OK**.
   It can take a while for the Select Trap dialog box to close. When it does, it updates the Trap Name field with the modified traps.
30. To delete any of the existing traps, highlight the traps you want to delete and click on the Delete button located to the right of the Trap Name field.
31. Modify the trap parameter settings by clicking on the Parameter Settings to the right of the Trap Name field.
32. Add any values to the variables displayed in the Set Alarm Parameters dialog box.
33. Click **OK**.
   These parameters vary based on the trap you have selected in the Trap Name field.
34. Click the Delete button [ ] if you want to remove the parameter from the parameter settings configuration. By deleting a parameter, you are removing it from IMC’s evaluation of the trap for alarming purposes.
35. Click the checkbox [ ] to the left of Time Range if you want to define when this trap to alarm rule generates alarms.
36. Select the period of time to which this trap to alarm rule applies from the Validity Period Configuration list.
37. Select Weekly if you want to define the days of the week and the hourly range.
38. Do one of the following:
   o Click the checkbox [ ] next to the day of the week in which you want to apply this trap to alarm rule, or
   o Click a checked box [ ] to remove the rule for that day.
39. Select By Time Range if you want to set a specific date and time range for this trap to alarm rule.
40. If you selected By Time Range, enter:
   o **Start Date**: You can auto populate this field by clicking the Calendar icon [ ] located to the right. A popup calendar appears. Select the start date from the calendar.
   o **End Date**: You can auto populate this field by clicking the Calendar icon [ ] located to the right. A popup calendar appears. Select the start date from the calendar.
41. Enter the Start Time for every day in which you have applied this trap to alarm rule.
42. Enter the Start Time and End Time for every day in which you have applied this trap to alarm rule.
43. Click **OK**.

**Enabling/disabling trap to alarm rules**

To enable or disable Trap to Alarm rules:
1. Navigate to **Trap to Alarm**.
2. Click the **Alarm** tab from the tabular navigation system on the top.
3. Click **Trap Management** on the navigation tree on the left.
4. Click **Trap to Alarm** under **Trap Management** from the navigation tree on the left.
5. Do one of the following:
   - To enable a **Trap to Alarm** rule, click the disabled status icon \(\times\) **Disable** in the **Status** field for the target rule, or
   - To disable a **Trap to Alarm** rule, click the enabled status icon \(\checkmark\) **Enable** in the **Status** field for the target rule.

**Trap definition settings**

You can define which of the received traps IMC can process and is considered known traps. Trap definitions determine which of all traps received are known to IMC.

**Viewing trap definitions**

To view all trap definitions in IMC:
1. Navigate to **Trap Definition**.
2. Click on the **Alarm** tab from the tabular navigation system on the top.
3. Click on **Trap Management** on the navigation tree on the left.
4. Click on **Trap Definition** under **Trap Management** from the navigation tree on the left.

IMC displays all trap definitions in the **Trap Definition** list displayed in the main pane of the **Trap Definition** screen.

   - **Trap Name**: Contains the name of the trap. The trap name serves as a link to navigate to the **Trap Definition Details** page.
   - **Trap OID**: This field Contains the Object ID of the trap.
   - **Enterprise Name (Enterprise ID)**: Contains the name of the Enterprise and its Object ID.
   - **Severity**: Contains the severity setting for the trap. The severity setting is equivalent to the alarm level in IMC.
   - **Type**: Contains the source of the trap, whether it is **System Defined** or **User Defined**.
   - **Modify**: Contains a link to the **Modify Trap** definition page for modifying the associated trap.
   - **Delete**: Contains an icon for deleting the associated trap.

You can sort the **Trap Definition** list by the **Trap Name**, **Trap OID**, **Severity**, or **Type** fields. Click the column label to sort the list by the selected field. The column label is a toggle switch that lets you toggle between the various sort options specific to each field.

5. Click **8**, **15**, **50**, **100**, or **200** from the right side of the main pane to configure how many items per page you want to view.
   - Click to page forward in the **Trap Definition** list.
   - Click to page forward to the end of the **Trap Definition** list.
6. For Trap Definition Lists that have more than one page, click 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 from the bottom right side or top center of the main pane.

7. To jump to a particular page of the trap list, click on the page number you want to jump to.

**Querying for a trap**

Operators can also query IMC for specific details in a trap.

To query IMC for a trap:

1. Navigate to Trap Definition.
2. Click the Alarm Tab from the tabular navigation system on the top.
3. Click Trap Management on the navigation tree on the left.
4. Click Trap Definition under Trap Management from the navigation tree on the left.
5. Enter one or more of the following search criteria in the Trap Query section of the Trap Definition window, using partial or complete entries as IMC supports fuzzy matching:
   - **Trap Name**: Enter a partial or complete name for the trap. For example, to query for a trap definition with the name, alarmFeBlock, enter alarmFeBlock in the **Trap Name** field.
   - **Enterprise Name**: Enter partial or complete name for the vendor whose MIB contains the trap you want to query for. For example, to query for all 3Com traps, enter 3Com in the **Enterprise Name** field.
   - **Trap OID**: Enter partial or complete Object ID for the trap in which you want to query. For example, the object ID for alarmFeBlock is 1.3.6.1.4.1.43.1.12.3.6.155. Enter 1.3.6.1.4.1.43.1.12.3.6.155 in the **Trap OID** field to retrieve traps with this Object ID.
   - **Enterprise ID**: Enter partial or complete Enterprise ID for the vendor whose MIB contains the trap in which you want to query. For example, the Enterprise ID for 3Com is 1.3.6.1.4.1.43.1.12.3. Enter 1.3.6.1.4.1.43.1.12.3 to retrieve all traps by 3Com from the trap definition list.

**Adding trap definitions**

You can customize IMC by adding user defined trap definitions that process, interpret and display traps received by IMC. In addition, you can modify existing, system-defined traps.

IMC provides the ability to deduplicate multiple instances of the same trap for the same device or the same component on the same device for the same event. IMC provides a system defined trap filter, called the Duplicate Trap Filter that. To deduplicate traps in IMC, the trap Object ID, the source device, and the Key Parameter fields must be identical. The trap Object ID is defined in the MIB definition file and the source of the trap is defined by its IP address. With user defined trap definitions, the operator defines which object in a MIB file is used to deduplicate traps.

The same rules apply when you want to associate a clear or restore trap with the trap that reports an error or fault. To create a trap definition that automatically allows a restore trap to clear or recover an alarm in IMC that was generated by a trap, you first create the trap definition that reported the error. Then, you create another trap that is configured as a Restore Trap and includes in the Restore Trap configuration the traps that is cleared or recovered by the restore trap.

The trap reporting the error and the trap reporting the recovery must contain the same Object ID that is configured as the Key Parameter in the Set Parameter configuration.
For example, in the system defined trap definition for reporting a link down is Link Down. The Link Down trap OID is 1.3.6.1.6.3.1.1.5.2.0 and it has the Interface Index OID 1.3.6.1.2.1.2.2.1.1 configured as the Key Parameter. The system defined trap definition for automatically clearing or recovering the Link Down trap event is the Link Up trap. The Link UP trap OID is 1.3.6.1.6.3.1.1.5.3.0 and it also has the Interface Index OID 1.3.6.1.2.1.2.2.1.1 configured as the Key Parameter.

In its Restore Trap settings, it has the Link Down trap configured with the OID as 1.3.6.1.6.3.1.1.5.2.0. In essence, the trap definition for clearing the trap contains the key parameters and the trap definition that identifies the error condition.

Once you have added trap definitions to the trap definition list, then received traps are displayed in the Trap List of under Browse Trap feature. The Trap List displays all traps received by IMC. For more information on viewing received traps, see "Browsing alarms" (page 568).

You can also generate alarms based on traps received in the Trap to Alarm feature. For more information on this feature, see "Generating alarms from traps" (page 538).

To add a trap definition:

1. Navigate to Trap Definition.
2. Click the Alarm tab from the tabular navigation system on the top.
3. Click Trap Management on the navigation tree on the left.
4. Click Trap Definition under Trap Management from the navigation tree on the left. The Trap Definition page appears.
5. Click Add. The Add Trap page appears.
6. Enter the Object ID for this trap in the Trap OID field. This value must correspond with the Object ID of the received traps that is processed by this definition.

The Object ID for any trap can be found in the system or vendor’s MIB.

A trap OID is composed of three parts: the enterprise ID, the generic ID, and the specific ID. The number following the last dot "." is the specific ID. The number following the second to the last dot "." is the generic ID, and all remaining numbers constitute the enterprise ID.

For example, if the trap OID is:
1.3.6.1.4.1.2011.2.23.11.2.6.2001
- the specific ID is 2001
- the generic ID is 6
- the enterprise ID is 1.3.6.1.4.1.2011.2.23.11.2.

**IMC Rules for processing Trap Object IDs**

If the Object ID is a standard OID, the system does not process it.

If the enterprise ID exists in the system, the enterprise name you enter must be the same as that defined in the system.

If the number following the next to the last dot "." is "0", it is replaced with a "6" so that it can be used as the generic ID.

If the number following the next to the last dot is "6", IMC leaves this value unchanged as the generic ID.

If the number following the next to the last dot is neither "0" nor "6", the system adds ".6" after the number and use it as the generic ID.

For example following the rules outlined above,
1.3.6.1.4.1.2011.2.23.11.2.0.2001 is converted to 1.3.6.1.4.1.2011.2.23.11.2.6.2001
1.3.6.1.4.1.2011.2.23.11.2.0.2001 is converted to 1.3.6.1.4.1.2011.2.23.11.2.6.2001
and 1.3.6.1.4.1.2011.2.23.11.2.6.2001 l remains unchanged.

7. Enter a unique name for this trap in the Trap Name field. Maximum length is 64 characters.

8. Enter the enterprise name for this trap in the Enterprise Name field.
If the enterprise ID already exists in IMC, the enterprise name you enter must match the Enterprise Name defined in IMC.

9. Select the Trap Level (corresponds with Severity Level and Alarm Level) from the Trap Level list. Trap levels include Critical, Major, Minor, Warning, and Info.

10. Enter a description for this trap in the Description field.
The Description field is used to describe the condition that triggered the trap. A brief and clear description of the condition is important for support teams in addressing and communicating faults in the network infrastructure. You can also use the description of the condition that is described in the trap itself.

Using macros in the description field
You can use predefined macros in the Description field. The system replaces the macros with actual values after receiving traps.

The code below provides an example of macro usage in the Trap Description field:
the CPU usage ($4) of device $3 ($2) exceeds the threshold ($5).

Supported macros, listed in Table 29, include:

<table>
<thead>
<tr>
<th>Macro</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>$n</td>
<td>This macro displays the value of a trap variable in the format of a character string, in the range 1 to 99</td>
</tr>
<tr>
<td>$+n</td>
<td>Displays the name of a trap variable in the format of a character string, in the range 1 to 99</td>
</tr>
<tr>
<td>$O</td>
<td>Trap name</td>
</tr>
<tr>
<td>$o</td>
<td>Trap OID</td>
</tr>
<tr>
<td>$R</td>
<td>Trap source name</td>
</tr>
<tr>
<td>$a</td>
<td>Trap source IP address</td>
</tr>
<tr>
<td>$s</td>
<td>Trap severity level</td>
</tr>
<tr>
<td>$x</td>
<td>Date when the trap was generated</td>
</tr>
<tr>
<td>$X</td>
<td>Time when the trap was generated</td>
</tr>
<tr>
<td>$@</td>
<td>Time when the numerical trap was generated</td>
</tr>
<tr>
<td>$E</td>
<td>Trap Enterprise ID</td>
</tr>
<tr>
<td>$S</td>
<td>Trap Specific ID</td>
</tr>
<tr>
<td>$G</td>
<td>Trap Generic ID</td>
</tr>
<tr>
<td>$#</td>
<td>Number of trap variables</td>
</tr>
</tbody>
</table>

11. Enter the cause for the condition for which this trap was sent in the Trap Cause field.
Maximum length of this field is 512 characters.

12. Enter the remediation suggestion for the resolution to the condition indicated by this trap in the Remediation Suggestion field.
   Maximum field length is 128 characters.

13. If you want to define the parameters for this trap definition, click the checkbox next to Set Parameter to define the parameters for this trap definition.

14. Click Add under the Set Parameter checkbox.

15. Enter a name for the parameter in the Parameter Name field.
   Maximum length is 64 characters.

16. Enter the parameter’s Object ID in the Parameter OID field.

17. Select the type of parameter from the Parameter Type list.
   Parameter types for SNMP traps include, UInteger32, Integer32, Counter32, Gauge32, TimeTicks, IPAddress, OID, OctetString, Counter64, Opaque, and Others.
   The trap parameter Object ID and parameter type can be found in the vendor’s MIB definition file.

18. Set the key parameter setting by selecting Yes from the Key Parameter list if this is a key parameter. Select No if it is not.
   The Key Parameter field is used by IMC to pair or match traps sent by the same device or component of a device. For example, devices can generate Link Down and Link Up traps for every interface. You want IMC to process the Link Down trap and generate alarms for every interface that reports this condition.
   You also want IMC to process the Link Up traps that the device sends so that IMC can automatically clear or recover the Link Down alarm condition for the correct interface as soon as it receives the Link UP trap. To do so, you must use the same Object ID for the key parameter in the Link Down definition as you use for the trap definition that identifies the Link Up trap. For the system-defined Link Down/Link Up trap definitions, the Interface Index Object ID is used as the Key Parameter.

19. Click OK.

20. If the trap you are configuring is to clear or recover an event, click the checkbox next to Restore Trap to establish this trap definition as a clear/recover or restore trap definition.
   When configuring a restore trap definition, you must include the traps that are cleared, recovered, or restored by this trap definition.

21. Click Select Trap under the Restore Trap checkbox.

22. In the Select Trap dialog box, locate the MIB that contains the trap definition that are cleared/recovered or restored by this trap definition.

23. Do one of the following:
   o To expand your view of the MIB, click the arrow key next to the MIB that contains the trap that you want to add, or
   o Click the Expand all icon located in the upper right corner of the Select Trap dialog box to expand your view to display all traps.

24. Use the query function located at the top of the Select Trap dialog box to locate the trap you want to add.

25. Enter one or more of the following search criteria:
26. Click **Query** to submit your search criteria.
The results of your query are displayed in the dialog box.

27. Click **Reset** to clear your query criteria and to restore the full list of MIBs and traps.

28. Click the checkbox ✖️ to select the trap to be cleared/recovered or restored by this trap definition.

29. Click **OK**.
   It can take a while for the Select Trap dialog box to close. When it does, it updates the Restore Trap table with the configured restore trap settings.
   The Object ID of the key parameters in the trap to be restored must be the same as that of the key parameters of the trap definition that identifies the fault or error.
   The number of the key parameters in the trap to be restored must be the same as that of the key parameters of the trap definition that identifies the error or fault.
   For restore trap definitions, IMC evaluates the Restore Trap configuration to validate that it has the same Key Parameter configured as the traps listed in the restore trap configuration that identifies the faults. If the Key Parameters configured for all traps is identical, the **Check Result** field contains the value ✅ Pass. If the Key Parameter is not identical for all traps in the Restore Trap Configuration, the **Check Result** field contains the value ⏳ Not Pass.

30. Click **OK**.
   The values for many of the settings in a trap definition can be found in the trap itself. You can view the trap by browsing the MIB using the SNMP MIB browser, known in IMC as MIB Management or by viewing the vendor’s MIB file.

Once you have completed the trap definition configuration, IMC is ready to begin receiving traps from managed devices that are configured to send these traps to IMC. Refer to vendor information for each device’s SNMP configuration to ensure that these traps are configured and that the devices are configured to send traps to IMC.

**Modifying user-defined trap definitions**

You can modify system defined and user defined traps. Operators can change the **Trap Name**, **Enterprise Name**, **Trap Level**, **Description**, **Trap Cause** and **Remediation Suggestion** fields of a trap definition. The **Trap Object ID** field cannot be modified. This feature lets you modify traps to meet your organizational needs as they change.

The **Browse Trap** feature provides a view into real time network conditions. You can customize the information that is displayed with traps to provide network operational staff with meaningful and actionable information.

To modify user defined trap definitions:

1. Navigate to **Trap Definition**.
2. Click the **Alarm** tab from the tabular navigation system on the top.
3. Click **Trap Management** on the navigation tree on the left.

4. Click **Trap Definition** under **Trap Management** from the navigation tree on the left.

5. Click the **Modify** icon in the **Trap Definition** list associated with the trap definition you want to modify.
   
The Trap OID of an existing trap definition cannot be modified.

6. Modify the name for this trap in the **Trap Name** field. Maximum name length is 64 characters.

7. Modify the enterprise name for this trap in the **Enterprise Name** field.
   
   If the enterprise ID already exists in IMC, the enterprise name you enter must match the **Enterprise Name** defined in IMC.

8. Modify the **Trap Level** (corresponds with **Severity Level** and **Alarm Level**) from the **Trap Level** list. Trap levels include **Critical**, **Major**, **Minor**, **Warning**, and **Info**.

9. Modify the description for this trap in the **Description** field.
   
   You can use predefined macros in the **Description** field. The system replaces them with actual values after receiving traps.
   
   The code below provides an example of macro usage in the **Trap Description** field:

   the CPU usage ($4) of device $3 ($2) exceeds the threshold ($5).

   Supported macros, listed in Table 30, include:

**Table 30 Predefined Macro table**

<table>
<thead>
<tr>
<th>Macro</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>$n</td>
<td>This macro displays the value of a trap variable in the format of a character string, in the range 1 to 99</td>
</tr>
<tr>
<td>$+n</td>
<td>Displays the name of a trap variable in the format of a character string, in the range 1 to 99</td>
</tr>
<tr>
<td>$O</td>
<td>Trap name</td>
</tr>
<tr>
<td>$o</td>
<td>Trap OID</td>
</tr>
<tr>
<td>$R</td>
<td>Trap source name</td>
</tr>
<tr>
<td>$a</td>
<td>Trap source IP address</td>
</tr>
<tr>
<td>$s</td>
<td>Trap severity level</td>
</tr>
<tr>
<td>$x</td>
<td>Date when the trap was generated</td>
</tr>
<tr>
<td>$X</td>
<td>Time when the trap was generated</td>
</tr>
<tr>
<td>$@</td>
<td>Time when the numerical trap was generated</td>
</tr>
<tr>
<td>$E</td>
<td>Trap Enterprise ID</td>
</tr>
<tr>
<td>$S</td>
<td>Trap Specific ID</td>
</tr>
<tr>
<td>$G</td>
<td>Trap Generic ID</td>
</tr>
<tr>
<td>$#</td>
<td>Number of trap variables</td>
</tr>
</tbody>
</table>
10. Modify the cause for the condition for which this trap was sent in the **Trap Cause** field.
    Maximum length of this field is 512 characters.

11. Modify the remediation suggestion for the resolution to the condition indicated by this trap in the **Remediation Suggestion** field.
    Maximum field length is 128 characters.

12. If you want to set parameters for this trap definition, click the checkbox next to **Set Parameters** to define the parameters for this trap definition.

13. Click **Add** under the **Set Parameter** checkbox.

14. Modify the name for the parameter in the **Parameter Name** field.
    Maximum length is 64 characters.

15. Modify the parameter OID in the **Parameter OID** field.

16. Select the type of parameter from the Parameter Type list.
    Parameter types for SNMP traps include, **UInteger32**, **Integer32**, **Counter32**, **Gauge32**, **TimeTicks**, **IPAddress**, **OID**, **OctetString**, **Counter64**, **Opaque**, and **Others**.

17. Set the key parameter setting by selecting **Yes** from the **Key Parameter** list if this is a key parameter. Select **No** if it is not.
    The **Key Parameter** field is used by IMC to pair or match traps sent by the same device or component of a device. For example, devices can generate Link Down and Link Up traps for every interface. You want IMC to process the Link Down trap and generate alarms for every interface that reports this condition.
    You also want IMC to process the Link Up traps that the device sends so that IMC can automatically clear or recover the Link Down alarm condition for the correct interface as soon as it receives the Link UP trap. To do so, you must use the same Object ID for the key parameter in the Link Down definition as you use for the trap definition that identifies the Link Up trap. For the system-defined Link Down/Link Up trap definitions, the Interface Index Object ID is used as the **Key Parameter**.

18. Click the checkbox to the left of the parameters you want to move.

19. Click **Delete** to delete the parameters.
    You can reorder the parameters in the Trap rule using the icons located in the **Compositor** field as follows:
    - Use **↑** to move the parameter up one position.
    - Use **↑** to move the parameter to the top of the parameter list.
    - Use **↓** to move the parameter down one position.
    - Use **↓** to move the parameter to the bottom of the list.

20. Click **OK**.

21. If the trap you are configuring is to clear or recover an event, click the checkbox next to **Restore Trap** to establish this trap definition as a clear/recover or restore trap definition. When configuring a restore trap definition, you must include the traps that is cleared, recovered, or restored by this trap definition.

22. Click **Select Trap** under the **Restore Trap** checkbox.
23. In the Select Trap dialog box, locate the MIB that contains the trap definition that is cleared/recovered or restored by this trap definition.

24. Do one of the following:
   - To expand your view of the MIB, click the arrow key next to the MIB that contains the trap that you want to add, or
   - Click the Expand all icon located in the upper right corner of the Select Trap dialog box to expand your view to display all traps.

25. You can also use the query function located at the top of the Select Trap dialog box to locate the trap you want to add. Enter one or more of the following search criteria:
   - **Trap Name**: Enter a partial or complete object name for the trap you want to locate in the Trap Name field.
   - **Trap OID**: Enter a partial or complete Object ID for the trap in the Trap OID field.
   - **Enterprise Name**: Enter a partial or complete name for the Enterprise MIB you want to locate in the Enterprise Name field.
   - **Enterprise OID**: Enter a partial or complete Enterprise ID for the MIB you want to locate in the Enterprise OID field.

26. Click Query to submit your search criteria.
   The results of your query are displayed in the dialog box.

27. Click Reset to clear your query criteria and to restore the full list of MIBs and traps.

28. Click the checkbox to select the trap that is cleared/recovered or restored by this trap definition.

29. Click OK.
   It can take a while for the Select Trap dialog box to close. When it does, it updates the Restore Trap table with the configured restore trap settings.

30. Click the checkbox to the left of the traps you want to delete. Click Delete Trap to delete the traps.

**Restore trap conditions**

The Object ID of the key parameters in the trap to be restored must be the same as that of the key parameters of the trap definition that identifies the fault or error.

The number of the key parameters in the trap to be restored must be the same as that of the key parameters of the trap definition that identifies the error or fault.

For restore trap definitions, IMC evaluates the Restore Trap configuration to validate that it has the same Key Parameter configured as the traps listed in the restore trap configuration that identifies the faults. If the Key Parameters configured for all traps is identical, the Check Result field contains the value Pass. If the Key Parameter is not identical for all traps in the Restore Trap Configuration, the Check Result field contains the value Not Pass. Click OK.

**Modifying trap definition severity settings**

You can change the severity settings of trap definitions for many trap definitions at once.

To modify trap definition severity settings:
1. Navigate to Trap Definition.
2. Click the Alarm tab from the tabular navigation system on the top.
3. Click Trap Management on the navigation tree on the left.
4. Click 🗃 Trap Definition under Trap Management from the navigation tree on the left.

5. Click the checkbox ☑ to the left of the Trap Name for all trap definitions for which you want to change the Severity setting (also referred to as the Alarm Level or Trap Level).

6. Click Modify Severity.

   The Trap Severity Setting page appears.

7. Click the radio button ☑ next to the Setting Style you want to apply these changes to in the Trap Severity Setting page.
   - **All Setting**: Choose this option if you want to apply the same severity or alarm level setting to all selected alarm definitions.
     
     If you select this option, select the severity or alarm level setting you want to apply from the All Setting list.
   - **Individual Setting**: Choose this option if you want to apply severity or alarm level settings individually to every selected trap definition.

8. If you select this option, the Selected Traps list becomes active and you can select the Goal Trap Severity setting for every trap definition listed in the Selected Traps table.

9. Select the Goal Trap Severity setting for every trap definition in which you want to modify the severity setting.
   - **Default Severity**: Choose this option if you want to apply the default severity to all trap definitions listed in the Selected Traps table.

10. Click OK.

### Importing trap definitions from a MIB file

You can also import trap definitions from system or vendor MIBs.

To import trap definitions:

1. Copy the MIBs that contain trap definitions to
   IMC installation directory/client/TrapMIB

   Most MIBs have dependencies on other MIBs, most especially MIB2 or SNMP-v2-MIB and IF-MIB. These MIBs are compiled into IMC by default and should not be removed. There may also be other MIB dependencies that require you to compile them into IMC before you can compile the MIBs that contain the trap definitions you want to add. MIB definition files list their dependencies at the beginning of the MIB.

2. Navigate to Trap Definition.

3. Click the Alarm tab from the tabular navigation system on the top.

4. Click Trap Management on the navigation tree on the left.

5. Click 🗃 Trap Definition under Trap Management from the navigation tree on the left.

6. Click on the Import trap definition from MIB file link located to the far right of the Trap Definition list.

7. Click Compile.

8. Select the MIB file that contains the traps you want to import from the list of MIBs located below the Compile button.

   A dialog box is displayed that lists all of the traps in the selected MIB.

9. Click the checkbox to the left of the Trap Name you want to import.

10. Click Import.
The maximum number of MIBs that can be imported is 50.

**Syslog management**

Syslog is a standard for forwarding log messages over IP to devices configured to receive them. Entries in Syslog files are effective for monitoring failures in real time because devices write error conditions to Syslog files and most network infrastructure devices can be configured to forward Syslog entries to management systems such as IMC.

You can receive Syslog entries from managed devices and to review, filter, and generate alarms and notifications based on the Syslog entries received.

Syslog management is most effective when all devices in the network infrastructure are configured to forward Syslog messages to IMC and IMC is configured to manage all of the devices that are configured to forward Syslog messages to it. Syslog entries that IMC receives from unmanaged devices (by default) are filtered out.

To effectively use IMC as a Syslog server and a source for managing and displaying Syslog event information, you must first configure all devices to forward Syslog entries to IMC. Refer to each vendor’s support documentation for information on how to configure their devices to forward Syslog entries to a management system. Then, you must also add all devices (Syslog sources) to IMC. For more information on adding and managing devices in IMC, see "5 Resource management" (page 153). For information on the filtering out traps from unmanaged devices, see "Filtering traps with existing IMC Trap filter rules" (page 529) and "Modifying the unmanaged devices trap filter rule" (page 534).

**Syslog overview**

You have full visibility into all Syslog events received by IMC. With IMC, you can view all Syslog events from a single window.

From the Browse Syslog view, you can drill down to the Device Details view for the devices that generated the Syslog entry. The Device Details page provides access to monitor and manage the devices that generated the Syslog entry.

From the Device Syslog Detailed Information page, operators can view specific details about the Syslog entry.

From the Browse Syslog view, you can query the IMC logs for any Syslog entry using powerful search capabilities. You can also save those searches for future use and viewing.

**Browsing Syslog entries**

IMC provides a view that displays all Syslog events received by IMC. Through the Browse Syslog view, you can view all Syslog events received by IMC.

**Browsing Syslog entries**

To browse Syslog entries:

1. Navigate to Browse Syslog.
2. Click the Alarm tab from the tabular navigation system on the top.
3. Click Syslog Management on the navigation tree on the left.
4. Click Browse Syslog under Syslog Management from the navigation system on the left.
IMC displays all Syslog entries in the System Log List displayed in the main pane of the Browse Syslog window.

**Syslog List**
- **Level**: Contains the severity level for this Syslog entry as defined by the source of the event.
- **Syslog Source**: Contains the device name for the source of this Syslog entry. This field contains an active link that navigates to the Device Details page for the source device of this Syslog entry.
- **Device IP**: Contains the IP address for the source of this Syslog entry.
- **Description**: Contains a description of the condition on the source side that triggered this Syslog entry. This field contains an active link to the Device Syslog Detailed Information page.
- **Number of Repetitions**: Contains the number of duplicate Syslog events for the same condition.
- **Receive Time**: Contains the date and time stamp for this Syslog event.

You can sort the Syslog List by any field. Click the column label to sort the list by the selected field. The column label is a toggle switch that lets you toggle between the various sort options specific to each field.

1. Click to page forward in the Syslog List.
2. Click to page forward to the end of the Syslog List.
3. Click to page backward in the Syslog List.
4. Click to page backward to the front of the Syslog List.

5. Click 8, 15, 50, 100, or 200 from the right side of the main pane to configure how many items per page you want to view.

6. For lists that have more than one page, click on 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 ... from the bottom right side of the main pane to jump to a particular page of the list.

**To Export Syslog Entries**

You can export the first 2000 entries in the Syslog list.

To export Syslog entries:

1. Click Export as Excel link to the far right in the Syslog List.
2. Follow the instructions in the Syslog Data Download dialog boxes to complete the export of data to Excel.

**Querying Syslog entries in IMC**

IMC provides search capabilities for Syslog entries that can be accessed through the Browse Syslog page under the Alarm tab. There are two Syslog query methods in IMC, the Basic Query and the Advanced Query.

**Basic alarm query**

To query for Syslog entries using the Basic Query page:

1. Navigate to Browse Syslog.
2. Click the Alarm tab from the tabular navigation system on the top.
3. Click Syslog Management on the navigation tree on the left.
4. Click Browse Syslog under Syslog Management from the navigation system on the left.
The Query Syslog feature is displayed (by default) above the Syslog List. If the link to the far right is Advanced Query, then you are in Basic Query mode.

5. Enter your search criteria:
   - **Device IP**: lets you search for Syslog entries by a device’s IP address. Enter a partial or complete IP address for the node you want to view Syslog entries for in the Device IP field.
   - **Level**: lets you query for a specific Syslog severity level. Select this option from the Level list.
   - **Time**: lets you query for a time range in recently. Select this option from the Time list.

6. Click Query to begin you search. View the results of your query once the query has completed.

7. Click Reset to reset the query values. Re-enter your search criteria.

**Advanced alarm query**

To query for Syslog entries using the Advanced Query page:

1. Navigate to Browse Syslog.
2. Click the Alarm tab from the tabular navigation system on the top.
3. Click Syslog Management on the navigation tree on the left.
4. Click Browse Syslog under Syslog Management from the navigation system on the left.
   - The Query Syslog feature is displayed (by default) above the Syslog List. If the link to the far right is Advanced Query, then you are in the Easy Query mode.
5. To perform an advanced query, click on the Advanced Query link located to the far right of the Browse Syslog page.
6. Enter your search criteria in the Query Syslog window:
   - **Device IP**: Search for alarms by a device’s IP address. Enter a complete IP address for the node you want to view alarms for in the Device IP Field. Click Add after entering the IP address for every device you want to include in the query.
   - **Selected Devices**: Include in your query by clicking Select located to the right of the Selected Devices field. Select devices by using the By View or the Advanced options in the Select Devices dialog box.
   - **System Name**: Enter the name of the source device you want to find Syslog entries for.
   - **Module Name**: Enter the name of the source module that you want to find Syslog entries for.
   - **Digest Name**: Enter the name of the Syslog digest that you want to find Syslog entries for.
   - **Level**: Query for Syslog severity levels. Click the checkboxes to the left of the severity levels you want to search for.
   - **Receive Time**: Define the starting and ending date and time for your search.
   - **Description**: Enter a string to match against the contents of the description field of a Syslog entry.

7. Click Query to begin you search.
8. View the results of your query once the query has completed.
9. Click Reset to reset the query values.
10. Re-enter your search criteria.

**Syslog details**

The basic component of all Syslog browsing in IMC is the individual Syslog entry. Operators can view individual Syslog entries by clicking an individual entry in the Browse Syslog page.
The **Device Syslog Detailed Information** page provides information on a specific Syslog entry.

### To view device Syslog detailed information

To view the details for an individual Syslog entry:

1. Navigate to **Browse Syslog**.
2. Click the **Alarm** tab from the tabular navigation system on the top.
3. Click **Syslog Management** on the navigation tree on the left.
4. Click **Browse Syslog** under **Syslog Management**.
5. Click the link in the **Description** field in the **Syslog List** for the individual Syslog entry in which you want to view details for.

IMC displays all entries in the **Device Syslog Detailed Information** view displayed in the main pane of the **Browse Syslog**→**Detailed Information** window.

#### Device Syslog detailed information

- **System Name**: Contains the device name for the source of this Syslog entry.
- **Device IP**: Contains the IP address for the source of this Syslog entry.
- **Receive Time**: Contains the date and time stamp for this Syslog event.
- **Module Name**: Contains the name of the module from the source that generated this Syslog entry.
- **Level**: Contains the severity level for this Syslog entry as defined by the source of the event.
- **Repeat Time**: Contains the number of duplicate Syslog events for the same condition.
- **Description**: Contains a description of the condition on the source side that triggered this Syslog entry.

### Filtering Syslog entries

You can view system defined Syslog filtering rules.

#### Viewing Syslog filtering rules

To view Syslog filtering rules:

1. Navigate to **Filtering Syslog**.
2. Click the **Alarm** tab from the tabular navigation system on the top
3. Click **Syslog Management** on the navigation tree on the left.
4. Click **Filtering Syslog** under **Syslog Management** from the navigation system on the left.

#### Filtering Syslog list

- **Rule Name**: Contains the name of the Syslog filtering rule.
- **Rule Description**: Provides a brief description of the filtering performed by the rule.
- **State**: Provides current status of the functioning of the associated rule.
- Click **** to page forward in the **Filtering Syslog** list.
- Click **** to page forward to the end of the **Filtering Syslog** list.
- Click **** to page backward in the **Filtering Syslog** list.
- Click **** to page backward to the front of the **Filtering Syslog** list.
5. Click 8, 15, 50, 100, or 200 from the right side of the main pane to configure how many items per page you want to view.

6. For lists that have more than one page, click 1, 2, 3, 4, 5, 6, 7, 8, 9, or 10 … from the bottom right side of the main pane to jump to a particular page of the list.

Enabling/disabling Syslog filtering rules

To enable or disable Syslog filtering rules:
1. Navigate to Filtering Syslog.
2. Click the Alarm tab from the tabular navigation system on the top.
3. Click Syslog Management on the navigation tree on the left.
4. Click Filtering Syslog under Syslog Management from the navigation system on the left.
5. Do one of the following to enable or disable a Syslog filtering rule:
   - To enable a Syslog filtering rule, click on the disabled status link Disable in the State field for the target rule, or
   - To disable a Syslog filtering rule, click on the enabled status link Enable in the State field for the target rule.

Configuring alarms for Syslog messages

IMC relies on system and user defined rules to determine which of the Syslog events received by IMC generates alarms and the resolution of alarms. IMC includes many system defined rules that generate and resolve alarms based on Syslog events received by IMC. You can also create user defined rules that generate or resolve alarms based on Syslog events received by IMC.

IMC separates the identification of content in Syslog entries from the configuration of alarm generation and resolution rules. Syslog templates allow you to define the content that must exist in a Syslog entry to be escalated to an alarm or its resolution. Once created, the Syslog templates can then be applied to one or more alarm generation and resolution rules.

You can create both Syslog templates and Syslog alarm rules from scratch or they can be copied from existing system defined templates and rules and modified to meet your needs.

Using Syslog templates

Syslog templates are used by Syslog to Alarm rules to match Syslog template content against Syslog entries, which are used by the Syslog to Alarm rules to determine whether or not an alarm is generated. User defined Syslog templates must be created before the Syslog to Alarm rules that depend on them can be created.

You can view system defined Syslog templates. You can also create user defined Syslog templates or they can be copied from existing system defined templates.

Browsing Syslog templates

To view all Syslog templates:
1. Navigate to Syslog Template.
2. Click the Alarm tab from the tabular navigation system on the top.
3. Click Syslog Management on the navigation tree on the left.
4. Click Syslog Template under Syslog Management from the navigation system on the left.
Syslog Template page provides you with a list of all Syslog templates that are used in Syslog to alarm rules that generate alarms.

IMC displays all Syslog template entries in the Syslog Template List displayed in the main pane of the Syslog Template window.

Syslog template list

- **Template Name**: Contains the Syslog template name. Clicking the link in this field navigates you to the Syslog Template Details page that displays the details of this rule.
- **Template Content**: provides you with information on the contents of the Syslog template, including parameters and content to be matched.
- **Type**: identifies whether or not the associated Syslog template is system-defined or user-defined.
- **Modify**: provides you with a link for modifying the associated template. Only user-defined templates can be modified and therefore only user-defined templates have the Modify icon in this field.
- **Delete**: provides you with a link for deleting the associated template. Only user-defined templates can be deleted and therefore only user-defined templates have the Delete icon in this field.
- **Copy**: provides you with a link for copying an existing template to serve as a foundation for a user defined or operator defined template.

You can sort the Syslog Template List by the Template Name, Template Content, and Type fields. Click the column label to sort the list by the selected field. The column label is a toggle switch that lets you toggle between the various sort options specific to each field.

5. Click 8, 15, 50, 100, or 200 from the right side of the main pane to configure how many items per page you want to view.

   - Click ‼️ to page forward in the Syslog Template List.
   - Click ‌ to page forward to the end of the Syslog Template List.
   - Click   to page backward in the Syslog Template List.
   - Click ‌ to page backward to the front of the Syslog Template List.

6. For Syslog Template List with more than one page, click 1, 2, or 3 from the bottom right side of the main pane to jump to a particular page of the Syslog Template list.

Creating a user-defined Syslog template

To create a user defined Syslog template:

1. Navigate to Syslog Template.
2. Click the Alarm tab from the tabular navigation system on the top.
3. Click on Syslog Management on the navigation tree on the left.
4. Click ‼️ Syslog Template under Syslog Management from the navigation system on the left.
5. Click Add.
6. Enter a unique name for this Syslog template in the Name field.
   Valid length is 1-32 characters.
7. Enter the contents of the Syslog event that you want this template to search Syslog entries for in the Template Content field.
   Valid length is 1-512 characters.
Guidelines for the template content field

IMC supports the use of variables or parameters for matching dynamic content in Syslog entries. However, the use of variables or parameters in Syslog Templates is not required.

The template content to be matched can include an asterisk (*) as a wildcard. An asterisk represents one or more characters. You cannot, however, use asterisks to represent all of the content.

You cannot use the dollar sign ($) as content to be matched.

You can use variables or parameters to represent the content to be matched. Variables or parameters take the format of

\$(parameter-name)

For example,

Duplicate address \$(Duplicate IP) on \$(Source VLAN).

A parameter cannot include any of the following:

dollar sign ($), left parenthesis ((), right parenthesis ()), asterisk (*), left brace ({), right brace (}), left angle brackets (<), or right angle bracket (>).

Carriage returns and line feed characters are not allowed in a variable or parameter.

Content to be matched cannot include identical parameters.

At least one visible character must be placed between two parameters. This character cannot be an asterisk (*).

Spaces preceding or following a parameter are ignored. For example, the following two parameters are considered identical:

\$(parameter-name) and \$( parameter-name).

1. Enter a description for this template in the **Description** field.
   
   Valid length is 0-64 characters.

2. Click **OK**.

Modifying a user-defined Syslog template

To modify a user-defined Syslog template:

1. Navigate to **Syslog Template**.

2. Click the **Alarm** tab from the tabular navigation system on the top.

3. Click **Syslog Management** on the navigation tree on the left.

4. Click **Syslog Template** under **Syslog Management** from the navigation system on the left.

5. Click the **Modify** icon associated with the Syslog template you want to modify.

   You cannot modify the name of a Syslog template once it has been created.

6. Modify the contents of the Syslog event that you want this template to search Syslog entries for in the **Template Content** field.

Guidelines for the template content field

IMC supports the use of variables or parameters for matching dynamic content in Syslog entries. However, the use of variables or parameters in Syslog Templates is not required.
The template content to be matched can include an asterisk (*) as a wildcard. An asterisk represents for one or more characters. You cannot, however, use asterisks to represent the whole content.

You cannot use the dollar sign ($) as content to be matched.

You can use variables or parameters to represent the content to be matched. Variables or parameters take the format of

$(parameter-name)

For example,

Duplicate address $(Duplicate IP) on $(Source VLAN).

A parameter cannot include any of the following:

dollar sign ($), left parenthesis ((), right parenthesis ()), asterisk (*), left brace ({), right brace (}), left angle brackets (<), or right angle bracket (>).

Carriage returns and line feed characters are not allowed in a variable or parameter.

Content to be matched cannot include identical parameters.

At least one visible character must be placed between two parameters. This character cannot be an asterisk (*).

Spaces preceding or following a parameter are ignored. For example, the following two parameters are considered identical:

$(parameter-name) and $(parameter-name)

1. Modify the description for this template in the Description field.

2. Click OK.

Copying a Syslog template

The Copy feature for Syslog templates lets you create a new rule by making a copy of an existing system or user defined template and making whatever modifications are necessary to the copy. This feature lets you make changes to a system-defined template, as IMC does not allow modifications to system-defined templates.

To copy a system or user defined Syslog template:

1. Navigate to Syslog Template.

2. Click the Alarm tab from the tabular navigation system on the top.

3. Click Syslog Management on the navigation tree on the left.

4. Click Syslog Template under Syslog Management from the navigation tree on the left.

5. Click the Copy icon associated with the system or user defined Syslog template you want to copy.

6. Delete the existing name and enter a new name for the rule in the Name field of the Copy Syslog Template page.

7. Modify any of the Syslog Template settings as needed.

   For more information on modifying a Syslog template, see “Modifying a user-defined Syslog template” (page 560).

8. Click OK.

Deleting a user-defined Syslog template

To delete a user defined Syslog template:
1. Navigate to **Syslog Template**.
2. Click the **Alarm** tab from the tabular navigation system on the top.
3. Click **Syslog Management** on the navigation tree on the left.
4. Click **Syslog Template** under **Syslog Management** from the navigation tree on the left.
5. Click the **Delete** icon associated with the Syslog template you want to delete.
6. Click **OK** to confirm deletion of the Syslog template.

### Using Syslog to alarm rules

IMC uses system and user defined rules to determine which of the Syslog events received by IMC should be considered alarms. IMC includes system defined rules that, upon installation, generate alarms based on Syslog entries received by IMC.

You can also create user defined rules that generates alarms based on Syslog events received by IMC. You can create these from scratch or you can copy an existing system defined rule and modify it to meet your needs. You also have the ability to enable and disable system and user defined rules. The following section explores the use of Syslog to alarm rules.

#### Browsing Syslog to alarm rules

To view all Syslog to alarm rules:

1. Navigate to **Syslog to Alarm**.
2. Click the **Alarm** tab from the tabular navigation system on the top.
3. Click **Syslog Management** on the navigation tree on the left.
4. Click **Syslog to Alarm** under **Syslog Management** from the navigation system on the left.

IMC displays all Syslog to Alarm rule entries in the **Syslog to Alarm** Rule list displayed in the main pane of the **Syslog to Alarm** window.

#### Syslog to alarm rule list

- **Name**: Contains the Syslog-to-alarm rule name. Clicking on the link in this field navigates you to the **Rule Detailed Information** page that displays the details of this rule.
- **Type**: provides you with the creator of the rule system defined or operator (user) defined.
- **State**: provides you with a current status of the rule and the ability to enable or disable a rule.
- **Modify**: provides you with a link for modifying the associated rule.
- **Delete**: provides you with a link for deleting the associated rule.
- **Copy**: provides you with a link for copying an existing rule to serve as a foundation for a user defined or operator defined rule.

You can sort the **Syslog to Alarm** rule list by the **Name**, **Type**, and **State** fields. Click the column label to sort the list by the selected field. The column label is a toggle switch lets you toggle between the various sort options specific to each field.

5. Click **8, 15, 50, 100, or 200** from the right side of the main pane to configure how many items per page you want to view.

- Click **to page forward in the **Syslog to Alarm Rule List**. **
Creating a user-defined Syslog to alarm rule

To create a user defined Syslog to alarm rule:

1. Navigate to Syslog to Alarm.
2. Click the Alarm tab from the tabular navigation system on the top.
3. Click Syslog Management on the navigation tree on the left.
4. Click Syslog to Alarm under Syslog Management from the navigation tree on the left.
5. Click Add. The Add Rule page appears.
6. Enter a unique name in the Name field. Valid length is 1-32 characters.
7. Do one of the following:
   a. Click the radio button to the left of Disabled if you want this rule to be in a disabled state upon completion of rule creation, or
   b. Click the radio button to the left of Enabled if you want this rule to be in an enabled state upon completion of the rule.
8. Enter a description for this Syslog to Alarm rule in the Description field. Valid length is 0-128 characters.
9. Select the type of Syslog event to be processed by this rule from the Syslog Type list.
10. Select the Syslog levels of the events that is processed by this rule by clicking on the checkboxes to the left of the Syslog Level for each Syslog level you want to include in this rule definition.
   The Syslog level defined here refers to the level set within the Syslog event, not the severity or alarm level used by IMC to escalate alarms. The value you define here must match the Syslog level setting in the Syslog event for it to be processed by this rule.
   IMC lets you summarize duplicate Syslog entries that match the rule’s conditions. The method used for summarizing Syslog entries is set in the Statistic field. The two methods are: Network and Single Device.
11. Do one of the following to select the method for summarizing Syslog entries:
   a. Click the radio button to the left of Network if you want IMC to summarize matching Syslog entries for the entire network, or
   b. Click the radio button to the left of Single Device if you want IMC to summarize matching Syslog entries by device.
   IMC lets you configure how many times similar or duplicate Syslog entries are received before IMC escalates the entries to an alarm. This is determined by two variables: the Repeat Interval and the Repeat Times.
   Repeat Interval defines the window of time in seconds that IMC considers Syslog entries duplicate.
12. Enter the window of time in seconds in the Repeat Interval field. Valid range is 1–3600 seconds.
13. To select how many duplicate Syslog entries must be received before generating an alarm, enter the number of duplicate Syslog entries in the **Repeat Times** field.
   Valid range is 1–10,000.

14. Select the alarm level that IMC applies to all Syslog entries that match this rule from the **Alarm Level** list.

15. In the **Alarm Description** field, enter the string that matches some or all of the contents in the Syslog entry that must be matched for this rule to generate an alarm in IMC.
   Valid length is 0–128.

   The default value in the description field is %Syslog%. This value requires IMC to match the entire contents of the Syslog event. You can refine your matching and therefore what is escalated to an alarm by selecting a subset of the entire contents of the Syslog event. To do so, the string you define in the Alarm Description field must be a subset of what is defined in the Syslog template specified in the alarm generation rule.

   For Syslog events that point to a security issue, you can forward Syslog alarms to IMC’s Security Control Center (SCC).

16. Do one of the following to either forward or not forward Syslog events to SCC:
   - Click the radio button ☑ to the left of **Yes** in the **Forward to SCC** field, or
   - If you do not want to forward Syslog events to SCC, click the radio button ☐ to the left of **No** in the **Forward to SCC** field.

17. Select the Syslog template to apply to this rule by clicking **Select** located to the right of the **Syslog Template** field.

18. Select the Syslog template you want to use from the list of existing Syslog templates displayed in the **Select** dialog box.

19. Click the radio button ☑ to the left of the Syslog template you want to apply to this rule.

20. Verify that the Syslog template you selected appears in the **Syslog Template** field.

   If the Syslog template contains parameters, the **Add Rule** page updates to include a **Param Setting** section that lets you configure parameter settings for the template to match parameter values in the Syslog entry. IMC includes the following configuration options that determine how IMC counts Syslog entries:

   - **Count Type**: determines how IMC treats similar Syslog events with different parameter values.
   - **Summing Count**: if you want IMC to consider similar Syslog entries as one alarm without distinguishing between different parameter values.

21. Select **Summing Count** if you want IMC to consider similar Syslog entries as one alarm without distinguishing between different parameter values.

   Alarms are generated when the number of matched Syslog entries, regardless of parameter values, equals the number of Syslog entries configured in the **Repeated Times** field within the time configured in **Repeat Interval** window.

22. Select **Classifying Count** if you want IMC to consider similar Syslog entries with different parameter values as separate alarms.

   The Syslog entries with parameter values matching those configured in the **Param Value** fields is counted. When the number of Syslog entries with matched **Param Values** equals the number configured in the **Repeated Times** field within the time configured in the **Repeat Interval** window is escalated to an alarm.

   - **Count Parameter**: click the checkbox to the left of the parameter name under **Count Parameter** if you want IMC to match the value you define in the **Param Value** field to the right with the contents of each Syslog entry.
   - **Param Name**: Contains the parameter name that IMC uses to match against the contents of Syslog entries.
Param Value: Enter the value of the parameter that IMC uses to match against the contents of Syslog entries in the Param Value field.

**CAUTION:**
If you input ‘N/A’ in the Param Value field, or you uncheck the checkbox for Count Parameter, IMC evaluates Syslog entries by Count Type without evaluating the parameter values in the Syslog entries.

**Alarm recovery**

The following steps outline the configuration parameters for the alarm recovery or resolution configuration options for this rule.

1. If you want to associate a Syslog resolution event with the Syslog event identified in this rule, click the checkbox to the left of Alarm Recovery Rule.
2. Select the type of Syslog event that IMC uses to resolve the condition identified by this Syslog to alarm rule from the Syslog Type list.
3. Select the Syslog Levels of the events that is processed by this alarm recovery rule by clicking the checkboxes to the left of the Syslog Level.
4. Select the Syslog template to apply to this alarm recovery rule by clicking Select located to the right of the Syslog Template field in the Alarm Recovery Rule section of the Add Rule page.
5. Select the Syslog template you want to use from the list of existing Syslog templates displayed in the Select dialog box. Click the radio button to the left of the Syslog template you want to apply to this alarm recovery rule.
6. If the Syslog template contains variables or parameters, the Add Rule page updates to include a Recovery Alarm key Parameters field that lets you select one or more parameters. To add parameters to the alarm recovery or resolution rule:
   a. Click the right arrow key to add one parameter, or
   b. Click to add all parameters, or
   c. Click the left arrow key to remove one parameter, or
   d. Click to remove all parameters.

If your Syslog to Alarm rule requires a user-defined Syslog template, you must create that template before creating the Syslog to Admin rule.

8. Click OK.

**Modifying a user-defined Syslog to alarm rule**

To modify a user defined Syslog to alarm rule:

1. Navigate to Syslog to Alarm.
2. Click the Alarm tab from the tabular navigation system on the top.
3. Click Syslog Management on the navigation tree on the left.
4. Click Syslog to Alarm under Syslog Management from the navigation tree on the left.
5. Click the Modify icon associated with the Syslog to alarm rule you want to modify.
   You can only modify user defined Syslog to alarm rules. In addition, you cannot modify the name of a Syslog to alarm rule once the rule has been created.
6. Do one of the following:
Click the radio button ☐ to the left of Disabled if you want to disable this rule, or click the radio button ☐ to the left of Enabled to enable this rule.

7. Modify the description for this Syslog to Alarm rule. Valid length is 0-128 characters. The following steps outline the configuration parameters for the alarm generation aspects of this rule.

8. Select the type of Syslog event to be processed by this rule from the Syslog Type list.

9. Select the Syslog Levels of the events that is processed by this rule by clicking the checkboxes to the left of the Syslog Level.

10. Do one of the following:
    ○ Click the radio button ☐ to the left of Network if you want IMC to summarize matching Syslog entries for the entire network, or
    ○ Click the radio button ☐ to the left of Single Device if you want IMC to summarize matching Syslog entries by device.

Repeat Interval defines the window of time in seconds that Syslog entries can be considered duplicate.

11. Change the window of time value by entering a new value in seconds in the Repeat Interval field.

12. To modify how many duplicate Syslog entries must be received before generating an alarm, enter the new number of duplicate Syslog entries in the Repeat Times field.

13. Select the alarm level that IMC applies to all Syslog entries that match this rule from the Alarm Level list.

14. In the Alarm Description field, enter a new string that matches some or all of the content in the Syslog event description field that must be matched for this rule to generate an alarm in IMC.

15. Do one of the following:
    ○ If you want to forward alarms generated by this rule to SCC, click the radio button ☐ to the left of Yes in the Forward to SCC field, or
    ○ If you do not want to forward Syslog events to SCC, click the radio button ☐ to the left of No in the Forward to SCC field.

16. Modify the Syslog template to be used with this rule clicking Select located to the right of the Syslog Template field.

17. Select the Syslog template you want to use from the list of existing Syslog templates displayed in the Select dialog box.

18. Click the radio button ☐ to the left of the Syslog template you want to apply to this rule.
    If the Syslog template contains parameters, the Add Rule page updates to include a Param Setting section that lets you configure parameter settings for the template to match parameter values in the Syslog entry. IMC includes the following configuration options that determine how IMC counts Syslog entries:
    ○ Count Type: Determines how IMC treats similar Syslog events with different parameter values.
    ○ Summing Count: If you want IMC to consider similar Syslog entries as one alarm without distinguishing between different parameter values.

    Alarms is generated when the number of matched Syslog entries, regardless of parameter values, equals the number of Syslog entries configured in the Repeated Times field within the time configured in Repeat Interval window.

19. Select Classifying Count if you want IMC to consider similar Syslog entries with different parameter values as separate alarms.

    The Syslog entries with parameter values matching those configured in the Param Value fields is counted. When the number of Syslog entries with matched Param Values equals the number
configured in the **Repeated Times** field within the time configured in the **Repeat Interval** window is escalated to an alarm.

- **Count Parameter:** click the checkbox to the left of the parameter name under **Count Parameter** if you want IMC to match the value you define in the **Param Value** field to the right with the contents of each Syslog entry.
- **Param Name:** Contains the parameter name that IMC uses to match against the contents of Syslog entries.
- **Param Value:** Enter the value of the parameter that IMC uses to match against the contents of Syslog entries in the **Param Value** field.

⚠️ CAUTION:

If you input ‘N/A’ in the **Param Value** field, or you uncheck the checkbox for **Count Parameter**, IMC evaluates Syslog entries by **Count Type** without evaluating the parameter values in the Syslog entries.

The following steps outline the configuration parameters for the alarm recovery or resolution configuration for this rule.

21. If you want to modify the Syslog resolution event to the Syslog event identified in this rule, click the checkbox to the left of **Alarm Recovery Rule**.

22. Select the type of Syslog event that IMC uses to resolve the condition identified by this Syslog to Alarm rule from the **Syslog Type** list.

23. Select the Syslog Levels of the events that are processed by this alarm recovery rule by clicking the checkboxes to the left of the **Syslog Level**.

24. Select the Syslog template to apply to this alarm recovery rule by clicking **Select** located to the right of the **Syslog Template** field in the **Alarm Recovery Rule** section of the **Add Rule** page.

25. Select the Syslog template you want to use from the list of existing Syslog templates displayed in the **Select** dialog box. Click the radio button to the left of the Syslog template you want to apply to this alarm recovery rule.

If the Syslog template contains variables or parameters, the **Add Rule** page updates to include a **Recovery Alarm key Parameters** field that lets you select one or more parameters.

26. To add parameters to the alarm recovery or resolution rule, do one of the following:

- Click the right arrow key to add one parameter, or
- Click to add all parameters, or
- Click on the left arrow key to remove one parameter, or
- Click to remove all parameters.

27. Click **OK**.

### Copying a Syslog to alarm rule

To copy a system or user defined Syslog to alarm rule:

1. Navigate to **Syslog to Alarm**.
2. Click the **Alarm** tab from the tabular navigation system on the top.
3. Click **Syslog Management** on the navigation tree on the left.
4. Click ![Syslog to Alarm] under **Syslog Management** from the navigation tree on the left.
5. Click the **Copy** icon associated with the system or user defined Syslog to alarm rule you want to copy.
6. Delete the existing name and enter a new name for the rule in the **Name** field of the Copy Rule page.
7. Modify any of the Syslog to Alarm rule settings as needed.
   For more information on modifying a Syslog to Alarm rule, see "Modifying a user-defined Syslog to alarm rule" (page 565).
8. Click **OK**.

**Enabling/disabling Syslog to alarm rules**

To enable or disable **Syslog to Alarm** rules:
1. Navigate to **Syslog to Alarm**.
2. Click the **Alarm** tab from the tabular navigation system on the top.
3. Click **Syslog Management** on the navigation tree on the left.
4. Click **Syslog to Alarm** under **Syslog Management** from the navigation tree on the left.
5. Do one of the following:
   - To enable a **Syslog to Alarm** rule, click the disabled status icon **Disable** in the **State** field for the rule, or
   - To disable a **Syslog to Alarm** rule, click the enabled status icon **Enable** in the **State** field for the rule.

**Deleting a user-defined Syslog to alarm rule**

To modify a user defined Syslog to alarm rule:
1. Navigate to **Syslog to Alarm**.
2. Click the **Alarm** tab from the tabular navigation system on the top.
3. Click **Syslog Management** on the navigation tree on the left.
4. Click **Syslog to Alarm** under **Syslog Management** from the navigation tree on the left.
5. Click the **Delete** icon associated with the Syslog to alarm rule you want to delete.
6. Click **OK** to confirm deletion of the selected rule.

**Browsing alarms**

IMC provides full visibility into all alarms generated by IMC. IMC provides you with alarm views for **Real-Time Alarms** and **Root Alarms** and an **All Alarms** view.

The **Real Time Alarms** list provides you with a view of the last 50 unrecovered alarms in real time.

The **Root Alarms** list displays all unrecovered, root alarms although operators can modify the configuration of this list to included non-root alarms.

The **All Alarms** list provides you with a view of all alarms, root and symptom, recovered or cleared and unrecovered. From the **All Alarms** view, you can also query the alarm database through search capabilities and save those searches for future use.
All views of alarms offer drilldown capabilities to the device details for the devices that generated the event. The Device Details page provides access for monitoring and managing reporting errors for the selected device. From the Device Details page, you can also view the ten most recent alarms for the selected device.

All views of alarms also offer drilldown capabilities to the Alarm Details page, where you can view specific details about the alarm and take actions to recover, acknowledge, delete, annotate or report on alarms.

IMC also provides views of all faults or errors on the network through the Alarm Statistics charts and TopN views with the ability to create user defined Alarm Statistics charts.

Alarm details

The basic component of all alarm browsing in IMC is the individual alarm itself. You can view individual alarms through the Alarm Details page but you can only access this page through the three alarm browsing portals available in IMC: Real-Time Alarms, Root Alarms and All Alarms browsing. Before covering these alarm views, we provide an overview of the Alarm Details page.

The Alarm Details page provides you with information on a specific alarm and active links to related alarms and the Device Details page for details on the source device of the alarm. From this page, you can also perform actions on an alarm and access the Alarm Relations Report page.

Each of the three alarm views, Real-Time Alarms, Root Alarms, and All Alarms has different navigation paths to the Alarm Details page. The instructions below provide the steps for navigating to the Alarm Details page from and information on alarm actions and alarm reporting.

To view alarm details

To view alarm details:

1. Navigate to Alarm Browse.

2. Click the Alarm tab from the tabular navigation system on the top.

3. Click Alarm Browse on the navigation tree on the left.

To view alarm details from the real-time alarms page

1. Click 🔄 Real-Time Alarms under Alarm Browse from the navigation system on the left.

2. Click the link in the Description field in the Real-Time Unrecovered Alarms list for the alarm you want to view details for.

To view alarm details from the root alarms page

1. Click 🔄 Root Alarms under Alarm Browse from the navigation system on the left.

2. Click the link in the Information field in the Root Alarms list for the alarm you want to view details for.

To view alarm details from the all alarms page

1. Click 🔄 All Alarms under Alarm Browse from the navigation system on the left.

2. Click the link in the Description field in the Alarm List for the alarm in which you want to view details.

Alarm actions in the alarm details page

The Alarm Details page offers you the ability to take action on each alarm. To execute actions from the Alarm Details page:

1. Navigate to the Alarm Details page using the navigation steps provided in the previous section for the alarms page you want to use.

2. Locate the Action navigation tree located on the right of the Alarm Details page.
3. Click the ✅ Recover link to recover or clear the alarm. Recovering an alarm has the effect of clearing it in IMC.

When an alarm has been recovered, the selected alarm instance is considered resolved and removed from notification functions, though recovered alarms can still be viewed from the All Alarms view. Recovered alarms are removed from the alarms database according to the configuration for Data Export. For more information on the Data Export feature, see "Data export" (page 147).

There might be a time lag between the recovering or clearing of an alarm and its removal from IMC Alarm browsing views. Click Refresh to update the Alarm Browsing view.

4. Click the ⚠ Acknowledge link to acknowledge the alarm.

5. Click the ✗ Delete link to delete the alarm.

6. Click the 📊 Edit Maintenance Experience link to annotate the alarm with maintenance notes.

7. Enter your maintenance notes in the Maintenance Experience field in the Edit Maintenance Experience dialog box.

8. Click the 📉 Alarm Relation Report link to view the report for this alarm.

9. Click the ⬅ Back link to return to the previous page.

**Alarm relation report**

With the Alarm Relation Report, you can view and print to PDF a formatted report that includes the details for an individual alarm. In addition, you can export the data in the Alarm Relation Report to Microsoft Excel (XLS), Microsoft Word (DOC), Adobe Acrobat (PDF), Comma Separated Value (CSV), or Rich Text Format (RTF).

To view, print, and export Alarm Relation Reports

1. Click the 📉 Alarm Relation Report link located on the Action navigation tree on the right of the Alarm Details page.

   The Alarm Relation Report is displayed in the Intelligent Analysis Report Viewer window.

**Printing to PDF**

2. To print to PDF, click the Print icon 📑 located on the toolbar on the top of the Alarm Relation Report.

3. Select the desired page range from Page Range.

4. Click Export.

**Exporting alarm relation report data**

1. To export the alarm relation report, click the Export icon 📁 located on the toolbar on the top of the Alarm Relation Report.

2. Select the desired export file format from the File Format list.

   Options include Crystal Reports (RPT), Adobe Acrobat (PDF), Microsoft Excel (97-2003), Microsoft Excel (97-2003) Data Only, Microsoft Word (97-2003) – Editable, Rich Text Format (RTF), and Comma Separated Values (CSV).

3. Select the desired page range from Page Range.

4. Click Export.
Querying alarms in IMC

IMC provides search capabilities that are accessed through one or more of the alarm browsing views accessed under the **Alarm** tab. There are two alarm query methods in IMC, the **Basic Query** and the **Advanced Query**.

**Alarm basic query**

To query for alarms using the **Basic Query** method:
1. Navigate to **All Alarms**.
2. Click the **Alarm** tab from the tabular navigation system on the top.
3. Click **Alarm Browse** on the navigation tree on the left.
4. Click **All Alarms** under **Alarm Browse** from the navigation system on the left.

The **Basic Query** feature is displayed (by default) above the **All Alarms** list. If the link to the far right is **Advanced Query**, then you are in the **Basic Query** mode.

Enter your search criteria:
- **Time**: Query for alarms by time range. Select the range from the **Alarm Time** list.
- **Device Label/IP**: Search for alarms by a device’s label or IP address. This option supports fuzzy matching. Therefore, you can enter the entire label or IP address, or just a portion. Enter the device label or IP address of the node you want to view alarms for in the **Device Label/IP** field.
- **Alarm Level**: Query for a specific alarm or severity level. Select this option from the **Alarm Level** list.
- **Type**: Select the alarm source type: **Trap**, **Syslog**, or **IMC**. Select the option you want to query by from the **Type** list. If you want to search for alarms whose source are SNMP traps, select **trap**. If you want to search for alarms whose source is Syslog events, select **Syslog**. If you want to search for or filter the list for alarms that were generated by IMC itself, select **IMC**.
- **Recovery Status**: Choose the alarm status to query for **Recovered** or **Unrecovered**. Select this option from the **Recovery Status** list.
- **Acknowledgement Status**: Select alarms that have or have not been acknowledged by an operator. Select this option from the **Acknowledgement Status** list.

5. Click **Query** to begin your search.
6. View the results of your query once the query has completed.
7. Click **Reset** to reset both the query values and the search results.
8. Re-enter your search criteria.
9. Click **Save As** to save your query as a query view.

Once you have saved a query view, you can access it by clicking the expand button located to the left of the **All Alarms** link on the left navigation tree.

**Alarm advanced query**

To query for alarms using the **Advanced Query** method:
1. Navigate to **All Alarms**.
2. Click the **Alarm** tab from the tabular navigation system on the top.
3. Click **Alarm Browse** on the navigation tree on the left.
4. Click **All Alarms** under **Alarm Browse** from the navigation system on the left.
5. Click the **Advanced Query** link located to the right of the **All Alarms** list.
If this link says **Basic Query**, then you are in the **Advanced Query** mode.

**Enter your search criteria:**

- **Device IP**: Search for alarms by a device’s IP address. This option supports fuzzy matching. Therefore, you can enter the entire IP address or just a portion.

6. Enter the IP address of the node you want to view alarms for in the **Device IP** field.

7. Click **Add** after entering the IP address for every device you want to include in the query. The Selected Device field is updated to display the IP addresses you have added.

8. Select the devices you want to include in your query by clicking **Select** located to the right of the **Selected Devices** field.

9. Select devices by using the **By View** or the **Advanced** options in the **Select Devices** dialog box. See "Adding devices by View" (page 85) and "Adding devices by Advanced query" (page 85).

### Browsing real-time alarms

The **Real Time Alarms List** provides you with a view of the last 50 unrecovered alarms in real time. In addition, you can view the particular details of an individual alarm, take action on the selected alarm including recover, acknowledge, delete or annotate an alarm and print or export the individual alarm details.

#### Browsing real-time alarms

To browse real time alarms:

1. Navigate to **Real-Time Alarms**.
2. Click the **Alarm** tab from the tabular navigation system on the top.
3. Click **Alarm Browse** on the navigation tree on the left.

4. Click **Real-Time Alarms** under **Alarm Browse** from the navigation system on the left.

IMC displays fifty real-time unrecovered alarms in the **Real-Time Unrecovered Alarms** list displayed in the main pane of the **Real-Time Alarms** window.

#### Real-time unrecovered alarms List

- **Level**: Contains the alarm or severity level of the alarm. For more information on alarm or severity levels see "3 Exploring the IMC interface" (page 29).

- **Alarm Source**: Contains the name and or IP address of the device to which this alarm refers. Device names and device IP addresses that are grayed out indicate either that the alarm is generated by the IMC server or that the device is unmanaged.

This field contains an active link to navigate you to the **Device Details** page for the source of this alarm.

5. Click this link to navigate to details on the source device of this alarm.

- **Type**: Contains the source type of this alarm. The contents of this field identify whether the alarm was generated by a trap, by IMC, or by a Syslog entry.

- **Description**: Contains a description of the condition that triggered this alarm.

This field contains an active link to navigate you to the **Alarm Details** page for this alarm. The **Alarm Details** page provides more detailed information for each alarm. For more information on the **Alarm Details** page, see "Alarm details" (page 569).
This field also contains a link to the Crystal Reports Alarm Relation Report. For more information on this report, see "Alarm relation report" (page 570).

- **Alarm At**: Contains the date and time stamp for IMC’s receipt of this alarm.

6. Modify the refresh rate for this page by clicking the **Refresh Interval** list located in the upper right corner of the Real-Time Unrecovered Alarms view.

You can only view alarms for devices over which you have management access and control. In addition, you can recover, acknowledge or delete alarms for only those devices to which you have write access.

**To view alarm details from the real-time alarms page**

To view alarm details:

1. Navigate to **Alarm Details**.
2. Click the **Alarm** tab from the tabular navigation system on the top.
3. Click **Alarm Browse** on the navigation tree on the left.
4. Click **Real-Time Alarms** under **Alarm Browse** from the navigation system on the left.
5. Locate and click the link in the **Description** field in the Real-Time Unrecovered Alarms list for the alarm you want to view details for.

**Alarm actions in the alarm details page**

To take actions on the alarm in the Alarm Details page:

1. Locate the **Action** navigation tree located on the right of the Alarm Details page.
2. Click the **Recover** link to recover the alarm.
   
   Recovering an alarm has the effect of clearing it in IMC. When an alarm has been recovered, the selected alarm instance is removed from IMC browsing and notification functions. There may be a time lag between recovering or clearing an alarm and its removal from IMC Alarm browsing views. Click **Refresh** to update the Alarm Browsing view.
3. Click the **Acknowledgement** link to acknowledge the alarm.
4. Click the **Delete** link to delete the alarm.
5. Click the **Edit Maintenance Experience** link to annotate the alarm with maintenance notes.
6. Enter your maintenance notes in the **Maintenance Experience** field in the Edit Maintenance Experience dialog box.
7. Click the **Alarm Relation Report** link to view the report for this alarm.
8. Click the **Back** link to return to the previous page.

**Alarm relation report**

To view the **Alarm Relation Report**

1. Locate the **Action** navigation tree located on the right of the Alarm Details page.
2. Click the **Alarm Relation Report** link to view the report for this alarm.
3. With the **Alarm Relation Report**, you can view and print to PDF a formatted report that includes the details of individual alarms.

In addition, you can export the data in **Alarm Relation Reports** to Microsoft Excel (XLS), Microsoft Word (DOC), Adobe Acrobat (PDF), Comma Separated Value (CSV), or Rich Text Format (RTF).

**To print and export the Alarm Relation Reports**

1. Click the **Alarm Relation Report** link located on the **Action** navigation tree on the right of the **Alarm Details** page.
   
   The **Alarm Relation Report** is displayed in the **Intelligent Analysis Report Viewer** window.

2. Click the **Print** icon located on the toolbar on the top of the **Alarm Relation Report**.
3. Select the desired page range from **Page Range**.
4. Click **Export**.

5. To export the Alarm Relation report, click the **Export** icon located on the toolbar on the top of the **Alarm Relation Report**.

6. Select the desired export file format from the **File Format** list.

   Options include **Crystal Reports (RPT)**, **Adobe Acrobat (PDF)**, **Microsoft Excel (97-2003)**, **Microsoft Excel (97-2003) Data Only**, **Microsoft Word (97-2003) – Editable**, **Rich Text Format (RTF)**, and **Comma Separated Values (CSV)**.

7. Select the desired page range from **Page Range**.

8. Click **Export**.

**Recovering alarms from the real-time alarms page**

You can recover one or more alarms from the **Real-Time Unrecovered Alarms** list. Recovering an alarm has the effect of clearing it from the real-time view. When an alarm has been recovered, the selected alarm instance is considered resolved and removed from notification functions, though recovered alarms can still be viewed from the **All Alarms** view.

Recovered alarms are removed from the alarms database according to the configuration for **Data Export**. For more information on the **Data Export** feature, see "Data export" (page 147).

**To recover one or more alarms from the Real-Time Alarms page:**

1. Navigate to **Real-Time Alarms**.
2. Click the **Alarm** tab from the tabular navigation system on the top.
3. Click **Alarm Browse** on the navigation tree on the left.

4. Click **Real-Time Alarms** under **Alarm Browse** from the navigation system on the left.

5. Click the checkbox to the left of the real time alarms you want to recover.

6. Click the **Recover** button located in the upper left corner of the **Real-Time Unrecovered Alarms** window.

**Deleting alarms from the real-time alarms list**

Deleting alarms is one way of removing alarms from the alarms database. However, HP does not recommend this method because deleting an alarm removes the event from the alarm database and along with it the ability to report on it. Alarm histories are a valuable data source for performance management of the network infrastructure and this should be considered before deleting alarms.
Rather than deleting, you can recover an alarm. Recovering an alarm clears it from I alarm views while retaining it in the alarm database for a period of time. You can configure the data export function to export the Alarm database in order to keep a history of alarms. For more information on data exporting, see “Data export” (page 147).

To delete an alarm:
1. Navigate to **Real-Time Alarms**.
2. Click the **Alarm** tab from the tabular navigation system on the top.
3. Click **Alarm Browse** on the navigation tree on the left.
4. Click **Real-Time Alarms** under **Alarm Browse** from the navigation system on the left.
5. Click the checkbox to the left of the real time alarms you want to delete.
6. Click **Delete** located in the upper left corner or the **Real-Time Unrecovered Alarms** page.
7. Click **OK** when prompted to confirm deletion.

**Browsing root alarms**

The **Root Alarms** list displays all unrecovered, root alarms although you can modify the configuration of this list to include non-root alarms as well. Through this view, you can view all root alarms, take action, sort, and query from the **Root Alarms** view.

In addition, you can view the particular details of an individual alarm, take action on the selected alarm including recover, acknowledge, delete or annotate an alarm and print or export the individual alarm details.

**Browsing root alarms**

To browse root alarms:
1. Navigate to **Root Alarms**.
2. Click the **Alarm** tab from the tabular navigation system on the top.
3. Click **Alarm Browse** on the navigation tree on the left.
4. Click **Root Alarms** under **Alarm Browse** from the navigation system on the left.

**IMC** displays all root alarm entries in the **Root Alarms** list displayed in the main pane of the **Root Alarms** window.

**Root Alarms List**

- **Level**: Contains the Alarm or severity level of the alarm. For more information on Alarm or severity levels see “3 Exploring the IMC interface” (page 29).
- **Source**: Contains the name and or IP address of the device to which this alarm refers. This field contains an active link to navigate you to the **Device Details** page for the source of this alarm.

5. Click this link to navigate to details on the source device of this alarm.

Device names and device IP addresses that are grayed out indicate that the alarm is generated by the IMC server or an unmanaged device.

- **Type**: Contains the source type of this alarm. For example, if this alarm was generated by a trap, by IMC, or by a Syslog entry.
- **Information**: Contains a description of the condition that triggered this alarm.
This field contains an active link to navigate you to the Alarm Details page for this alarm. The Alarm Details page provides more detailed information for each alarm. For more information on the Alarm Details page, see “Alarm details” (page 569).

- **Time**: Contains the time stamp for IMC’s receipt of this alarm condition.
- **Root**: indicates whether or not the alarm is a root alarm or a symptom alarm. IMC can distinguish between an event that is a symptom of another error condition on the network versus an event that signifies the root error condition. The value “root” in the Root field indicates that the condition being alarmed on is a root error condition and not a symptom. The value “symptom” in the Root field indicates that the condition being alarmed on is the symptom of another error condition.

You can sort the Root Alarms list by any field. Click the column label. The down arrow key appears. Click the down arrow key to view a list of display options for the selected column. Display options include Sort Ascending and Sort Descending. You can also select which columns you want displayed by clicking the Columns field. You can also group the Root Alarms table by the selected field. You can disable and enable the group option.

From the list navigation bar at the bottom of the Root Alarms list:
- Click to page forward in the Root Alarms list.
- Click to page forward to the end of the Root Alarms list.
- Click to page backward in the Root Alarms list.
- Click to page backward to the front of the Root Alarms list.
- Click to refresh the Root Alarms list.

6. For lists that have more than one page, enter the page number in the field located the bottom left side of the main pane to jump to a particular page of the list.

The Root Alarms list summarizes alarms by date with the list displaying only the current day’s alarms.

7. To view alarms for previous days, scroll to the bottom of the current day’s list. You see a summarized entry for previous days.

8. Click the expand button to the left of the previous date to view alarms for that date. You can only view alarms for devices over which you have management access and control. In addition, you can recover, acknowledge or delete alarms for only those devices to which you have write access.

**To take actions from the root alarms page**

The Root Alarms page provides you with several actions that can be taken for alarms provided on this page. Actions that can be taken include recovering or clearing an alarm and its symptom alarms, acknowledging an alarm and its symptom alarms, deleting an alarm and its symptom alarms.

In addition, from the Root Alarms page, you can filter the current list to display root alarms only or all alarms. IMC also provides you with the ability to query the root alarms page to locate specific alarms. To take action on one or more alarms:

1. Navigate to Root Alarms.
2. Click the Alarm tab from the tabular navigation system on the top.
3. Click Alarm Browse on the navigation tree on the left.
4. Click Root Alarms under Alarm Browse from the navigation system on the left.
5. Click the checkbox to the left of the alarms for which you want to take action.
6. Locate the action toolbar located at the top of the Root Alarms list.

7. Click on the ✅ Recover link to recover the alarms. Using the down arrow key ⬇️ located to the right of ✅ Recover link, select the option you want to apply.

Recovering an alarm has the effect of clearing it from the view. When an alarm has been recovered, the selected alarm instance is considered resolved and removed from notification functions, though recovered alarms can still be viewed from the All Alarms view. Recovered alarms are removed from the alarms database according to the configuration for Data Export. For more information, “Data export” (page 147).

8. Select Recover selected alarms if you want this action to apply to only those alarms you have selected.

9. Select Recover selected alarms and their symptom alarms if you want this action to apply to the alarms you have selected and all alarms associated with this error condition.

There might be a time lag between the recovering or clearing of an alarm and its removal from IMC Alarm browsing views. Click on Refresh to update the Alarm Browsing view.

10. Click the 🔄 Ack link to acknowledge the selected alarms.

11. Select Acknowledge selected alarms if you want this action to apply to only those alarms you have selected.

12. Select Acknowledge selected alarms and their symptom alarms if you want this action to apply to the alarms you have selected and all alarms associated with this error condition.

13. Click the ❌ Delete link to delete the selected alarms.

14. Select Delete selected alarms if you want this action to apply to only those alarms you have selected.

15. Select Delete selected alarms and their symptom alarms if you want this action to apply to the alarms you have selected and all alarms associated with this error condition.

16. Click Show All Alarms/ Show Root Alarms Only to view all or a subset of all root alarms. This is a toggle switch whose appearance varies with the current selection.

17. Click Show All Alarms to view all root alarms and any associated or symptom alarms.

18. Click Show Root Alarms Only to view only the root alarms of an event or condition.

19. Click Query Condition to query the Root Alarms list for alarms based on your search criteria.

Query options include:

- **Alarm At**: Query for alarms by time range. Select the range from the Alarm At list.

- **Device IP**: Search for alarms by a device’s IP address. Enter the IP address of the node you want to view alarms for in the Device IP Field. This option supports fuzzy matching. Therefore, you can enter the entire IP address or just a portion. Enter the IP address of the node you want to view alarms for in the Device IP field.

- **Alarm Level**: Query for a specific alarm or severity level. Select this option from the Alarm Level list.

- **Alarm Type**: Select the alarm source type: Trap, Syslog, or IMC. Select this option from the Alarm Type list.

- **Recovery Status**: Choose the alarm status to query for: recovered or unrecovered. Select this option from the Recovery Status list.

- **Acknowledgement Status**: Select alarms that have or have not been acknowledged by an operator. Select this option from the Acknowledgement Status list.
20. Click OK.

To view alarm details from the root alarms page

To view alarm details from the Root Alarms page:
1. Navigate to Root Alarms.
2. Click the Alarm tab from the tabular navigation system on the top.
3. Click Alarm Browse on the navigation tree on the left.
4. Click Root Alarms under Alarm Browse from the navigation system on the left.
5. Locate and click the link in the Information field in the Root Alarms list for the alarm in which you want to view details.

Alarm actions in the alarm details page

To take actions on the alarm in the Alarm Details page:
1. Locate the Action navigation tree located on the right of the Alarm Details page.
2. Click the ✔ Recover link to recover the alarm.
   Recovering an alarm has the effect of clearing it in the root view. When an alarm has been recovered, the selected alarm instance is considered resolved and removed from notification functions, though recovered alarms can still be viewed from the All Alarms view. Recovered alarms are removed from the alarms database according to the configuration for Data Export. For more information, see “Data export” (page 147).
   There might be a time lag between the recovering or clearing of an alarm and its removal from IMC Alarm browsing views.
3. Click the ⚠ Acknowledge link to acknowledge the alarm.
4. Click the ✗ Delete link to delete the alarm.
5. Click the ✍ Edit Maintenance Experience link to annotate the alarm with maintenance notes. Enter your maintenance notes in the Maintenance Experience field in the Edit Maintenance Experience dialog box.
6. Click the 📊 Alarm Relation Report link to view the report for this alarm.
7. Click the Back link to return to the previous page.

Alarm relation report

To view the Alarm Relation Report:
1. Locate the Action navigation tree located on the right of the Alarm Details page.
2. Click the 📊 Alarm Relation Report link to view the report for this alarm.
   With the Alarm Relation Report, you can view and print to PDF a formatted report that includes the details of individual alarms. In addition, you can export the data in Alarm Relation Reports to XLS, DOC, PDF, CSV, or RTF.
3. Click the 📊 Alarm Relation Report link located on the Action navigation tree on the right of the Alarm Details page.
   The Alarm Relation Report is displayed in the Intelligent Analysis Report Viewer window.
Printing to PDF

1. Click the Print icon located on the toolbar on the top of the Alarm Relation Report.
2. Select the desired pages from Page Range.
3. Click Export.

Exporting alarm relation report data

1. Click on the Export icon located on the toolbar on the top of the Alarm Relation Report.
2. Select the desired export file format from the File Format list.
   - Options include Crystal Reports (RPT), Adobe Acrobat (PDF), Microsoft Excel (97-2003), Microsoft Excel (97-2003) Data Only, Microsoft Word (97-2003) – Editable, Rich Text Format (RTF), and Comma Separated Values (CSV).
3. Select the desired pages from Page Range.
4. Click Export.

Recovering alarms from the root alarms view

Operators can recover one or more alarms from the root alarms list. Recovering an alarm clears it from the root view. When an alarm has been recovered, the selected alarm instance is considered resolved and removed from notification functions, though recovered alarms can still be viewed from the All Alarms view. Recovered alarms are removed from the alarms database according to configuration for Data Export. For more information on the Data Export feature, see “Data export” (page 147).

To recover one or more alarms from the Root Alarms page:

1. Navigate to Root Alarms.
2. Click the Alarm tab from the tabular navigation system on the top.
3. Click Alarm Browse on the navigation tree on the left.
4. Click Root Alarms under Alarm Browse from the navigation system on the left.
5. Click the checkbox to the left of the alarms you want to recover.
6. Click Recover located in the upper left corner of the Root Alarms window.

IMC distinguishes between the root alarm that signifies the root cause of the alarm and the symptom alarms that arise as a result of the root alarm condition.

You can recover only the alarms you have selected or you can recover the alarms you selected and their symptom alarms. Highlight Recover selected alarms if you do not want to recover their symptom alarms. Highlight Recover selected alarms and their symptom alarms if you want to recover both.

Deleting alarms from the root alarms list

Deleting alarms is one way of removing alarms from the alarms database. However, HP does not recommend this method because deleting an alarm removes the event from the alarm database and along with it the ability to report on it. Alarm histories are valuable data source for performance management of the network infrastructure and this should be considered before deleting alarms.

Rather than deleting, you can recover an alarm. Recovering an alarm clears it from the Root Alarms list though recovered alarms can still be viewed in the All Alarms view. You can configure the IMC data export function to export the alarm database in order to keep a history of alarms. For more information on data exporting, see “Data export” (page 147).
To delete one or more alarms from the Root Alarms page:

1. Navigate to **Root Alarms**.
2. Click the **Alarm** tab from the tabular navigation system on the top.
3. Click **Alarm Browse** on the navigation tree on the left.
4. Click **Root Alarms** under **Alarm Browse** from the navigation system on the left.
5. Click on the checkbox to the left of the alarms you want to delete.
6. Click **Delete** located on the action toolbar located at the top of the **Root Alarms** page.

IMC distinguishes between the root alarm that signifies the root cause of the alarm and the symptom alarms that arise as a result of the root alarm condition.

You can delete only the alarms you have selected or you can delete the alarms you selected and their symptom alarms. Highlight **Delete selected alarms** if you do not want to delete their symptom alarms. Highlight **Delete selected alarms and their symptom alarms** if you want to delete both.

### Browsing all alarms

The **All Alarms List** provides a view of all alarms, root and symptom, recovered or cleared and unrecovered. From the **All Alarms** view, you can also query the alarm database through search capabilities and save those searches for future use.

In addition, you can view the particular details of an individual alarm, take action on the selected alarm including recover, acknowledge, delete or annotate an alarm and print or export the individual alarm details.

#### Browsing all alarms

To browse all alarms:

1. Navigate to **All Alarms**.
2. Click the **Alarm** tab from the tabular navigation system on the top.
3. Click **Alarm Browse** on the navigation tree on the left.
4. Click **All Alarms** under **Alarm Browse** from the navigation system on the left.

IMC displays all alarm entries in the **Alarm List** displayed in the main pane of the **All Alarms** window.

#### Alarm list

- **Level**: Contains the alarm or severity level of the alarm. For more information on alarm or severity levels, see "Exploring the IMC interface" (page 29).

- **Alarm Source**: Contains the name and or IP address of the device to which this alarm refers. Device names and device IP addresses that are grayed out indicate that the alarm is generated by the IMC server or an unmanaged device.

  This field contains an active link to navigate you to the **Device Details** page for the source of this alarm.

5. Click this link to navigate to details on the source device of this alarm.

- **Type**: Contains the source type of this alarm. In other words, was this alarm generated by a trap, by IMC, or by a Syslog entry.

- **Description**: Contains a description of the condition that triggered this alarm.
This field contains an active link to navigate you to the Alarm Details page for this alarm. The Alarm Details page provides more detailed information for each alarm. For more information on the Alarm Details page, see “Alarm details” (page 569).

This field also contains a link to the Crystal Reports Alarm Relation Report. For more information on this report, see "Alarm relation report" (page 570).

- **Recovery Status**: Contains information on whether or not the alarm is recovered or unrecovered.
- **Acknowledgement Status**: Contains information on whether or not the alarm has been acknowledged or not. If the alarm has been acknowledged, it contains the name of the operator who acknowledged the alarm.
- **Alarm At**: Contains the date and time stamp for IMC’s receipt of this alarm condition.
- **Recovered At**: Contains the date and time stamp for the recovery or clearing of this event.
- **Persisted Time**: Contains the duration of the error condition. Persisted time is measured as the amount of time that transpired since the receipt of the event that triggered an alarm and the resolution of the event.

You can sort the All Alarms list by the Type, Level, Alarm Source, Description, Recovery Status, Acknowledgement Status, Alarm at, and Recovered at fields. Click the column label to sort the list by the selected field. The column label is a toggle switch that lets you toggle between the various sort options specific to each field.

- Click to page forward in the All Alarms list.
- Click to page forward to the end of the All Alarms list.
- Click to page backward in the All Alarms list.
- Click to page backward to the front of the All Alarms list.

6. Click 8, 15, 50, 100, or 200 from the right side of the main pane to configure how many items per page you want to view.

7. For lists that have more than one page, click 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 from the upper middle of the main pane to jump to a particular page of the list. You can only view alarms for devices over which you have management access and control. In addition, you can recover, acknowledge or delete alarms for only those devices to which you have write access.

### Alarm actions in the all alarms page

To take actions on the alarm in the All Alarms list:

1. Locate the Action buttons at the top of the Alarm List page.

2. Select the alarms you want to take action on from the Alarm List by clicking the checkbox to the left of the alarm.

3. Click Recover to recover the selected alarms.

   There might be a time lag between the recovering or clearing of an alarm and its removal from IMC Alarm browsing views.

4. Click Acknowledge to acknowledge the selected alarms.

5. Click Delete to delete the selected alarms.
Alarm query in the all alarms page

The All Alarms page lets you search the IMC Alarms database. For more information on querying alarms in IMC, see "Browsing all alarms" (page 580).

To view alarm details from the all alarms page

To view alarm details:
1. Navigate to All Alarms.
2. Click the Alarm tab from the tabular navigation system on the top.
3. Click Alarm Browse on the navigation tree on the left.
4. Click All Alarms under Alarm Browse from the navigation system on the left.
5. Locate and click the link in the Description field in the All Alarms list for the alarm you want to view details for.

Alarm actions in the alarm details page

To take actions on the alarm in the Alarm Details page:
1. Locate the Action navigation tree on the right of the Alarm Details page.
2. Click the ✔ Recover link to recover the alarm.
   Recovering an alarm has the effect of clearing it from the view. When an alarm has been recovered, the selected alarm instance is considered resolved and removed from notification functions, though recovered alarms can still be viewed from the All Alarms view. Recovered alarms are removed from the alarms database according to configuration for Data Export. For more information on IMC’s Data Export feature, see "Data export" (page 147).
   There might be a time lag between the recovering or clearing of an alarm and its removal from IMC Alarm browsing views.
3. Click the ⚖ Acknowledge link to acknowledge the alarm.
4. Click the ✗ Delete link to delete the alarm.
5. Click the ☰ Edit Maintenance Experience link to annotate the alarm with maintenance notes. Enter your maintenance notes in the Maintenance Experience field in the Edit Maintenance Experience dialog box.
6. Click the ☰ Alarm Relation Report link to view the report for this alarm.
7. Click the ☰ Back link to return to the previous page.

Alarm relation report

To view the Alarm Relation Report:
1. Locate the Action navigation tree on the right of the Alarm Details page.
2. Click the ☰ Alarm Relation Report link to view the report for this alarm.
   With the Alarm Relation Report, IMC operators can view and print to PDF a formatted report that includes the details of individual alarms. In addition, operators can export the data in Alarm Relation XLS, DOC, PDF, CSV, or RTF.

Printing to PDF
1. Click the Print icon located on the toolbar on the top of the Alarm Relation Report.
2. Select the desired pages from Page Range.
3. Click Export.

Exporting alarm relation report data
1. Click the Export icon located on the toolbar on the top of the Alarm Relation Report.
2. Select the desired export file format from the File Format list.
   Options include Crystal Reports (RPT), Adobe Acrobat (PDF), Microsoft Excel (97-2003), Microsoft Excel (97-2003) Data Only, Microsoft Word (97-2003) – Editable, Rich Text Format (RTF), and Comma Separated Values (CSV).
3. Select the desired pages from Page Range.
4. Click Export.

Customizing the all alarms list columns
Operators can customize the All Alarms list to meet their individual alarm view needs.
1. Navigate to All Alarms.
2. Click the Alarm tab from the tabular navigation system on the top.
3. Click Alarm Browse on the navigation tree on the left.
4. Click All Alarms under Alarm Browse from the navigation system on the left.
5. Click the Custom the table columns link to the far right in the Alarm List. The Custom the table columns dialog box appears.
6. Uncheck the checkboxes to the left of the column name to remove specific columns from the All Alarms list.
7. Reorder the appearance of one or more columns in the list by using the Compositor icons located to the right of each column name:
   o Use to move the column to the leftmost position, or
   o Use to move the column one position to the left, or
   o Use to move the column one position to the right, or
   o Use to move the column to the rightmost position.
8. Click OK to save your changes.
9. Click Default to restore the All Alarms list to its default appearance.

Recovering alarms from the all alarms page
Operators can recover one or more alarms from the All Alarms list. Recovering an alarm has the effect of clearing it from the view. When an alarm has been recovered, the selected alarm instance is considered
resolved and removed from notification functions, though recovered alarms can still be viewed from the All Alarms view.

Recovered alarms are removed from the alarms database according to configuration for Data Export. For more information on IMC’s Data Export feature, see "Data export" (page 147).

To recover one or more alarms from the All Alarms page:

1. Navigate to All Alarms.
2. Click the Alarm tab from the tabular navigation system on the top.
3. Click Alarm Browse on the navigation tree on the left.
4. Click All Alarms under Alarm Browse from the navigation system on the left.
5. Click the checkbox to the left of the alarms you want to recover.
6. Click Recover located in the upper left corner of the All Alarms window.

Deleting alarms from the root alarms list

Deleting is one option for removing alarms from the IMC alarms database. However, HP does not recommend this option because deleting an alarm removes the event from IMC alarm database and along with it the ability to report on it.

Alarm histories are a very valuable data source for performance management of the network infrastructure and this should be considered before deleting alarms. Rather than deleting, you can recover an alarm. Recovering an alarm clears it from IMC alarm views while retaining it in the alarm database for a period of time. You can configure the IMC data export function to export the Alarm database in order to keep a history of alarms. For more information on data exporting, see "Data export" (page 147).

Deleting alarms from the all alarms page

To delete an alarm from the All Alarms list:

1. Navigate to All Alarms.
2. Click the Alarm tab from the tabular navigation system on the top.
3. Click Alarm Browse on the navigation tree on the left.
4. Click All Alarms under Alarm Browse from the navigation system on the left.
5. Click the checkbox to the left of the alarms you want to delete.
6. Click Delete located in the upper left corner of the All Alarms List page.
7. Click OK to confirm deletion of the selected alarms.

Exporting alarms from the all alarms page to Excel

IMC provides you with the ability to export alarms to Excel for further analysis. Using this feature, you can export 2,000 alarm entries from the All Alarms list.

To export all alarms from the All Alarms list to Excel:

1. Navigate to All Alarms.
2. Click the Alarm tab from the tabular navigation system on the top.
3. Click Alarm Browse on the navigation tree on the left.
4. Click All Alarms under Alarm Browse from the navigation system on the left.
5. Click the Export as Excel link to the far right in the Alarm List.
Follow the instructions in the **Download Exported Fault Data** dialog boxes to complete the export of data to Excel.

### Faulty devices

The **Faulty Devices** view offers you a graphical view of devices in the network infrastructure that are reporting errors. From this view, you can navigate to the device details page for quick access to devices that are reporting errors.

To access the **Faulty Devices** view:

1. Navigate to **Faulty Devices**.
2. Click the **Alarm** tab from the tabular navigation system on the top.
3. Click **Alarm Browse** on the navigation tree on the left.
4. Click **Faulty Devices** on the navigation tree on the left.

   To view updates to the **Faulty Devices** list, click **Refresh** located in the upper left corner of the page. IMC rechecks the alarms database and update the **Faulty Devices** list with updates.

Graphical icons and device names and IP addresses are displayed in the **Faulty Devices** list for those devices that are reporting errors. To view alarms for these devices, click on the icon or device name to drill down to the **Device Details** page. For more information on navigating the **Device Details** page, see "Device details page" (page 212).

Operators can only view devices that they have been granted management access to.

The color of a device icon in the **Faulty Devices List** represents the alarm or severity level for the most severe alarm condition for that device.

If a device’s most severe alarm condition is "Info", the device is not displayed in the Faulty Device list as these alarms are ignored.

### Alarm statistics

The **Alarm Statistics** view provides a summary of unrecovered alarm statistics. The statistical summaries offered in this view include alarms by application, configuration, security, performance, device, and a graph for all unrecovered alarms.

In addition, the **Alarm Statistics** view offers drilldown capabilities from the summary reports to the **All Alarms** list and the powerful search capabilities of the **All Alarms** page.

#### Viewing alarm statistics charts

To view the **Alarm Statistics** page:

1. Navigate to **Alarm Statistics**.
2. Click the **Alarm** tab from the tabular navigation system on the top.
3. Click **Alarm Browse** on the navigation tree on the left.
4. Click **Alarm Statistics** under **Alarm Browse** on the navigation tree on the left. The **Alarm Statistics** page appears.

The **Alarm Statistics** page summarizes alarms by category with active links embedded in the summary charts.

5. To view the individual alarms that underlie the summary charts, click the summary chart.
6. To view more details about the statistical breakdown by alarm category, click the active chart titles located at the top of each summary chart.

7. Click on **Refresh** to refresh the **Alarm Statistics** charts.

**Creating user-defined alarm statistics charts**

To add your own statistical charts to the **Alarm Statistics** page:

1. Navigate to **Alarm Statistics**.
2. Click the **Alarm** tab from the tabular navigation system on the top.
3. Click **Alarm Browse** on the navigation tree on the left.
4. Click **Alarm Statistics** under **Alarm Browse** on the navigation tree on the left.
   
   The **Alarm Statistics** page appears.
5. Click the **Add Alarm Stat** link located to the far right of the **Alarm Statistics** window.
6. Enter a name for this chart in the **Statistics Name** field.
7. Click **Select** under **Select Alarm Category** to choose the alarm categories you want to create a summary **Alarm Statistics** chart for.
8. Click the checkbox ☑ to the left of the **Main Category** names to add that category to your chart.
9. Click **OK**.
10. Select the devices you want to include in this **Alarm Statistics** chart.
11. Click the checkbox ☑ to the left of **All Devices** if you want this chart to summarize alarms for all devices in IMC.
12. Click **Select** if you want specify which devices or groups of devices you want to summarize alarms for in this chart.
13. Select the devices you want to add by using the add **By View** or by **Advanced** query functions in the **Select Devices** dialog box.
   
   See "Adding devices by View" (page 85) and "Adding devices by Advanced query" (page 85).
14. Click **OK** when you have completed your selection of devices.
   
   The user defined **Alarm Statistics** chart you have created appears in the **Alarm Statistics** page.
15. To modify the user defined **Alarm Statistics** chart you have created, click the **Modify** icon located in the upper right corner of the chart.
16. Modify any parameters as needed.
17. Click **OK**.
18. To delete a user defined Alarm Statistics chart you have created, click the **Delete** icon located in the upper right corner of the chart.
19. Click **OK** to confirm deletion of the user defined chart you have created.

**TopN**

The **TopN** view offers you a view of devices in the network infrastructure that are reporting the highest number of errors by the alarm or severity level. From this view, you can quickly navigate to the device details page for those devices that are reporting the most errors. Operators can also configure how many devices to include in the **TopN** view.
To access the TopN view:
1. Navigate to TopN.
2. Click the Alarm tab from the tabular navigation system on the top.
3. Click Alarm Browse on the navigation tree on the left.
4. Click 📢 TopN under Alarm Browse on the navigation tree on the left.
5. To adjust the number of devices included in the TopN view, select the number from the TopN list located in the upper right corner of the TopN page.
6. Click on Refresh to refresh the contents of the TopN page.
7. Device names and IP addresses are displayed in the subsections of the TopN list for those devices that are reporting the highest number of errors for each severity or alarm level. To view alarms for these devices, click the device name to drill down to the Device Details page. For more information on navigating the Device Details page, see "Device details page" (page 212).

Configuring alarm notifications

IMC supports the ability to send notifications for alarms and can be configured to:
- Send notifications by email or text messaging to designated recipients
- Forward alarms to other management systems such as help desk systems for proactive escalation of alarms generated by IMC.
- Forward alarms to other IMC instances in a distributed architecture for centralized alarm viewing and notification.
- Manage the number of alarms generated, directly affecting how IMC escalates root alarms through its configuration of relationship to network devices.

Managing email alarm notifications

IMC provides extensive control and flexibility over the management of alarms it generates. You can:
- Set alarms to trigger email and SMS text message notifications to recipients defined by the administrator.
- Forward alarms to other management systems.
- Configure times of the day and days of the week that notifications are sent or forwarded to other management systems.
- Configure which alarm types generate notifications or forwarding to other management systems.
- Configure which devices trigger email, SMS messaging, or alarm forwarding to other management systems when an alarm condition occurs.
- Configure which severity or alarm levels trigger email, SMS messaging notification or alarm forwarding to another management system.

All of these alarm configuration options can be combined into one or more alarm notification rules, providing the ability to customize IMC to meet organizational alarm notification needs.

Adding an email alarm notification rule

To add an email alarm notification:
1. Navigate to Alarm Notification.
   a. Click the Alarm tab from the tabular navigation system on the top.
b. Click **Alarm Settings** on the navigation tree on the left.

   c. Click **Alarm Notification** under **Alarm Settings** from the navigation tree on the left.

2. Click **Add** under **Mail Notification** in the main pane.

3. Enter a name for this mail alarm notification rule in the **Rule Name** field.
   Once you create a rule, you cannot modify its name.

4. Enter the destination mail address of the recipient for mail notifications for this rule in the **Destination Mail Address** field.

5. Do one of the following:
   - Click **Add**, or
   - Add multiple recipients by clicking **Add** after entering the destination mail addresses for each recipient in the **Destination Mail Address** field.

6. Do one of the following:
   - Click the checkbox ☑️ to the left of the alarm level you want to apply to this mail notification rule next to **Concerned Alarm Levels**, or
   - To remove an alarm level setting, click the checked box ☑️ next to each of the severity or alarm levels you want to exclude for this alarm rule.

   This configuration parameter determines which severity or alarm levels trigger a notification.
   For new alarm notification rules, all alarm levels with the exception of **Info** are checked.

7. Select **All Devices** or **Selected Devices** from the **Concerned Devices** list.
   - **All Devices**: With this option, all devices in IMC trigger a mail notification if the alarm condition meets the rule’s **Alarm Level** setting.
     For example, if you set the alarm level to critical and major, then all devices in the network infrastructure that have a condition that is configured in IMC as a critical or major alarm generate a mail notification to all recipients configured in this rule.
   - **Selected Devices**: With this option, only the selected devices trigger an email notification if the alarm condition meets the rule’s **Alarm Level** setting.
     You can select devices by **Device IP address**, by **Custom Views**, by **Network Segment** or by a combination of the three.

Selecting devices by IP address

a. Enter the IP address for the device you want to send email notifications for in the **Device IP** field.

b. Click **Add**.

c. Add multiple devices by clicking **Add** after entering the IP address in the **Device IP** field for each device you want to add.

Selecting devices by custom view

a. Expand the **Selected Custom View** section of the **Add Mail Notification** dialog box by clicking the **Expand** icon ☰️ located at the far right of **Selected Custom View**.

b. Select the custom view from the list.

   c. Click **Add**.
d. Add multiple device groups by custom views by clicking Add after selecting one custom view from the Custom View list.

Selecting devices by network segment

a. Expand the Selected Network Segment section of the Add Mail Notification page by clicking the Expand icon located at the far right of Selected Network Segment.
b. Enter the IP address range for the range of devices that you want to send email notifications for, by entering the first IP address in the range in the Start IP field and the last IP address in the End IP field.
c. Click Add.
d. Add multiple network segment groups by clicking Add after entering the IP address range in the Start IP and End IP fields.

You can add devices by using either the View or Advanced query option. For example, you can enter the IP address of one device, an IP address range, and groups defined by custom view. The alarm notification rule sends email notifications for all devices or groups of devices configured in the rule.

See "Adding devices by View" (page 85) and "Adding devices by Advanced query" (page 85).

2. Select All Alarms or Selected Alarms from the Concerned Alarms list.

This option allows you to configure which error conditions trigger mail notifications.

- All Alarms: With this option, all alarms configured in IMC trigger an email notification to be sent if the alarm condition is triggered.
- Selected Alarms: With this option, only the alarms you select in alarm notification trigger an email notification if the alarm condition is triggered. Further, if you choose Selected Alarms, you can select which alarm conditions generate email notifications.

3. To configure which conditions to send notifications for:

a. Click Select located to the right of the Concerned Alarms field. The Select Alarm dialog box appears.

b. In the Select Alarm dialog box, locate the Enterprise MIB that contains an object or condition that you want to alarm on.

c. To expand your view of the MIB, click on the arrow key next to the MIB that contains an object or condition that you want to alarm on.

d. Click the Expand all icon located in the upper right corner of the Select Alarm dialog box to expand your view to display all MIBs, or

Use the query function located at the top of the Select Alarm dialog box to locate the object that you want alarm on.

4. Enter one or more of the following search criteria:

- Trap Name: Enter the object name for the trap you want to locate in the Trap Name field.
- Trap OID: Enter the Object ID for the trap in the Trap OID field.
- Enterprise Name: Enter a partial or complete name for the Enterprise MIB you want to locate in the Enterprise Name field.
- Enterprise OID: Enter a partial or complete Enterprise ID for the MIB you want to locate in the Enterprise OID field.

5. Do one of the following:

- Click Query to submit your search criteria, or
6. Click the checkbox to select a MIB object that you want to alarm on.
7. Click OK.

It may take a while for the Select Alarm dialog box to close. When the box closes, it updates the Concerned Alarms field with the configured object or alarm condition.

You can click on multiple checkboxes to select multiple objects or conditions to alarm on. Each alarm condition is listed in the Concerned Alarms field below the list.
8. Click Parameter Setting located to the right of the Concerned Alarm field, the Set Alarm Parameter dialog box appears with all alarms with parameters listed.
9. Click the trap name to expand the alarm parameters.
10. Input the value in the field right of the parameters name:
    a. To set multiple values for a parameter, click the icon to add a line, or
    b. To remove a line, click the icon, or
    c. To restore a parameter that you have removed, enter the Set Alarm Parameter page again.
11. Click OK.

IMC determines whether to forward the received alarms according to the configured parameters.
12. To delete one or more alarm conditions, highlight the condition(s) and click Delete.

Not all alarms have parameters.

When you select multiple MIB objects or alarm conditions, the alarm conditions are evaluated and performed as an OR operation. With OR operations, only one of the conditions that you select must be true for the alarm notification rule to generate an email notification.

13. Confirm that the MIB objects or conditions you selected have populated the Concerned Alarms field in the Add Mail Notification page.

If IMC does not have the vendor’s MIBs you want to send email notifications, you can add them and then add a mail notification rule. For adding a MIB to IMC, see "MIB management" (page 138).
14. Enter the hourly range in the Time Ranges field for each day of the week, using an hh:mm-hh:mm format.

To exclude a day of the week, delete any values, including 00:00, from the hourly range for that day.
15. Click OK.

You must configure IMC to forward email notifications to the SMTP server in your environment for recipients to receive email alarm notifications. For information on configuring IMC to forward emails to your SMTP server, see "Mail server settings" (page 135).

Modifying an email alarm notification rule

To modify an email alarm notification:
1. Navigate to Alarm Notification:
   a. Click the Alarm tab from the tabular navigation system on the top.
   b. Click Alarm Settings on the navigation tree on the left.
   c. Click Alarm Notification under Alarm Settings from the navigation tree on the left.
2. Click the Modify icon in the Alarm Notification main pane associated with the mail notification rule you want to modify.

You cannot modify the name of an alarm rule once you have created it.

3. Add or remove email addresses as needed in the Destination Mail Address field.

4. Do one of the following:
   - Click Add after adding a valid email address, or
   - To add multiple recipients, click Add after entering each email address in the Destination Mail Address field, or
   - To delete one or more email recipients, highlight the recipient(s) you want to delete and click Delete.

5. Do one of the following:
   - Click the checkbox next to each of the severity or alarm levels next to the Concerned Alarm Levels you want to add for this alarm rule, or
   - Click the checked box next the alarm level you want to remove.

6. Select All Devices or Selected Devices from the Concerned Devices list.
   - All Devices: If you select this option after initially configuring this option with Selected Devices, then IMC overrides the existing configuration by configuring the alarm rule to send to all devices.
   - Selected Devices: With this option, only the selected devices trigger an email notification if the alarm condition meets the rule's Alarm Level setting.

You can modify your selection of devices by Device IP address, by Custom Views, by Network Segment or by a combination of the three.

For more information, see "Selecting devices by IP address" (page 588), "Selecting devices by custom view" (page 588), or "Selecting devices by network segment" (589).

You can also select devices by using the Select button located to the right of the Device IP field. This enables you to use IMC's display and search capabilities to select the device(s) from established groups and views either By View or by query using the Advanced feature. See "Adding devices by View" (page 85) and "Adding devices by Advanced query" (page 85).

7. Modify which error conditions trigger mail notifications from the Concerned Alarms list. Operators can select all conditions or only a specified subset of conditions that trigger alarms.
   - All Alarms: With this option, all alarms configured in IMC trigger an email notification to be sent if the alarm condition is triggered.
   - Selected Alarms: With this option, only the alarms you select in alarm notification generate an email notification if the alarm condition is triggered. Further, if you choose Selected Alarms, you can select which alarm conditions generate email alarm notifications.

8. To configure which conditions to send notifications for:
   a. Click Select located to the right of the Concerned Alarms field. The Select Alarm dialog box appears.
   b. In the Select Alarm dialog box, locate the Enterprise MIB that contains an object or condition that you want to alarm on, or
9. To expand your view of the MIB, click the arrow key \( \uparrow \) next to the MIB that contains an object or condition that you want to alarm on, or click the **Expand all** icon \( \rightarrow \) located in the upper right corner of the **Select Alarm** dialog box to expand your view to display all MIB.

10. You can also use the query function located at the top of the **Select Alarm** dialog box to locate the object that you want alarm on by entering one or more of the following search criteria:
   - **Trap Name**: Enter the object name for the trap you want to locate in the **Trap Name** field.
   - **Trap OID**: Enter the Object ID for the trap in the **Trap OID** field.
   - **Enterprise Name**: Enter a partial or complete name for the Enterprise MIB you want to locate in the **Enterprise Name** field.
   - **Enterprise OID**: Enter a partial or complete Enterprise ID for the MIB you want to locate in the **Enterprise OID** field.

11. Do one of the following:
   - Click **Query** to submit your search criteria. The results of your query display in the dialog box, or
   - Click **Reset** to clear your query criteria and to restore the full list of MIBs and traps, or
   - Click the checkbox \( \square \) to select a MIB object that you want to add to this alarm rule, or
   - Scroll down to the bottom of the MIB list and click **OK**.

   It may take a while for the **Select Alarm** dialog box to close. When the box closes, it updates the **Concerned Alarms** field with the configured object or alarm condition.

   You can click multiple checkboxes to select multiple objects or conditions to alarm on. Each alarm condition is listed in the **Concerned Alarms** field below the list.

12. Click **Parameter Setting** located to the right of the **Concerned Alarm** field and to set the parameters for the Concerned Alarms. The **Set Alarm Parameter** dialog box appears.

   All alarms that have parameters appear.

13. Click the trap name to expand the alarm parameters.

14. Input the value in the field right of the parameters name:
   - To set multiple values for a parameter, click the icon \( \rightarrow \) to add a line, or
   - To remove a line, click the icon \( \times \), or
   - To restore a parameter that you have removed, enter the **Set Alarm Parameter** page again.

15. Click **OK**.

   IMC determines whether to forward the received alarms according to the configured parameters.

16. To delete one or more alarm conditions, highlight the condition(s) and click **Delete**.

   Not all alarms have parameters.

   When you select multiple MIB objects or alarm conditions, the alarm conditions are evaluated and performed as an OR operation. With OR operations, only one of the conditions that you select must be true for the alarm notification rule to generate an email notification.

17. Confirm that the MIB objects or conditions you selected have populated the **Concerned Alarms** field in the **Add Mail Notification** page.

18. Enter the hourly range in the **Time Ranges** field for each day of the week, using an hh:mm-hh:mm format.

   To exclude a day of the week, delete any values, including 00:00, from the hourly range for that day.
19. Click OK.

Copying an email alarm notification rule

To copy an email alarm notification rule:
1. Navigate to Alarm Notification:
   a. Click the Alarm tab from the tabular navigation system on the top.
   b. Click Alarm Settings on the navigation tree on the left.
   c. Click Alarm Notification under Alarm Settings from the navigation tree on the left.
2. Click the Copy icon in the Mail Notification list associated with the alarm rule you want to copy.
3. Rename the rule by giving it a unique name.
4. Make any necessary modifications to the rule in the Copy Mail Notification page. For more information on modifying a mail Notification, see "Modifying an email alarm notification rule" (page 590).
5. Click OK.

Enabling/disabling an email alarm notification rule

To enable or disable an email alarm notification rule:
1. Navigate to Alarm Notification.
   a. Click the Alarm tab from the tabular navigation system on the top.
   b. Click Alarm Settings on the navigation tree on the left.
   c. Click Alarm Notification under Alarm Settings from the navigation tree on the left.
2. Do one of the following:
   o To enable, click the disabled status icon Disable in the Mail Notification Status field associated with the email rule you want to enable, or
   o To disable, click the enabled status icon Enable in the Mail Notification Status field associated with the email rule you want to disable.

Deleting an email alarm notification rule

To delete an email alarm notification rule:
1. Navigate to Alarm Notification.
   a. Click the Alarm tab from the tabular navigation system on the top.
   b. Click Alarm Settings on the navigation tree on the left.
   c. Click Alarm Notification under Alarm Settings from the navigation tree on the left.
2. Click the Delete icon in the Mail Notification list associated with the alarm rule you want to delete.
3. Click OK to confirm deletion of the rule.
Managing SMS alarm notifications

You can configure alarm notifications, which are implemented by notification rules, to be sent by SMS (text messaging) to devices configured to receive them.

You can configure one or more rules that define who receives SMS notifications for faults or errors and their resolution in the network infrastructure that are specified by the IMC administrator. In addition, you can configure which device(s) or groups of devices, which error condition, which alarm or severity levels generate SMS notifications.

Adding an SMS messaging alarm notification rule

To add an SMS message alarm notification:

1. Navigate to **Alarm Notification**:
   a. Click the **Alarm** tab from the tabular navigation system on the top.
   b. Click **Alarm Settings** on the navigation tree on the left.
   c. Click **Alarm Notification** under **Alarm Settings** from the navigation tree on the left.

2. Click **Add** under **Message Notification** in the main pane.

3. Enter a name for this SMS message notification rule in the **Rule Name** field.
   Once you create a rule, you cannot modify its name.
   - Enter the telephone number, including country code and area code if needed of the recipient for SMS notifications for this rule in the **Telephone Number** field, and click **Add**, or
   - Add multiple recipients by clicking **Add** button after entering the phone numbers for all recipients in the **Telephone Number** field.
   Only digits (0,1,2,3,4,5,6,7,8,9), parentheses (()), plus sign (+), hyphen (-), and spaces ( ) are permitted in the **Telephone Number** field.

4. Click the checkbox to the left of the alarm level you want to apply to this SMS message notification rule next to **Concerned Alarm Levels**.
   This configuration parameter determines which severity or alarm levels trigger a notification. For new notification rules, all alarm levels are checked with the exception of **Info**.

5. To remove an alarm level setting, click the checked box next to each of the severity or alarm levels you want to exclude for this alarm rule.

6. Select **All Devices** or **Selected Devices** from the **Concerned Devices** list.
   - **All Devices**: If you select this option after initially configuring this option with **Selected Devices**, then IMC overrides the existing configuration by configuring the alarm rule to send to all devices.
   - **Selected Devices**: With this option, only the selected devices trigger an email notification if the alarm condition meets the rule’s **Alarm Level** setting.

You can select devices by **Device IP** address, by **Custom Views**, by **Network Segment** or by a combination of the three. For more information, see “Selecting devices by IP address” (page 588), “Selecting devices by custom view” (page 588), or “Selecting devices by network segment” (589).

7. Select devices by using either the View or Advanced query option.
   For example, you can enter the IP address of one device, an IP address Range, and groups defined by custom view. The alarm notification rule forwards alarms for all devices or groups of devices configured in the rule.
See "Adding devices by View" (page 85) and "Adding devices by Advanced query" (page 85).

8. Select All Alarms or Selected Alarms from the Concerned Alarms list, allowing you to configure which error conditions trigger SMS message notifications.
   - **All Alarms**: With this option, all alarms configured in IMC generate a SMS Message notification to be sent if the alarm condition is triggered.
   - **Selected Alarms**: With this option, only the alarms you select in alarm notification trigger a SMS Message notification if the alarm condition is triggered. Further, if you choose Selected Alarms, you can select which alarm conditions generate SMS Message notifications.

9. To configure which conditions to send notifications for:
   a. Click **Select** located to the right of the Concerned Alarms field. The Select Alarm dialog box appears.
   b. In the Select Alarm dialog box, locate the Enterprise MIB that contains an object or condition that you want to alarm on.
   c. To expand your view of the MIB, click on the arrow key next to the MIB that contains an object or condition that you want to alarm on.
   d. Click the Expand all icon located in the upper right corner of the Select Alarm dialog box to expand your view to display all MIBs, or
      Use the query function located at the top of the Select Alarm dialog box to locate the object that you want alarm on.

10. Enter one or more of the following search criteria:
    o **Trap Name**: Enter the object name for the trap you want to locate in the Trap Name field.
    o **Trap OID**: Enter the Object ID for the trap in the Trap OID field.
    o **Enterprise Name**: Enter a partial or complete name for the Enterprise MIB you want to locate in the Enterprise Name field.
    o **Enterprise OID**: Enter a partial or complete Enterprise ID for the MIB you want to locate in the Enterprise OID field.

11. Click **Query** to submit your search criteria. The results of your query display in the dialog box.
    Optional: Click **Reset** to clear your query criteria and to restore the full list of MIBs and traps.

12. Click the checkbox to select a MIB object that you want to alarm on.
13. Click **OK**.
    It may take a while for the Select Alarm dialog box to close. When the box closes, it updates the Concerned Alarms field with the configured object or alarm condition.
    You can click on multiple checkboxes to select multiple objects or conditions to alarm on. Each alarm condition will be listed in the Concerned Alarms field below the list.

14. Click **Parameter Setting** located to the right of the Concerned Alarm field, the Set Alarm Parameter dialog box appears with all alarms with parameters listed.
15. Click the trap name to expand the alarm parameters.
16. Input the value in the field right of the parameters name:
    o To set multiple values for a parameter, click the icon to add a line, or
    o To remove a line, click the icon , or
To restore a parameter that you have removed, enter the Set Alarm Parameter page again.

17. Click OK.

IMC determines whether to forward the received alarms according to the configured parameters.

18. To delete one or more alarm conditions, highlight the condition(s) and click Delete.

Not all alarms have parameters.

When you select multiple MIB objects or alarm conditions, the alarm conditions are evaluated and performed as an OR operation. With OR operations, only one of the conditions that you select must be true for the alarm notification rule to generate an email notification.

19. Confirm that the MIB objects or conditions you selected have populated the Concerned Alarms field in the Add Mail Notification page.

If IMC does not have the vendor’s MIBs you want to send email notifications, you can add them and then add a mail notification rule. For adding a MIB to IMC, see "MIB management" (page 138).

20. Enter the hourly range in the Time Ranges field for each day of the week, using an hh:mm-hh:mm format.

To exclude a day of the week, delete any values, including 00:00, from the hourly range for that day.

21. Click OK.

You must configure IMC to forward email notifications to the SMTP server in your environment for recipients to receive email alarm notifications. For information on configuring IMC to forward emails to your SMTP server, see "Mail server settings" (page 135).

You must configure the SMSC settings in IMC to forward messaging notifications. For information on configuring SMSC settings, see "SMSC settings" (page 136).

Modifying an SMS alarm notification rule

To modify an SMS alarm notification:

1. Navigate to Alarm Notification.

   a. Click the Alarm tab from the tabular navigation system on the top.

   b. Click Alarm Settings on the navigation tree on the left.

   c. Click Alarm Notification under Alarm Settings from the navigation tree on the left.

2. Click the Modify icon in the Alarm Notification main pane associated with the message or SMS notification rule you want to modify.

You cannot modify the name of an alarm rule once you have created it.

3. Add, modify or remove telephone numbers as needed and click Add.

   Only digits (0,1,2,3,4,5,6,7,8,9), parentheses (()), plus sign (+), hyphen (-), and spaces ( ) are permitted in the Telephone Number field.

   Be sure to include the country code and area code of the recipient if needed for SMS notifications for this rule.

   o To add multiple recipients, click Add after entering each SMS address in the Telephone Number field.

   o To delete one or more SMS recipients, highlight the recipient(s) you want to delete and click Delete.

4. Do one of the following:
Click the checkbox ☑ to the left of the alarm level you want to apply to this SMS message notification rule next to Concerned Alarm Levels.

Click the checked box ☑ next the alarm level you want to exclude.

5. Select All Devices or Selected Devices from the Concerned Devices list.
   - All Devices: If you select this option after initially configuring this option with Selected Devices, then IMC overrides the existing configuration by configuring the alarm rule to send to all devices.
   - Selected Devices: With this option, only the selected devices trigger an SMS notification if the alarm condition meets the rule’s Concerned Alarm Levels setting.

6. Select devices by Device IP address, by Custom Views, by Network Segment or by a combination of the three.
   For more information, see "Selecting devices by IP address" (page 588), "Selecting devices by custom view" (page 588), or "Selecting devices by network segment" (589).

7. Select devices by using Select located to the right of the Device IP field.
   This enables you to use IMC’s display and search capabilities to select the device(s) from established groups and views either By View or by query using the Advanced feature. See "Adding devices by View" (page 85) and "Adding devices by Advanced query" (page 85).

8. Modify which error conditions triggers SMS notifications from the Concerned Alarms list. Operators can select all conditions or only a specified subset of conditions that trigger alarms.
   - All Alarms: With this option, all alarms configured in IMC trigger an SMS notification to be sent if the alarm condition is triggered.
   - Selected Alarms: With this option, only the alarms you select in alarm notification trigger an SMS notification if the alarm condition is triggered. Further, you can select which alarm conditions generate SMS alarm notifications.

9. To configure which conditions to send notifications for:
   a. Click Select located to the right of the Concerned Alarms field. The Select Alarm dialog box appears.
   b. In the Select Alarm dialog box, locate the Enterprise MIB that contains an object or condition that you want to alarm on.
   c. To expand your view of the MIB, click on the arrow key ▶ next to the MIB that contains an object or condition that you want to alarm on.
   d. Click the Expand all icon + located in the upper right corner of the Select Alarm dialog box to expand your view to display all MIBs, or
   e. Use the query function located at the top of the Select Alarm dialog box to locate the object that you want alarm on.

10. Enter one or more of the following search criteria:
    - Trap Name: Enter the object name for the trap you want to locate in the Trap Name field.
    - Trap OID: Enter the Object ID for the trap in the Trap OID field.
    - Enterprise Name: Enter a partial or complete name for the Enterprise MIB you want to locate in the Enterprise Name field.
    - Enterprise OID: Enter a partial or complete Enterprise ID for the MIB you want to locate in the Enterprise OID field.
11. Click **Query** to submit your search criteria. The results of your query display in the dialog box. Optional: Click **Reset** to clear your query criteria and to restore the full list of MIBs and traps.

12. Click the checkbox ☑️ to select a MIB object that you want to alarm on.

13. Click **OK**.

   It may take a while for the **Select Alarm** dialog box to close. When the box closes, it updates the **Concerned Alarms** field with the configured object or alarm condition.

   You can click on multiple checkboxes to select multiple objects or conditions to alarm on. Each alarm condition is listed in the **Concerned Alarms** field below the list.

14. Click **Parameter Setting** located to the right of the **Concerned Alarm** field, the **Set Alarm Parameter** dialog box appears with all alarms with parameters listed.

15. Click the trap name to expand the alarm parameters.

16. Input the value in the field right of the parameters name:
   - To set multiple values for a parameter, click the icon ☐️ to add a line, or
   - To remove a line, click the icon ✗, or
   - To restore a parameter that you have removed, enter the **Set Alarm Parameter** page again.

17. Click **OK**.

   IMC determines whether to forward the received alarms according to the configured parameters.

18. To delete one or more alarm conditions, highlight the condition(s) and click **Delete**.

   Not all alarms have parameters.

   When you select multiple MIB objects or alarm conditions, the alarm conditions are evaluated and performed as an OR operation. With OR operations, only one of the conditions that you select must be true for the alarm notification rule to generate an email notification.

19. Confirm that the MIB objects or conditions you selected have populated the **Concerned Alarms** field in the **Add Mail Notification** page.

   If IMC does not have the vendor’s MIBs you want to send email notifications, you can add them and then add a mail notification rule. For adding a MIB to IMC, see "MIB management" (page 138).

20. Enter the hourly range in the **Time Ranges** field for each day of the week, using an hh:mm-hh:mm format.

   To exclude a day of the week, delete any values, including 00:00, from the hourly range for that day.

21. Click **OK**.

**Copying an SMS alarm notification**

To copy an SMS alarm notification rule:

1. Navigate to **Alarm Notification**:
   a. Click the **Alarm** tab from the tabular navigation system on the top.
   b. Click **Alarm Settings** on the navigation tree on the left.
   c. Click **Alarm Notification** under **Alarm Settings** from the navigation tree on the left.

2. Click the **Copy** icon ☞️ in the **Message Notification** list associated with the alarm rule you want to copy.

3. Rename the rule by giving it a unique name.
4. Make any necessary modifications to the rule in the Copy Message Notification page. For more information on modifying an SMS Notification, see "Modifying an SMS alarm notification rule" (page 596).

5. Click OK.

Enabling/disabling an SMS alarm notification

To enable or disable an SMS alarm notification rule:
1. Navigate to Alarm Notification:
   a. Click the Alarm tab from the tabular navigation system on the top.
   b. Click Alarm Settings on the navigation tree on the left.
   c. Click Alarm Notification under Alarm Settings from the navigation tree on the left.
2. Do one of the following:
   o To enable, click the disabled status icon Disable in the Message Notification Status field associated with the message rule you want to enable, or
   o To disable, click the enabled status icon Enable in the Message Notification Status field associated with the message rule you want to disable.

Deleting an SMS alarm notification rule

To delete an SMS alarm notification rule:
1. Navigate to Alarm Notification:
   a. Click the Alarm tab from the tabular navigation system on the top.
   b. Click Alarm Settings on the navigation tree on the left.
   c. Click Alarm Notification under Alarm Settings from the navigation tree on the left.
2. Click the Delete icon in the SMS Notification list associated with the alarm rule you want to delete.
3. Click OK to confirm deletion of the rule.

Managing alarm forwarding: Integrating with other management systems

You can configure IMC to forward alarm notifications to other management systems including help desk ticketing systems by establishing notification rules that contain the configuration parameters necessary to forward alarms.

You can configure one or more rules that define which faults or errors in the network infrastructure are forwarded to other management systems. Alarm forwarding rules can also be included to forward alarms by device or groups of devices as well as by day and time of day.

Adding an alarm forwarding rule

To add an alarm forwarding rule:
1. Navigate to Alarm Notification:
   a. Click the Alarm tab from the tabular navigation system on the top.
b. Click **Alarm Settings** on the navigation tree on the left.

c. Click **Alarm Notification** under **Alarm Settings** from the navigation tree on the left.

2. Click **Add** under **Alarm Forwarding** in the main pane.

3. Enter a name for this alarm forwarding rule in the **Rule Name** field. Once you create a rule, you cannot modify its name.

4. Enter the IP address of the destination management system for this rule in the **Destination IP Address** field.

5. Enter the destination port number for the management system for this rule in the **Port** field.

6. Click the checkbox to the left of the alarm level you want to apply to this forwarding rule next to **Concerned Alarm Levels**.

   This configuration parameter determines which severity or alarm levels trigger alarm forwarding. For new alarm forwarding rules, all alarm levels are checked with the exception of **Info** alarms.

   a. To remove an alarm level setting, click the checked box next to each of the severity or alarm levels you want to exclude for this alarm rule.

7. Select **All Devices** or **Selected Devices** from the **Concerned Devices** list.

   a. **All Devices**: With this option, all devices in IMC trigger alarm forwarding if the alarm condition meets the rule’s **Concerned Alarm Level** setting. For example, if you set the alarm level to critical and major, then all devices in the network infrastructure that have a condition that is configured in IMC as critical and major generate alarm forwarding to all recipients configured in this rule.

   b. **Selected Devices**: With this option, only the selected devices trigger alarm forwarding if the alarm condition meets the rule’s **Concerned Alarm Level** setting. You can select devices by **Device IP address**, by **Custom Views**, by **Network Segment** or by a combination of the three. For more information, see "Selecting devices by IP address" (page 588), "Selecting devices by custom view" (page 588), or "Selecting devices by network segment" (589). You can select devices by using either the View or Advanced query option. See "Adding devices by View" (page 85) and "Adding devices by Advanced query" (page 85).

   You can add devices using one or more of the **Selected Devices** options. For example, you can enter the IP address of one device and an IP address range, and groups defined by custom view. The alarm notification rule forwards alarms for all devices or groups configured in the rule.

8. Select which error conditions trigger alarm forwarding from the **Concerned Alarms** list. Operators can select all conditions or only a specified subset of conditions that trigger alarm forwarding.

   a. **All Alarms**: With this option, all alarms configured in IMC generate alarm forwarding if the alarm condition is triggered.

   b. **Selected Alarms**: With this option, only the alarms you select in alarm notification generate alarm forwarding if the alarm condition is triggered. Further, you can select which alarms trigger alarm forwarding.

9. To configure which conditions to send notifications for:

   a. Click **Select** located to the right of the **Concerned Alarms** field. The **Select Alarm** dialog box appears.

   b. In the **Select Alarm** dialog box, locate the Enterprise MIB that contains an object or condition that you want to alarm on.
c. To expand your view of the MIB, click on the arrow key next to the MIB that contains an object or condition that you want to alarm on.

d. Click the Expand all icon located in the upper right corner of the Select Alarm dialog box to expand your view to display all MIBs, or

Use the query function located at the top of the Select Alarm dialog box to locate the object that you want alarm on.

10. Enter one or more of the following search criteria:
   - **Trap Name**: Enter the object name for the trap you want to locate in the Trap Name field.
   - **Trap OID**: Enter the Object ID for the trap in the Trap OID field.
   - **Enterprise Name**: Enter a partial or complete name for the Enterprise MIB you want to locate in the Enterprise Name field.
   - **Enterprise OID**: Enter a partial or complete Enterprise ID for the MIB you want to locate in the Enterprise OID field.

11. Click Query to submit your search criteria. The results of your query display in the dialog box.

Optional: Click Reset to clear your query criteria and to restore the full list of MIBs and traps.

12. Click the checkbox to select a MIB object that you want to alarm on.

13. Click OK.

It may take a while for the Select Alarm dialog box to close. When the box closes, it updates the Concerned Alarms field with the configured object or alarm condition.

You can click on multiple checkboxes to select multiple objects or conditions to alarm on. Each alarm condition is listed in the Concerned Alarms field below the list.

14. Click Parameter Setting located to the right of the Concerned Alarm field, the Set Alarm Parameter dialog box appears with all alarms with parameters listed.

15. Click the trap name to expand the alarm parameters.

16. Input the value in the field right of the parameters name:
   - To set multiple values for a parameter, click the icon to add a line, or
   - To remove a line, click the icon , or
   - To restore a parameter that you have removed, enter the Set Alarm Parameter page again.

17. Click OK.

IMC determines whether to forward the received alarms according to the configured parameters.

18. To delete one or more alarm conditions, highlight the conditions and click Delete.

Not all alarms have parameters. When you select multiple MIB objects or alarm conditions, the alarm conditions are evaluated and performed as an OR operation. With OR operations, only one of the conditions that you select must be true for the alarm notification rule to generate an email notification.

19. Confirm that the MIB objects or conditions you selected have populated the Concerned Alarms field in the Add Mail Notification page.

If IMC does not have the vendor’s MIBs you want to send email notifications, you can add them and then add a mail notification rule. For adding a MIB to IMC, see “MIB management” (page 138).

20. Enter the hourly range in the Time Ranges field for each day of the week, using an hh:mm-hh:mm format.

To exclude a day of the week, delete any values, including 00:00, from the hourly range for that day.
21. Click OK.

You can integrate IMC into multiple systems by creating one forwarding rule for each system.

Modifying an alarm forwarding rule

To modify an alarm forwarding rule:

1. Navigate to Alarm Notification:
   a. Click the Alarm tab from the tabular navigation system on the top.
   b. Click Alarm Settings on the navigation tree on the left.
   c. Click Alarm Notification under Alarm Settings from the navigation tree on the left.

2. Click the Modify icon in the Alarm Notification main pane associated with the alarm forwarding rule you want to modify.

You cannot modify the name of an alarm rule once you have created it.

3. Modify the IP address of the destination management system for this rule as needed in the Destination IP Address field.

4. Modify the destination port number for the management system for this rule as needed in the Port field.

5. Do one of the following:
   - Click the checkbox to the left of the alarm level you want to apply to this mail notification rule next to Concerned Alarm Levels.
   - To remove an alarm level setting, click the checked box next to each of the severity or alarm levels you want to exclude for this alarm rule.

6. Select All Devices or Selected Devices from the Concerned Devices list.
   - All Devices: If you select this option after initially configuring this option with Selected Devices, then IMC overrides the existing configuration by configuring the alarm rule to send to all devices.
   - Selected Devices: With this option, only the selected devices trigger alarm forwarding if the alarm condition meets the rule’s Concerned Alarm Level setting.

You can modify your selection devices by Device IP address, by Custom Views, by Network Segment or by a combination of the three. For more information, see "Selecting devices by IP address" (page 588), "Selecting devices by custom view" (page 588), or "Selecting devices by network segment" (589).

You can also select devices by using Select located to the right of the Device IP field. This enables you to use IMC’s display and search capabilities to select the device(s) from established groups and views either By View or by query using the Advanced feature. See "Adding devices by View" (page 85) and "Adding devices by Advanced query" (page 85).

7. Modify which error conditions trigger alarm forwarding from the Concerned Alarms list. Operators can select all conditions or only a specified subset of conditions that trigger alarm forwarding.
   - All Alarms: With this option, all alarms configured in IMC trigger alarm forwarding if the alarm condition is triggered.
   - Selected Alarms: With this option, only the alarms you select in alarm notification trigger alarm forwarding if the alarm condition is triggered. If you choose Selected Alarms, you can choose which alarm conditions trigger alarm forwarding.

8. Click Select to configure which conditions to alarm on.
9. In the Select Alarm dialog box, locate the Enterprise MIB that contains an object or condition that you want to alarm on.

10. To expand your view of the MIB, click the arrow key next to the MIB that contains an object or condition that you want to alarm on.

11. Do one of the following:
   - Click the Expand all icon located in the upper right corner of the Select Alarm dialog box to expand your view to display all MIB, or
   - Use the query function located at the top of the Select Alarm dialog box to locate the object that you want alarm on by entering one or more of the following search criteria:
     - Trap Name: Enter the object name for the trap you want to locate in the Trap Name field.
     - Trap OID: Enter the Object ID for the trap in the Trap OID field.
     - Enterprise Name: Enter a partial or complete name for the Enterprise MIB you want to locate in the Enterprise Name field.
     - Enterprise OID: Enter a partial or complete Enterprise ID for the MIB you want to locate in the Enterprise OID field.
   - Click Query to submit your search criteria.

The results of your query displayed in the dialog box.

Click Reset to clear your query criteria and to restore the full list of MIBs and traps.

12. Click the checkbox to select a MIB object that you want to add to this alarm rule.

13. Click OK.

It may take a while for the Select Alarm dialog box to close. When the box closes, it updates the Concerned Alarms field with the configured object or alarm condition.

14. Click multiple checkboxes to select multiple objects or conditions to alarm on. Each alarm condition is listed in the Concerned Alarms field below the list.

15. Click Parameter Setting located to the right of the Concerned Alarm field and to set the parameters for the Concerned Alarms.

The Set Alarm Parameter dialog box displays with all alarms that have parameters shown.

16. Click the trap name to expand the alarm parameters.

17. Input the value in the field right of the parameters name:
   - If multiple values need to be set for a parameter, click the icon to add a line, or
   - To remove a line, click the icon.

18. To restore a parameter that you have removed, enter the Set Alarm Parameter page again.

19. Click OK.

20. To delete one or more alarm conditions, highlight the condition(s) and click Delete.

IMC determines whether to forward the received alarms according to the configured parameters.

Not all alarms have parameters. When you select multiple MIB objects or alarm conditions, the alarm conditions are evaluated and performed as an OR operation. With OR operations, only one of the conditions that you selected must be true for the alarm notification rule to generate an email notification.

21. Confirm that the MIB objects or conditions you have either added or removed have populated the Concerned Alarms field in the Modify Alarm Forwarding page.
22. Modify the hourly range in the **Time Ranges** field for each day of the week, using the hh:mm-hh:mm format.

23. To exclude a day of the week, delete any values, including 00:00, from the hourly range for that day.

24. Click OK.

### Copying an alarm forwarding rule

To copy an alarm forwarding rule:

1. Navigate to **Alarm Notification**.
   - a. Click the **Alarm Tab** from the tabular navigation system on the top.
   - b. Click **Alarm Settings** on the navigation tree on the left.
   - c. Click **Alarm Notification** under **Alarm Settings** from the navigation tree on the left.

2. Click the **Copy** icon in the **Alarm Forwarding** list associated with the alarm rule you want to copy.

3. Rename the rule by giving it a unique name.

4. Make any necessary modifications to the rule in the **Copy Alarm Forwarding** page. For more information on modifying an alarm forwarding rule, see "Modifying an alarm forwarding rule" (page 602).

5. Click OK.

### Enabling/disabling an alarm forwarding rule

To enable or disable an alarm forwarding rule:

1. Navigate to **Alarm Notification**:
   - a. Click the **Alarm** tab from the tabular navigation system on the top.
   - b. Click **Alarm Settings** on the navigation tree on the left.
   - c. Click **Alarm Notification** under **Alarm Settings** from the navigation tree on the left.

2. Do one of the following:
   - To enable an alarm forwarding rule, click the disabled status icon **Disable** in the **Alarm Forwarding Status** field for the target rule, or
   - To disable an alarm forwarding rule, click the enabled status icon **Enable** in the **Alarm Forwarding Status** field for the target rule.

### Deleting an alarm forwarding rule

To delete an alarm forwarding rule:

1. Navigate to **Alarm Notification**:
   - a. Click the **Alarm** tab from the tabular navigation system on the top.
   - b. Click **Alarm Settings** on the navigation tree on the left.
   - c. Click **Alarm Notification** under **Alarm Settings** from the navigation tree on the left.

2. Click the **Delete** icon in the **Alarm Forwarding** list associated with the alarm rule you want to delete.
3. Click OK to confirm deletion of the rule.

Managing hierarchical alarm settings

You can aggregate alarms by forwarding alarms to other instances of IMC. For more information on configuring IMC to forward alarms in a hierarchical configuration of IMC, see "IMC hierarchical alarm configuration" (page 137).

Access device and core device alarm settings

An event storm occurs when many alarms are generated for what can be attributed to a single failure or error in the network. While event storms can be an unfortunate consequence of a managed network infrastructure, they are not unusual because many managed devices, users, or services can be affected by a failure or error on one device and managed devices report errors when they are configured to do so.

Most event management systems, IMC included, have capabilities for managing event storms. However, management systems can still generate event storms if the event management system is unaware of or unable to accurately determine its place in the network relative to all managed devices.

IMC manages event storms automatically by accurately determining its place in the network and combining knowledge of its position with sophisticated rules based on years of research around the behavior of networks, failures, and event suppression techniques. The net result is a dramatic reduction in alarming and event storms. As part of this process, IMC distinguishes between and labels root alarms as those alarms that indicate the root cause of a failure from symptom alarms, those events that suggest or point to a problem elsewhere.

You can modify how IMC understands its place in the network infrastructure by adding to the knowledge of what is considered an access device and what is considered a core device.

⚠️ CAUTION:
These changes can affect how IMC responds to failures and manages alarm suppression. Use this feature with caution and keep in mind the recipients of alarm notifications when making these changes.

Adding an access device

To add an access device:

1. Navigate to Access Devices and Core Devices:
   a. Click the Alarm tab from the tabular navigation system on the top.
   b. Click Alarm Settings on the navigation tree on the left.
   c. Click Access Device and Core Device under Alarm Settings from the navigation tree on the left.

2. Click Add under Access Device in the Access Device and Core Device window.

3. Add devices by using either the View or Advanced query option. See "Adding devices by View" (page 85) and "Adding devices by Advanced query" (page 85).

4. Highlight the device you want to add and click Add selected to add it to the Selected Devices list.

5. Confirm that the device you have found has been added.

6. Click OK. Confirm that the device has been added to the Access Device portion of the Access Device and Core Device window.
Deleting an access device

To delete an access device:

1. Navigate to Access Devices and Core Devices:
   a. Click the Alarm tab from the tabular navigation system on the top.
   b. Click Alarm Settings on the navigation tree on the left.
   c. Click Access Device and Core Device under Alarm Settings from the navigation tree on the left.

2. Click the Delete icon \( \times \) next to the access device you want to delete from the Access Device and Core Device window.

Adding a core device

To add a core device:

1. Navigate to Access Devices and Core Devices:
   a. Click the Alarm tab from the tabular navigation system on the top.
   b. Click Alarm Settings on the navigation tree on the left.
   c. Click Access Device and Core Device under Alarm Settings from the navigation tree on the left.

2. Click Add under Core Device in the Access Device and Core Device window.
3. Add devices by using either the By View or Advanced query option. See "Adding devices by View" (page 85) and "Adding devices by Advanced query" (page 85).
4. Highlight the device(s) you want to select and click Add selected \( \square \) to add them to the Selected Devices list:
   - To select all of the devices displayed in the Devices Found list, click Add all \( \square \), or
   - To remove one or more device(s), select them and click Remove selected \( \square \), or
   - To remove all of the selected devices, click Remove all \( \square \).
5. Confirm that the device you have found has been added.
6. Click OK.
7. Confirm that the device has been added to the Core Device portion of the Access Device and Core Device window.

Deleting a core device

To delete a core device:

1. Navigate to Access Devices and Core Devices:
   a. Click the Alarm tab from the tabular navigation system on the top.
   b. Click Alarm Settings on the navigation tree on the left.
   c. Click Access Device and Core Device under Alarm Settings from the navigation tree on the left.

2. Click the Delete icon \( \times \) next to the core device you want to delete from the Access Device and Core Device window.
IMC provides real time and historical performance management for managed devices. The Performance Management features provide you with the ability to customize the collection, alarming and presentation of performance data. In addition, you can leverage system or user defined global or individual monitors to collect performance information, generate historical reports on the performance of devices or generate alarms when performance monitors meet threshold conditions.

Upon installation, you have access to several groups of more than two hundred globally defined monitors that define the monitoring options for configuring monitoring for individual devices.

Within these global monitors, sixteen come configured with polling intervals, threshold settings, and alarm settings configured to enable immediate, proactive performance monitoring of devices managed in IMC.

Of the sixteen global monitors, four are immediately added to the performance monitoring of devices whenever devices are added to IMC, providing a standard set of monitors for immediate performance monitoring and reporting. These four monitors include Device Un-reachability Proportion, Device Response Time, CPU Usage, and Memory Usage.

IMC also provides the ability to customize the list of global monitors that define performance monitoring. You can add custom monitors to the set of global index settings monitors, modify or remove the threshold settings for global monitors that already have these settings defined, add threshold settings for global monitors that have no pre-defined thresholds set, or add, remove, or modify the set of default global monitors that are applied when a device is added to IMC.

In addition to global monitoring options, you can also customize the list and configuration of monitors that are applied to individual devices or groups of devices or add monitors to or remove monitors from the list for one or more devices. Naturally, you can also add, modify, or remove the threshold settings for performance monitors that determine when a performance monitor generates an alarm.

Once monitors have been created for a device, you can create views for viewing the historical data collected by the performance monitors. You can also organize views by folders and create shortcuts for easy access to performance views from the left navigation tree. Lastly, you can customize which performance views are available from the Network Topology.

Managing performance with global index settings

IMC provides you with over two hundred globally defined monitors organized into eight monitor groups. The first of these is a system monitoring group that includes monitoring for general system performance such as reachability, CPU, memory, and device response time.

In addition, the Performance Management feature provides device specific performance monitoring for IPsec VPNs, WLANs, IVS, QoS, VSM, and RMON. All of these monitors can be found under Global Index Settings.

There are sixteen global monitors already configured with polling intervals, threshold settings and alarm level settings, enabling you to immediately and proactively monitor the performance of devices managed in IMC.

Out of the box, you have a standard set of monitors for performance monitoring and reporting along with over 200 monitors that can be configured with threshold settings and applied to specific devices for more
comprehensive and technology specific performance monitoring, allowing you to create custom global monitors to expand the set of global performance monitors.

Once you have configured global monitors, these monitor settings can be applied to individual devices using the Monitoring Settings feature within the Performance Management service.

**Accessing global index settings**

All global monitors are listed in the Global Index Settings list in IMC.

To access the Global Index Settings List:

1. Navigate to Resource ➔ Global Index Settings:
   a. Click the Resource tab from the tabular navigation system on the top.
   b. Click Performance Management link on the navigation tree on the left.
   c. Click Global Index Settings under Performance Management from the navigation system on the left.

   The Global Index Settings page displays with monitors grouped by type.

2. To view the individual monitors, click the expand icon located to the left of the group name.
   o Index Name: Contains the name for the monitor index.
   o Threshold 1: Contains the value of the first threshold for the associated monitor index.
   o Alarm Level: Contains the severity or alarm level for alarms that are generated when the condition of the first threshold is met.
   o Repeat Time: Contains the number of sequential data samples that must be collected and meet the first threshold value to trigger an alarm in IMC.
   o Threshold 2: Contains the value for the second threshold for the associated monitor index.
   o Alarm Level: Contains the severity or alarm level for alarms that are generated when the condition of the second threshold is met.
   o Repeat Time: Contains the number of sequential data samples that must be collected and meet the second threshold value to trigger an alarm in IMC.
   o Interval (Sec.): contains the sampling interval in seconds for the associated monitor.

3. If the Global Index Settings list contains multiple entries, the navigational icons shown below may appear:
   o Click ➔ to page forward in the Global Index Settings list.
   o Click ➔ to page forward to the end of the Global Index Settings list.
   o Click ➔ to page backward in the Global Index Settings list.
   o Click ➔ to page backward to the front of the Global Index Settings list.
   o Click ➔ at the bottom of the Global Index Settings list to refresh the list.

**Searching global index settings**

To query the Global Index Settings:

1. Navigate to Resource ➔ Global Index Settings:
a. Click the **Resource** tab from the tabular navigation system on the top.

b. Click the **Performance Management** link on the navigation tree on the left.

c. Click ![Global Index Settings](image) under **Performance Management** from the navigation system on the left.

   The **Global Index Settings** page displays with monitors grouped by type.

   To view the individual monitors, click the expand icon ![Expand](image) located to the left of the group name.

2. Click the ![Query Criteria](image) button located on the toolbar at the top of the **Global Index Settings** list.

3. Enter one or more of the search criteria listed below:
   - **Index Name**: Enter a partial or complete index name in the **Index Name** field.
   - **Index Group Name**: To filter the list by group name, enter the name of the group in the **Index Group Name** field.

4. Click **Query** to begin your search.

   The result of your search displays in the **Global Index Settings** list.

### Managing global index settings

You can create custom global monitors using the **Add Custom Index** option, modify the threshold and alarming features of a global performance monitor, or modify the list of default monitors that are applied to all devices when added to IMC.

### Adding a user defined monitor to the global index settings

In addition to the system defined global monitors that are available in IMC by default, you can also add your own custom monitors to the list of global index settings or monitors.

To add a custom or user defined global monitor:

1. Navigate to **Resource** → **Global Index Settings**:
   a. Click the **Resource** tab from the tabular navigation system on the top.
   b. Click the **Performance Management** link on the navigation tree on the left.

2. **Click ![Global Index Settings](image) under **Performance Management** from the navigation system on the left.**

   The **Global Index Settings** page displays with monitors grouped by type.

   To view the individual monitors, click the expand icon ![Expand](image) located to the left of the group name.

   The page is updated to display an expanded list of monitors.

2. Click the ![Add Custom Index](image) button located on the toolbar at the top of the **Global Index Settings** list.

   The **Add Custom Index** page appears.

3. Enter a name for the custom global monitor in the **Name** field.

4. To define the unit of measure, do one of the following:
   - To use a pre-defined unit of measure, select it from the **Predefined** list, or
   - To define a custom unit of measure, click the radio button ![Custom](image) to the left of **Custom** and enter the unit of measure in the field to the right of **Custom**.
The **Type** field defines the user-defined instance of the performance monitor as defined in the MIB definition.

Multi-level MIB objects are supported.

5. Enter the monitor format in the **Type** field using the following format:

```
[index1[0|2]:NAME:TYPE:LENGTH].[index2[0|2]:NAME:TYPE:LENGTH]
```

- The parameter `indexN` defines the hierarchy level of a monitor instance. For example, `[index1[2]:Frame:1:0].[index2[2]:Slot:1:0].[index3[2]:Memory:1:0]` indicates the memory on the slot of the frame.
- 0 indicates a MIB leaf node and 2 indicates a non-leaf node.
- The value in the **NAME** field identifies the name of the instance for the performance monitor. This name is used by IMC as the name of the instance for the performance monitor.
- 1 in the **TYPE** field indicates an integer and 2 indicates a string.
- The value in the **LENGTH** field indicates the index length, which is 0 for integer index and non-hierarchical index.
- Use a colon `:"` to separate each field in the definition.
- Use a dot `"."` to separate length values for hierarchical indices.

For example, `[index1[2]:Interface:1:0]` and `[index1[2]:Frame:1:0].[index2[2]:Slot:1:0].[index3[2]:Memory:1:0]` are both valid entries for the **Type** field.

6. Enter the object identifier (OID) of the MIB object you want to use to translate numeric values into user friendly values in the **Definition OID** field.

7. Use a colon `":"` to separate the OIDs for hierarchical indices, and enter 0 if no OID is provided.

IMC displays user friendly values together with the instance names you defined in **Step 5**.

For example, the ifIndex object of the ifEntry table of the MIB2 ifTable contains numeric values for every interface in the table. The ifDescr object of the ifEntry table contains a name or description for every interface in the table and is more readable. The **Definition OID** field allows you to use the values contained in ifDescr to translate the ifIndex value into the more usable descriptions for interfaces on the device being monitored.

8. Do one of the following:

- To use IMC’s integrated MIB browser to select the object:
  a. Click **Select OID**.
  b. Locate the section of the MIB tree that contains the object you want to use for this global index.
  c. To expand your view of the MIB, click the arrow key `»` to the left of the MIB Tree.
  d. Continue to expand using this arrow key until you have located the object you want to use.
  e. Click **OK**.

9. Enter the MIB object to be monitored and the calculation algorithm in the **Formula** field.

The results calculated by this algorithm are the performance data of the monitored instance.

The characters that can be used in this field include `+ - * / t' ( )`, where `"t"` must be lowercase, indicating the query interval.

The quotation mark (`'`) must be placed immediately to the right of the OID, indicating the value of the previous poll. This is used to offset the calculation.

- An example of a valid entry in the **Formula** field would be:

```
1.3.6.1.2.1.2.2.1.10
```
This formula instructs IMC to use the MIB object, ifInOctets (inbound traffic of the interface) as the returned value for this monitor. This formula would return the data collected for ifInOctets for one poll cycle. In this example, since ifInOctets is an object in the ifEntry table, the Definition OID for this formula would be ifDescr (1.3.6.1.2.1.2.2.1.2) and the Type field could be [index1][2]:Interface:1:0.

- Another example of a valid entry in the Formula field would be:
  
  \[1.3.6.1.2.1.2.2.1.10-1.3.6.1.2.1.2.2.1.10']\]

  \(1.3.6.1.2.1.2.2.1.10'\) indicates the value of ifInOctets in the first poll. \(1.3.6.1.2.1.2.2.1.10\) indicates the value of ifInOctets in the second poll. The formula \(1.3.6.1.2.1.2.2.1.10-1.3.6.1.2.1.2.2.1.10'\) shows the difference of ifInOctets in the two polls.

  In this example, since ifInOctets is an object in the ifEntry table, the Definition OID for this formula would be ifDescr (1.3.6.1.2.1.2.2.1.2) and the Type field could be [index1][2]:Interface:1:0.

  A third example of a valid entry in the Formula field would be:

  \[(1.3.6.1.2.1.2.2.1.10-1.3.6.1.2.1.2.2.1.10')/t\]

  The formula \(1.3.6.1.2.1.2.2.1.10-1.3.6.1.2.1.2.2.1.10')/t\) indicates that the value you get by diving the difference by the polling interval is the inbound traffic rate of the interface.

  In this example, since ifInOctets is an object in the ifEntry table, the Definition OID for this formula would be ifDescr (1.3.6.1.2.1.2.2.1.2) and the Type field could be [index1][2]:Interface:1:0.

- As a final example, provided below is a formula for calculating bandwidth utilization for a half duplex link. In this example, the Measurement field contains %

  Type field contains [index1][2]:Interface:1:0

  Definition OID field contains 1.3.6.1.2.1.2.2.1.2

  Formula field contains

  \(((1.3.6.1.2.1.2.2.1.10-1.3.6.1.2.1.2.2.1.10')+(1.3.6.1.2.1.2.2.1.16-1.3.6.1.2.1.2.2.1.16'))*8\]

  \(*100/(t*1.3.6.1.2.1.2.2.1.5))\]

- Here is the same formula using MIB object names rather than the Object ID.

  \(((ifInOctets-ifInOctets')+( ifOutOctets-ifOutOctets'))*8*100/(t*ifSpeed))\]

  a. To use IMC’s integrated MIB browser that has a graphical interface for selecting each MIB object in the formula, click Select OID.

- Locate the section of the MIB tree that contains the object you want to use for this global index setting.

- b. To expand your view of the MIB, click on the arrow key \(\text{ }\) to the left of the MIB Tree.

- c. Click the MIB object you want to use to select it.

- d. Click OK. The Object ID for the object you selected displays in the Formula field.

- e. Repeat as necessary for each MIB object you want to use in the formula.

10. Click Test to validate the proper functioning of your custom global index definition.

    The page updates to display the Test Customized Index page.

11. Do the following to continue the validation test:

    a. Enter the IP address of the device you want to use to test your formula in the Select Device or Enter IP Address field. You can also select the device you want to use by clicking Select located to the right of this field.

    b. Select the instance from the Select Instance list.
c. To have IMC populate a list of interfaces for the selected device, click **Resolve** located to the right of the **Select Instance** list.

The page and the **Select Instance** list update to include all available interfaces.

d. Click **Start** to begin the data collection test process for the monitor you have created.

The results of the data collection display in the **Result** table. This table presents the results of sequential polls for the selected device and interface.

e. Scroll to the bottom of the **Result** table and click **Back** when you have completed testing of the formula for the user-defined monitor you have created.

12. When you completed the configuration of the custom index setting and the test results were successful, click **Apply** to create the custom global index.

Once you create a user-defined monitor, you can no longer access the configuration page for modifying it. You can only modify its threshold and interval settings or delete it.

You can compile MIBs into IMC for monitoring the performance of devices. Once MIBs are compiled into IMC, their MIB objects become available for performance monitoring and fault management. For more information on compiling MIBs into IMC, see "Compiling a MIB in IMC" (page XX).

**Modifying a global monitor in the global index settings**

You can modify system defined threshold settings for global monitors. Changing threshold settings for global indices changes the threshold settings for all existing monitors as well as all monitors that are created after the threshold setting change was made.

To modify the performance thresholds for a global index:

1. Navigate to **Resource**→**Global Index Settings**:
   a. Click the **Resource** tab from the tabular navigation system on the top.
   b. Click the **Performance Management** link on the navigation tree on the left.
   c. Click **Global Index Settings** under **Performance Management** from the navigation system on the left.

   The **Global Index Settings** page displays with monitors grouped by type.

2. To view the individual monitors, click the expand icon located to the left of the group name.

3. Double click the global index or monitor what you want to modify.

   The **Modify Index** dialog box appears.

4. Do one of the following:
   o Click the checkbox to the right of **Threshold 1** if you want to enable the pre-defined settings for the first threshold, or
   o Click the checked box to the right of **Threshold 1** if you want to clear the pre-defined settings for the first threshold and disable setting the threshold.

   **WARNING:**

   Disabling the threshold settings by clicking the checked box deletes the threshold settings.

5. Select the operator you want to use from the **Match Mode** list.

   Options include greater than or equal to, less than or equal to, or **Between**. The option **Between** allows you define a range of values that trigger an alarm.

   The **Match Mode** applies to both **Threshold 1** and **Threshold 2**.
6. Enter the operand or threshold value in the Value 1 field. If you selected Between as your operation in the Match Mode field, enter an operand or a threshold value in the Value 1 field. If you selected Between as your operation in the Match Mode field, enter the second operand or threshold value in the Value 2 field.

7. Select the form of measurement from the Measurement list. The options for this field vary based on the type of monitor instance you are modifying.

8. Enter the number of successive data samples collected that must meet the threshold requirements in the Repeat Time field.

9. Select the severity or alarm level for this monitor from the Alarm Level list.

10. Enter the amount of time between data collections in the Interval (Sec.) field.

11. Do one of the following:
   o Click the check box to the right of Threshold 2 if you want to enable the pre-defined settings for the second threshold, or
   o Click the checked box to the right of Threshold 2 if you want to clear the pre-defined settings for the second threshold and disable setting the threshold.

12. Enter the operand or threshold value in the Value 1 field. If you selected Between as your operation in the Match Mode field, enter an operand or a threshold value in the Value 1 field.

13. If you selected Between as your operation in the Match Mode field, enter the second operand or threshold value in the Value 2 field.

14. Select the form of measurement from the Measurement list. The options for this field vary based on the type of the monitor instance you are modifying.

15. Enter the number of data samples collected that must meet the threshold requirements in the Repeat Time field.

16. Select the severity or alarm level for this monitor from the Alarm Level list. The alarm level of Threshold 2 must be higher than that of Threshold 1.

17. Click OK to accept your threshold settings for the selected monitor.

**Deleting a user-defined monitor from the global index settings**

You can delete user-defined global index monitors but you cannot delete system defined global monitors.

To delete a user-defined global index monitor:

1. Navigate to Resource→Global Index Settings:
   a. Click the Resource tab from the tabular navigation system on the top.
   b. Click the Performance Management link on the navigation tree on the left.
   c. Click Global Index Settings under Performance Management from the navigation system on the left.
      The Global Index Settings page displays with monitors organized into groups.

2. To view the individual monitors, click the expand icon located to the left of the group name. Navigate to the section of the Global Index Setting list that contains user defined monitors.

3. Right-click the user-defined global index or monitor you want to delete. The Delete option appears.
4. Click **Delete**.
5. Click **Yes** to confirm the deletion of the user-defined global index monitor.

### Managing individual device monitoring settings

IMC enables you to fully customize the monitors used to manage the performance of devices. With each device that is added, four monitors are automatically added to the performance management of the device. In addition, you can add new, individual monitors for specific devices, based on the list of monitors found in Global index settings list. You can then use system defined global monitors or the custom monitors added to the Global index settings list. Monitor threshold settings for individual devices can also be customized which overrides the system defined threshold settings of global monitors.

### Accessing the monitor list

All performance management monitors for all devices are displayed in the **Monitor List**. This list can be found under the Monitoring Settings option of Performance Management.

To access the monitor list:

1. Navigate to **Resource** → **Monitoring Settings**:
   - a. Click the Resource tab from the tabular navigation system on the top.
   - b. Click the Performance Management link on the navigation tree on the left.
   - c. Click **Monitoring Settings** under Performance Management from the navigation system on the left.

   The **Monitor List** displays with all devices managed in IMC as the default.
   - **Device Name**: Contains the name or label for the device that is being monitored.
   - **IP Address**: Contains the IP address of the monitored device.
   - **Device Type**: Contains device model information. If the device is managed using SNMP, this field displays the device model. If the device is managed for reachability using ICMP only and thus no device model information is available, this field contains "ICMP."
   - **Instances**: Contains an active link. The link is the number of the monitor instance for the device that is being monitored.

   When the device is managed using SNMP, **CPU Usage (%)**, **Memory Usage (%)**, **Response Time of Device (ms)**, and **Device Unreachability Proportion (%)** are monitored by default.

   When the device is managed for reachability using ICMP only, **Response Time of Device (ms)** and **Device Unreachability Proportion (%)** are monitored by default.

2. Click the **link** of the Data field to view the details of the monitored instances.

   For more information on monitored instances, see "Managing device monitors" (page XX).

   The **CPU Usage (%)** and **Memory Usage (%)** of some devices cannot be monitored if they use proprietary MIBs.
   - **Operation**: Contains three active links. These links are Add Monitor, Cancel Monitor, and Alarm Threshold. For more information on the functions of these links, see "Managing device monitors" (page 617).

   - **Data**: Contains one active link **. Click this link to enter the Performance at a Glance page of the device. For more information on the Performance at a Glance, see "9 Performance management" (page 607).
If the Monitor List contains multiple entries, the following navigational aids may appear:

- Click to page forward in the Monitor List.
- Click to page forward to the end of the Monitor List.
- Click to page backward in the Monitor List.
- Click to page backward to the front of the Monitor List.

3. Click 8, 15, 50, 100, or 200 from the right side of the main pane to configure how many items per page you want to view.

4. For Performance View lists that have more than one page, click on 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 … from the bottom right side of the main pane to jump to a particular page.

You can sort the Monitor List by the Device Name, IP Address, or Device Type fields. Click the column label to sort the list by the selected field. The column label is a toggle switch that allows you to toggle between the various sort options specific to each field.

Switching monitor list

The monitor list, which displays all devices managed in IMC and the numbers of monitored instances of each device, can be in device list or instance list mode.

To switch the monitor list:

1. Navigate to Resource→Monitoring Settings:
   a. Click the Resource tab from the tabular navigation system on the top.
   b. Click the Performance Management link on the navigation tree on the left.
   c. Click Monitoring Settings under Performance Management from the navigation system on the left.

   The Monitor List displays with the Monitor List in the device list mode.

2. Click the Switch to Instance List link located in the upper right corner of the Monitor List.
   The page refreshes to display all the monitor instances. If the link is Switch to Instance List, then you are in the Device List view.

3. Click the Switch to Device List link located in the upper right corner of the Monitor List.
   The page refreshes to display all managed devices. If the link is Switch to Device List, then you are in the Instance List view.

Searching for monitors

Searching for monitors in the device list

   a. Click the Resource tab from the tabular navigation system on the top.
   b. Click the Performance Management link on the navigation tree on the left.
   c. Click Monitoring Settings under Performance Management from the navigation system on the left.
The **Monitor List** displays with the **Monitor List** in the device list mode.

The **Query** area is at the top of the monitor list.

2. Enter one or more of the following search criteria:
   - **Device Name**: Enter a partial or complete device name in the **Device Name** field for the device(s) you want to locate.
   - **IP Address**: Enter a partial or complete IP address in the **IP Address** field for the device(s) you want to locate.
   - **Filtered by View**: Select the custom view, device view, or IP view from the **Filtered by View** list to filter for devices that are members of the selected view.
   - **Device Series**: Select the device series from the **Device Series** list to filter for devices that are members of the selected series.

3. Click **Query** to begin your search. The results of your search display in the **Monitor List**.

4. Click **Reset** to clear the query criteria you entered in the **Query** area and query all the devices in IMC.

**Searching for monitors in the instance list**

   - Click the **Resource** tab from the tabular navigation system on the top.
   - Click the **Performance Management** link on the navigation tree on the left.
   - Click **Monitoring Settings** under **Performance Management** from the navigation system on the left.
     - The **Monitor List** appears.

2. Click the **Switch to Instance List** link located in the upper right corner of the **Monitor List**.
   - The **Query** area is at the top of the monitor list.

3. Enter one or more of the following search criteria:
   - **Device Name**: Enter a partial or complete device name in the **Device Name** field for the device(s) you want to locate.
   - **IP Address**: Enter a partial or complete IP address in the **IP Address** field for the device(s) you want to locate.
   - **Filtered by View**: Select the custom view, device view, or IP view from the **Filtered by View** list to filter for devices that are members of the selected view.
   - **Device Series**: Select the device series from the **Device Series** list to filter for devices that are members of the selected series.
   - **Item Name**: Select the monitor item from the **Item Name** list to filter for instances that are using the selected monitor item.
   - **Instance Name**: Enter a partial or complete instance name in the **Instance Name** field for the instance(s) you want to locate.

4. Click **Query** to begin your search. The results of your search display in the **Monitor List**.

5. Click **Reset** to clear the query criteria you typed in the **Query** area and query all the monitored instances.
Managing device monitors

Adding Monitor Instances

In addition to the default monitor instances that are created for all devices by default, you can add monitor instances by choosing from a list of system or globally defined monitor indices. Once a monitor instance is created, you can modify the monitor instance to add thresholds for alarming on performance issues for selected devices.

To add a monitored instance:

1. Navigate to Resource→Monitoring Settings:
   a. Click the Resource tab from the tabular navigation system on the top.
   b. Click the Performance Management link on the navigation tree on the left.
   c. Click Monitoring Settings under Performance Management from the navigation system on the left.
      The device Monitor List appears.

2. To enter the Add Monitor page, do one of the following:
   a. Click Add Monitor at the top of the Monitor List; or
   b. Click the Add of the device you want to add instances for in the Operation column in the Device List.

3. To select the devices you want to add monitored instances for, click Select Device at the top of the Device List.
   The Select Devices dialog box appears.

4. Add devices by using either the View or Advanced query option.
   See "Adding devices by View" (page 85) and "Adding devices by Advanced query" (page 85).

5. Highlight the device(s) you want to select and do one of the following:
   a. Click Add selected to add them to the Selected Devices list, or
   b. To select all of the devices displayed in the Devices Found list, click Add all, or
   c. To remove one or more device(s), select them and click Remove selected, or
   d. To remove all of the selected devices, click Remove all.

6. Confirm that the devices you want to select have been added.

7. Click OK. Confirm that the devices now appear in the Device List.

8. Select indices by selecting an item from the Select Index list.

9. Select one of the following items from the Select Index list.
   The index or indices appear under the selected item.

10. Click the checkbox to the left of each index as needed.
    You cannot select indices from different items at one time. To monitor indices from multiple items, add monitored instances from one item at a time and repeat your operation until you have added indices from desired items.

11. Select specific instances (optional).
    a. Click the Modify Index checkbox in the upper right corner of the Device List.
b. Click the device link(s) under Device Name to display unmonitored instance(s) and click the checkbox to the left of the instance(s) you want to monitor.

If you do not click the Custom Instances checkbox, all the instances of selected devices are monitored.

If you click the Custom Instances checkbox, you cannot add monitored instances for devices that do not have instances to be monitored. Then, de-select the Custom Instances checkbox.

12. Click Customize Properties in the lower right corner of the Add Monitor window.

The Modify Index dialog box appears. If you selected multiple types of monitor indices, the dialog box lists the indices in each tab.

13. To set the alarm thresholds, do the following:
   a. Double click the tab to launch the unique configuration area to set the alarm thresholds.
   
   b. Click the checked checkbox to the right of Global Index Settings. This disables the application of the default global settings for the selected monitor instance(s) and enables you to configure and apply custom threshold settings.
   
   c. Click the checkbox to the right of Threshold 1 to enable the configuration of the settings for the first threshold.
   
   d. Select the operator you want to use from the Match Mode list.

   Options include greater than or equal to, less than or equal to, or Between. The option Between allows you define a range of values that trigger an alarm. The Match Mode applies to both Threshold 1 and Threshold 2.

   e. Enter the operand or threshold value in the Value 1 field. If you selected Between as your operator in the Match Mode field, enter an operand or a threshold value in the Value 1 field.

   f. If you selected Between as your operator in the Match Mode field, enter the second operand or threshold value in the Value 2 field.

   g. Select the form of measurement from the Measurement list. The options for this field vary based on the type of the monitor instance.

   h. Enter the number of successive data samples collected that must meet the threshold requirements in the Repeat Times field.

   i. Select the severity or alarm level for this monitor type from the Alarm Level list.

   j. Enter the amount of time between data collections in the Interval (Sec.) field.

   k. If you want to apply a second threshold setting for this monitor instance, click the checkbox to the right of Threshold 2 to enable the configuration of the settings for the second threshold.

   l. Enter the operand or threshold value in the Value 1 field. If you selected Between as your operator in the Match Mode field, enter an operand or a threshold value in the Value 1 field.

   m. If you selected Between as your operator in the Match Mode field, enter the second operand or threshold value in the Value 2 field.

   n. Select the form of measurement from the Measurement list. The options for this field vary based on the type of the monitor instance.

   o. Enter the number of data samples collected that must meet the threshold requirements in the Repeat Times field.

   p. Select the severity or alarm level for this monitor type from the Alarm Level list.

   The alarm level of Threshold 2 must be higher than that of Threshold 1.
q. Repeat this step to modify alarm thresholds for other monitor instances.
r. Click **OK** to save your threshold settings.

14. Click **OK** to create the monitor instances. In the **Result** table, you can verify that the task succeeded.

15. Do one of the following:
   o If the task was successful, the **Result** field contains the content, [✓] Succeeded, or
   o If the task failed, the **Result** field contains the content, [✗] Failed. Click the contents of this field to drill down for more information on the cause of the failure.

If you received a [✗] Failed in the **Result** field, it may be because the monitored index is not supported by the device(s) you have chosen.

16. When you have finished reviewing the results of the task, click **OK** to return to the **Monitor List**.

**WARNING:**
If you do not perform Step 5, IMC adds a monitor for every unique instance on the device. For example, if you add a monitor that measures packet errors for the interfaces on a switch, IMC adds a monitor for every interface, including loopback, auxiliary and null interfaces. In addition, it is very likely that you do not want to monitor every interface instance. Therefore, after you have added a monitor to the device, review all monitors that have been added and delete any that you do not want to collect data or generate alarms for. For more information on deleting monitors, see “Deleting monitor instances” (page 621).

Now that you have created monitor instances for the selected devices, you can view reports for the selected monitors by clicking the [‡] link in the **Data** column of the **Monitor List**. For more information on the **Performance Monitor**, see “9 Performance management” (page 607).

You can also modify thresholds for alarming in IMC by modifying the monitor instances you have created.

**Modifying monitor instances**

The **Modify Index** option provides you with the ability to add, remove, or fine tune threshold settings for monitor instances that trigger alarms in IMC. You can modify the threshold settings for one or more monitor instances of the same type or different types for one or more devices.

You can modify the individual monitor instances for any device, whether the monitor instance was created by the operator or was created automatically when the device was added to IMC.

To modify one or more monitor instances:

1. Navigate to **Resource→Monitoring Settings**:
   a. Click the **Resource** tab from the tabular navigation system on the top.
   b. Click the **Performance Management** link on the navigation tree on the left.
   c. Click **Monitoring Settings** under **Performance Management** from the navigation system on the left.

   The **Monitor List** appears.

2. Enter the **Modify Index** page, using any of the following methods:
   o Click the checkbox [☐] to the left of the devices you want to modify. Click **Modify Index** at the top of the **Monitor List** to modify all the monitor instances of the selected devices;
   o Click the **Modify Index** link of the device you want to modify in the **Operation** column to modify all the monitor instances of the device;
Click the **Switch to Instance List** link located in the upper right corner of the **Monitor List**. Click the checkbox □ to the left of the instance(s) you want to modify. Click **Modify Index** at the top of the **Monitor List** to modify all the selected monitor instances;

- Click the **Switch to Instance List** link located in the upper right corner of the **Monitor List**. Click the **Modify Index** of the instance you want to modify in the **Operation** column to modify the monitor instance.

Each monitor instance is displayed in a tab.

3. Click each tab to launch the unique configuration area to set the alarm thresholds.

4. Click the checked checkbox □ to the right of **Global Index Settings**.
   This disables the application of the default global settings for the selected monitor instance(s) and enables you to configure and apply custom threshold settings.

5. Click the checkbox □ to the right of **Threshold 1** to enable the configuration of the settings for the first threshold.

6. Select the operator you want to use from the **Match Mode** list.
   Options include ≥ greater than or equal to, ≤ less than or equal to, or **Between**.
   The option **Between** allows you to define a range of values that trigger an alarm. The **Match Mode** applies to both **Threshold 1** and **Threshold 2**.

7. Enter the operand or threshold value in the **Value 1** field. If you selected **Between** as your operator in the **Match Mode** field, enter an operand or a threshold value in the **Value 2** field.

8. If you selected **Between** as your operator in the **Match Mode** field, enter the second operand or threshold value in the **Value 2** field.

9. Select the form of measurement from the **Measurement** list.
   The options for this field vary based on the type of the monitor instance you are modifying.

10. Enter the number of successive data samples collected that must meet the threshold requirements in the **Repeat Times** field.

11. Select the severity or alarm level for this monitor instance from the **Alarm Level** list.

12. Enter the amount of time between data collections in the **Interval (Sec.)** field.

13. If you want to apply a second threshold setting for this monitor instance, click the checkbox □ to the right of **Threshold 2** to enable the configuration of the settings for the second threshold.

14. Enter the operand or threshold value in the **Value 1** field. If you selected **Between** as your operator in the **Match Mode** field, enter an operand or a threshold value in the **Value 2** field.

15. If you selected **Between** as your operator in the **Match Mode** field, enter the second operand or threshold value in the **Value 2** field.

16. Select the form of measurement from the **Measurement** list. The options for this field vary based on the type of the monitor instance you are modifying.

17. Enter the number of data samples collected that must meet the threshold requirements in the **Repeat Times** field.

18. Select the severity or alarm level for this monitor type from the **Alarm Level** list.
   The alarm level of **Threshold 2** must be higher than that of **Threshold 1**.

19. Repeat Steps 3-18 to modify alarm thresholds for other monitor instances.

20. Click **OK** to save your threshold settings for the monitor instances.
21. In the Result table, you can verify that modifying the selected monitor instance succeeded:
   o If the task was successful, the Result field contains the content, ☑️ Succeeded, or
   o If the task failed, the Result field contains the content, ✗ Failed. Click the contents of this field to drill down for more information on the cause of the failure.

22. When you have finished reviewing the results of the task, click OK to return to the Monitor Instance List.

Deleting monitor instances

You can delete monitor instances for any device, whether the monitor instance was created by the operator or was created automatically when the device was added to IMC. Deleting an individual monitor instance does not delete the global monitor setting.

To delete one or more monitor instances:

1. Navigate to Resource → Monitoring Settings:
   a. Click the Resource tab from the tabular navigation system on the top.
   b. Click the Performance Management link on the navigation tree on the left.
   c. Click Monitoring Settings under Performance Management from the navigation system on the left.
   The Monitor List appears.

2. To delete one or more monitor instances, do one of the following:
   o Click the checkbox ☑️ to the left of the device(s). Click Cancel Monitor at the top of the Monitor List to delete all the monitor instances of the selected devices, or
   o Click the Cancel link of a device whose instances you want to delete in the Operation column to delete all the monitor instances of the device, or
   o Click the Switch to Instance List link located in the upper right corner of the Monitor List. Click the checkbox ☑️ to the left of the instance(s) you want to delete. Click Cancel Monitor at the top of the Monitor List to delete all the selected monitor instances; or,
   o Click the Switch to Instance List link located in the upper right corner of the Monitor List. Click the Cancel link of the instance you want to delete in the Operation column to delete the monitor instance.

3. Click OK to confirm the deletion of the selected monitor instances.
   The page updates to reflect the results of the deletion.

4. Review the results of this operation in the Result table.

5. Check the Result field to verify that deleting the selected monitor instances succeeded:
   o If the task was successful, the Result field contains the content, ☑️ Succeeded, or
   o If the task failed, the Result field contains the content, ✗ Failed. Click the contents of this field to drill down for more information on the cause of the failure.

6. When you have finished reviewing the results of the task, click Back to return to the Monitor List.

Displaying monitored devices only

To display monitored devices only:

1. Navigate to Resource → Monitoring Settings:
   a. Click the Resource tab from the tabular navigation system on the top.
b. Click the **Performance Management** link on the navigation tree on the left.

c. Click **Monitoring Settings** under **Performance Management** from the navigation system on the left.

The **Monitor List** appears.

2. Click the checkbox \( \square \) to the left of **Only Display Monitored Devices** located in the upper right corner of the **Monitor List**.

The data in the **Monitor List** is refreshed, and only the monitored devices appear.

### Saving monitors to a performance view

A performance view is a collection of one or more charts that display the data collected by IMC for the configured monitors. IMC provides you with the ability to quickly and easily add one or more monitors to a new performance view or to existing performance views. For more information on adding monitors to a new or existing performance view, see "Creating a performance view" (page 625) and "Saving monitors to an existing performance view from the monitor settings page" (page 627).

### Modifying the default indices

IMC is configured to automatically gather performance data for all managed devices using a pre-defined set of monitors. Administrators and operators can customize this list of monitors by adding or removing monitors from the list. For more information on customizing the set of default monitors for devices managed by IMC, see "Configuring default monitor indices" (page 151).

### Viewing performance reports

IMC provides you with several avenues for viewing the performance data collected by monitors. The **Performance View** option under **Performance Management** enables you to customize views by choosing monitors to be included in a particular view. Once created, you can add a shortcut to the left navigation tree for quick and convenient access to the performance reports contained within a **Performance View**.

You can create new views directly from the **Monitor Settings** page, add selected monitors to an existing view from the Monitor Settings page, or create a new performance view from the **Performance View** list. You can also create folders to organize views.

### Accessing performance view list

All performance views are displayed in the **Performance View List**, allowing you to access and manage all aspects of any view.

To access the list of performance views:

1. Navigate to **Resource**→**Performance View**:
   a. Click the **Resource** tab from the tabular navigation system on the top.
   b. Click the **Performance Management** link on the navigation tree on the left.
   c. Click **Performance View** under **Performance Management** from the navigation system on the left.

   The **Performance View** page displays with the **Performance View List** on this page.

2. To view all performance views that have been added to the navigation tree, click the expand button \( \square \) to the left of the **Performance View** link on the left navigation tree.

**Performance view list**
Name: Contains the name for the performance view. The contents of this field also serve as a link for accessing the performance view.

Description: Contains the description for the associated performance view.

Creator: Contains the operator who created the performance view.

Creation Time: Contains the date and timestamp for the creation of the associated view.

Navigation Tree: Contains a link for adding the associated view to the left navigation tree or for removing it from the left navigation tree.

Delete: Contains a link for deleting the associated view. TopN view cannot be deleted.

Operation: Contains links for viewing, or modifying the associated view. To access these options, click the icon in the Operation field.

If the Performance View List contains multiple entries, the navigational aids shown below may display:

- Click to page forward in the Performance View List.
- Click to page forward to the end of the Performance View List.
- Click to page backward in the Performance View List.
- Click to page backward to the front of the Performance View List.

3. Click 8, 15, 50, 100, or 200 from the right side of the main pane to configure how many items per page you want to view.

4. For Performance View lists that have more than one page, click 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 … from the bottom right side of the main pane to jump to a specific page.

You can sort the Performance View list by the Name, Description, Creator, and Creation Time fields. Click the column label to sort the list by the selected field. The column label is a toggle switch that allows you to toggle between the various sort options specific to each field.

### Querying performance view list

To search the list of performance views for a specific performance view:

1. Navigate to Resource→Performance View:
   
   a. Click the Resource tab from the tabular navigation system on the top.
   b. Click the Performance Management link on the navigation tree on the left.
   c. Click Performance View under Performance Management from the navigation system on the left.

   The Performance View page displays with the populated Performance View List.

2. Enter the partial or complete name for the performance view in the Name field of the Query section.

3. Click Query.

   The page updates to display the results of your query in the Performance View List.

4. Review the results of your search.

5. Click Reset when you have finished your review of your query results and want to restore the full Performance View List.
Organizing performance views with folders

IMC offers you the ability to create as many performance views as needed to manage the ongoing task of network performance management. In large environments, you can easily create dozens of performance views to meet the needs of the network support organization.

In addition to the ability to create performance views, you can create folders to organize performance views. Performance view folders work the same way as do folders or directories in file systems, allowing you to create folders at the root level in addition to nesting folders within folders. You can group performance views by device type, location, or device function, just to name a few. As with performance views, there is no limit to the number of folders you can create.

Performance view subfolders are accessed by selecting their parent folder in the same way that subdirectories are accessed by double clicking the parent directory.

Creating a performance view folder

To create a performance view folder:

1. Navigate to Resource → Performance View:
   a. Click the Resource tab from the tabular navigation system on the top.
   b. Click the Performance Management link on the navigation tree on the left.
   c. Click Performance View under Performance Management from the navigation system on the left.
   The Performance View page displays with the populated Performance View List.

2. Click the Add Folder link located to the far right of the Performance View List.
   The Add Folder dialog box appears.

3. Enter a name for the performance view folder in the Name field.
   A valid length for the folder name is 1-32 characters.

4. Select the operator group to which you want to assign access rights for the folder by clicking the checkbox to the left of the operator group in the Access Right section.

5. Enter a description for this folder in the Description field.
   A valid length for the folder description is 0-128 characters.

6. Click OK to create the performance view folder and then do one of the following:
   o To drill down into a performance view folder, click the link in Name field for the performance view, or
   o To navigate up one level in performance view folders, click the Back to Upper Folder link located at the far right of the Performance View List.

Once you have created performance view folders, you are ready to begin adding performance views to them. Performance views are added to folders when they are created.

For information on creating performance views and adding them to folders, see "Creating a performance view from the monitor settings page" (page 626) and "Saving monitors to an existing performance view from the monitor settings page" (page 627).

Modifying a performance view folder

To modify a performance view folder:

1. Navigate to Resource → Performance View:
   a. Click the Resource tab from the tabular navigation system on the top.
b. Click the Performance Management link on the navigation tree on the left.

c. Click Performance View under Performance Management from the navigation system on the left. The Performance View page displays with the Performance View List populated.

2. Click the icon in the Operation field associated with the folder you want to modify.

3. Select Modify from the popup menu.

   The Modify Folder dialog box appears.

4. Modify the folder name as needed.

   A valid length for the folder name is 1-32 characters.

5. Select the operator group to which you want to assign access rights for the folder.

6. Modify the description as needed.

   A valid length for the folder description is 0-128 characters.

7. Click OK to modify the performance view folder.

Deleting a performance view folder

To delete a performance view folder:

1. Navigate to Resource → Performance View:

   a. Click the Resource tab from the tabular navigation system on the top.

   b. Click the Performance Management link on the navigation tree on the left.

   c. Click Performance View under Performance Management from the navigation system on the left. The Performance View page displays with the Performance View List populated.

2. Click the delete icon in the Delete field associated with the folder you want to delete.

3. Click OK to confirm your deletion of the selected performance view folder.

To delete a performance view folder, you must first delete all subfolders and performance views within it. For more information on deleting performance views, see “Deleting a performance view” (page 630).

Managing performance views

This section explains several ways to create a performance view and to modify and delete views.

Creating a performance view

A performance view is a collection of one or more charts that display the data collected by IMC for the configured monitors. You can add one or more monitors to a new or existing performance view.

To create a performance view:

1. Navigate to Resource → Performance View:

   a. Click the Resource tab from the tabular navigation system on the top.

   b. Click the Performance Management link on the navigation tree on the left.

   c. Click Performance View under Performance Management from the navigation system on the left. The Performance View page displays with the Performance View List populated.

2. Navigate to the folder that you want to add the new performance view to.

3. Click Add.
The Add Performance View page appears.

4. Enter the name for this performance view in the View Name field. A valid length for the folder name is 1-32 characters.

5. Select the operator group to which you want to assign access rights for the view by clicking the checkbox to the left of the operator group in the Access Right section.

6. Enter a description for this performance view in the Description field. A valid length for the folder description is 0-128 characters.

7. Add/delete monitor instances

8. Select one item from the Select Index list.

The index or indices appear under the selected item.

9. Click the checkbox to the left of each index as needed.

You cannot select indices from different items at one time. To view indices from multiple items, create the performance view for one item at a time and repeat your operation until you can view the desired indices.

10. Click Select Device.

The Select Devices dialog box appears.

You can add devices by using either the View or Advanced query option. See "Adding devices by View" (page 85) and "Adding devices by Advanced query" (page 85).

11. Highlight the device(s) you want to select and do one of the following:

   o To add the devices to the Selected Devices list, click Add selected , or
   o To select all of the devices displayed in the Devices Found list, click Add all , or
   o To remove one or more device(s), select them and click Remove selected , or
   o To remove all of the selected devices, click Remove all .

12. Confirm that the devices you want to select have been added.

13. Click OK.

14. Confirm that the devices now appear in the list below the Select Device button.

The unmonitored instances of the selected devices display in the list under the Select Device button after you have selected the index or indices of the instances.

15. Highlight the instance(s) you want to select and click Add to add them to the Result list at a time, or choose from the following:

   o To select all of the instances, click Add All , or
   o To remove one or more instances, select them and click Remove, or
   o To remove all of the selected instances, click Remove All.

16. Click OK to create the performance view.

Once a performance view is created, its location cannot be moved or modified. To change a performance view’s location, you must delete the old view and recreate a new view in the new folder.

Creating a performance view from the monitor settings page

From the Monitor Settings page, you can select monitor instances and then initiate the creation of a new performance view using the selected monitor instances.

To create a new performance view:
1. Navigate to Resource→Monitoring Settings:
   a. Click the Resource tab from the tabular navigation system on the top.
   b. Click the Performance Management link on the navigation tree on the left.
   c. Click Monitoring Settings under Performance Management from the navigation system on the left.
      The Monitor List appears.

2. Save monitor instances using one of the following methods:
   o Click the checkbox to the left of the device(s). Click Save Performance View at the top of the Monitor List. Select Save as New View to save all the monitor instances of the selected device(s) to a new performance view; or,
   o Click the Switch to Instance List link located in the upper right corner of the Monitor List. Click the checkbox to the left of the instance(s). Click Save Performance View at the top of the Monitor List. Select Save as New View to save the selected monitor instance(s) to a new performance view.
      The Add Performance View page appears. The selected instances are displayed in the Select Instance area.

3. Enter the name for this performance view in the View Name field.
   A valid length is 1-32 characters.

4. Select the folder you want to store this performance view from the Select Folder list.
   Performance view folders must be created before views can be added to them. For more information on creating performance view folders, see "Creating a performance view folder" (page 624).

5. Select the operator group to which you want to assign access rights for the view by clicking the checkbox to the left of the operator group in the Access Right section.

6. Enter a description for this performance view in the Description field.
   A valid length is 0-128 characters.

7. Add or delete monitor instances as outlined in "Creating a performance view" (page 625).

8. Click OK to create the new performance view.
   Once a performance view is created, its location cannot be moved or modified. To change a performance view’s location, you must delete the old view and recreate a new view in the new folder.
   Once you have created performance views, you can view them in the Performance View List. For more information, see "Viewing a performance view report" (page 630).

**Saving monitors to an existing performance view from the monitor settings page**

To add monitor instances to an existing performance view:

1. Navigate to Resource→Monitoring Settings:
   a. Click the Resource tab from the tabular navigation system on the top.
   b. Click the Performance Management link on the navigation tree on the left.
   c. Click Monitoring Settings under Performance Management from the navigation system on the left.
      The Monitor List appears.

2. Save monitor instances by using one of the following methods:
Click the checkbox to the left of the device(s). Click Save Performance View at the top of the Monitor List. Select Save to Existed View to save all the monitor instances of the selected device(s) to an existing performance view; or,

Click the Switch to Instance List link located in the upper right corner of the Monitor List. Click the checkbox to the left of the instance(s). Click Save Performance View at the top of the Monitor List. Select Save to Existed View to save the selected monitor instance(s) to an existing performance view.

The Select View dialog box appears.

3. Click the radio button to the left of the performance view you want to add the selected monitor instances to.

4. Click OK to add the selected monitor instances to the existing performance view.

Once you have added the monitor instances to the performance views, you can launch the views from the Performance View List. For more information on performance views, see “Viewing a performance view report” (page 630).

**Adding a performance view shortcut to the left navigation tree**

Once a performance view has been created, you can add it to the left navigation tree for quick access to it.

To add performance views to the left navigation tree:

1. Navigate to Resource → Performance View:
   a. Click the Resource tab from the tabular navigation system on the top.
   b. Click the Performance Management link on the navigation tree on the left.
   c. Click Performance View under Performance Management from the navigation system on the left.

   The Performance View page displays with the Performance View List populated.

2. Navigate to the folder that contains the performance view you want to add to the left navigation tree.

3. Click the Add link in the Navigation Tree field associated with the performance view you want to add to the left navigation tree.

   The Performance View option under Performance Management updates to display the new performance view. You may need to click the expand icon located to the left of the Performance View option as well as to the left of any performance view folders to view all performance views.

   If the performance view is in a folder, IMC adds the folder as well as the performance view to the left navigation tree.

**Removing a performance view shortcut from the left navigation tree**

To remove performance views from the left navigation tree:

1. Navigate to Resource → Performance View:
   a. Click the Resource tab from the tabular navigation system on the top.
   b. Click the Performance Management link on the navigation tree on the left.
   c. Click Performance View under Performance Management from the navigation system on the left.

   The Performance View page displays with the Performance View List populated.

2. Navigate to the folder that contains the performance view you want to remove from the left navigation tree.

3. Click the Cancel link in the Navigation Tree field associated with the performance view you want to remove from the left navigation tree.
The Performance View option under Performance Management updates with the performance view removed.

If all the performance views in a folder are removed from the left navigation tree, IMC removes the folder from the left navigation tree.

Modifying a performance view

To modify a performance view:

1. Navigate to Resource → Performance View:
   a. Click the Resource tab from the tabular navigation system on the top.
   b. Click the Performance Management link on the navigation tree on the left.
   c. Click Performance View under Performance Management from the navigation system on the left.
      The Performance View page displays with the Performance View List populated.

2. Navigate to the folder that contains the performance view you want to modify.

3. Click the icon in the Operation field associated with the performance view you want to modify.

4. Select Modify from the popup menu.
   The Modify Performance View page appears.

5. Enter the new name for this performance view in the View Name field.
   A valid length is 1-32 characters.

6. Select the operator group to which you want to assign access rights for the view by clicking the checkbox to the left of the operator group in the Access Right section.

7. Modify the description for this performance view in the Description field.
   A valid length is 0-128 characters.

8. Set monitor instances.

9. Select one of the items from the Select Index list.
   The index or indices appear under the selected item.

10. Click the checkbox to the left of each index as needed.
    You cannot select indices from different items at one time.

11. Click Select Device.
    The Select Devices dialog box appears.

12. Add devices by using either the View or Advanced query option. See "Adding devices by View" (page 85) and "Adding devices by Advanced query" (page 85).

13. Highlight the device(s) you want to select and do one of the following:
    o To add them to the Selected Devices list, click Add selected, or
    o To select all of the devices displayed in the Devices Found list, click Add all, or
    o To remove one or more device(s), select them and click Remove selected, or
    o To remove all of the selected devices, click Remove all.

14. Confirm that the devices you want to select have been added.

15. Click OK. Confirm that the devices now appear in the list below the Select Device button.
The unmonitored instances of the selected devices display in the list under the Select Device button after you have selected the indices of the instances.

16. Highlight the instance(s) you want to select and click Add to add them to the Select Result list at a time, or do one of the following:
   - To select all of the instances and click Add All, or
   - To remove one or more instances, select them and click Remove, or
   - To remove all of the selected instances, click Remove All.

17. Click OK to accept your modifications to the performance view.

Deleting a performance view

To delete a performance view:
1. Navigate to Resource → Performance View:
   a. Click the Resource tab from the tabular navigation system on the top.
   b. Click the Performance Management link on the navigation tree on the left.
   c. Click Performance View under Performance Management from the navigation system on the left.
      The Performance View page displays with the Performance View List populated.

2. Navigate to the folder that contains the performance view you want to delete.

3. Click the delete icon in the Delete field associated with the performance view you want to delete.

4. Click OK to confirm the deletion.

Viewing a performance view report

To view a performance view report:
1. Navigate to Resource → Performance View:
   a. Click the Resource tab from the tabular navigation system on the top.
   b. Click the Performance Management link on the navigation tree on the left.
   c. Click Performance View under Performance Management from the navigation system on the left.
      The Performance View page displays with the Performance View List populated.

2. Navigate to the folder that contains the performance view you want to view.

3. Click the performance view name you want to view from the Performance View List.

There are features that apply to all charts in the performance view report and features for individual graphs in the report.

Features that apply to all charts

- Modifying a Performance View’s Date Range: By default, the most recent data display using "Today" as the time range. To display reports for a specific date or time range, select the date from the Time Range list.
- Adding a View Format: You can add a view format in the pre-defined TopN performance view or in a user-defined performance view. See the individual sections below to add a view.

TopN Performance View

By default, the TopN Performance View only displays CPU Usage TopN, Memory Usage TopN, Device Response Time TopN, and Device Unreachability Proportion TopN. By adding a view format, you can speed up adding other monitor indices TopN.
a. Click the Add View Format link located in the upper right corner of the current report. The Add Format dialog box appears.
b. Enter a name for the new monitor in the Title field.
c. Click Add Index to select the monitor index or indices you want to add. The Select Index dialog box appears.
d. Click the expand arrow to the left of each monitor group to view all of the monitor indices.
e. Click the checkbox to the left of the monitor index or indices you want to add.
f. Click OK. The current performance view is updated to include the new monitor index or indices.

User-Defined Performance View

By adding the view format, you can collect the import data in a chart from several Performance Views.

a. Click the Add View Format link located in the upper right corner of the current report. The Add Format dialog box appears.
b. Enter a name for the new monitor in the Title field.
c. Click the checkbox to the left of the monitor instance(s) you want to monitor separately. The monitor instances displayed are instances that have already been configured for this device. If you want to add a monitor instance that is not on this list, you must add it using the Monitor Settings option. For more information on adding a monitor instance for one or more devices, see "Adding Monitor Instances" (page 617).
d. Click OK. The current performance view report is updated to include a new chart for monitoring the selected instance(s) separately.

• Save Position: You can reorder the charts displayed in the current report. Once you have moved the charts to the desired position(s), you can use the Save Position link to retain permanently the current order of the performance view report.
a. Click and hold the chart title bar using the left mouse button and drag the chart to the desired position.
b. Click the Save Position link located in the upper right corner of the current report. The page updates to display the results of the save position operation.

• Refresh: To refresh the data for the selected performance review report, click the Refresh link located in the upper right corner of the performance view report.

Features that apply to individual graphs

• Report: Within the report feature, you can change the default time range, print the report to PDF, and export the report in multiple file formats. To access the Report feature, click the icon located to the far right on the graph’s title bar. The Set Query Condition dialog box appears.
  o To display reports for a specific date or time range, select the date from the Time Range list. Click OK. IMC displays the graph for the selected time range in a new Intelligent Analysis Report Viewer window.
To print the report to PDF, click the print icon located on the toolbar on the top of the report, select the desired page range from **Page Range** and click **Export**.

To export the report, click the export icon located on the toolbar on the top of the report. Select the desired export file format from the **File Format** list, select the desired page range from **Page Range** and click **Export**.

- **Refresh**: This feature allows you to refresh the data for the associated graph. To access this feature, click the icon located to the far right on the graph’s title bar.

- **Modify Chart**: This feature allows you to select the chart type and modify its dimensions. This feature allows you to select the chart type as well as to modify its dimensions.
  
  - Click the icon located to the far right on the graph’s title bar.
    
    The **Modify Chart** dialog box appears.
  
  - Select the chart type from the **Chart Type** list.
  
  - Select TopN performance view or user-defined performance view:
    
    - Select the number of resources you want to report on in the TopN chart from the **Top N** list.
    
    - To enter your own value, select **Custom**.
    
    - Enter the number of resources you want to report on in the **Custom TopN** field provided.
    
    - Enter the width for the chart in the **Width** field.
    
    - Enter the height in the **Height** field.
    
    - Click **OK** to accept your changes.

  **Top N and user-defined performance view options differ:**
  
  - **TopN performance** view options include **TopN Table** and **TopN Bar Chart**. Chart type options may vary.
  
  - User-defined performance view options include **Line Chart**, **Bar Chart**, **Area Chart**, and **Gather Data**. Chart type options may vary.

- **Modify Instance**: This feature allows you to add or remove monitor instances for the associated graph. Do the following to add or remove a monitor instance:

  This feature allows you to add or remove monitor instances for the associated graph.
  
  - Click the icon located to the far right on the graph’s title bar.
    
    The **Modify Format** dialog box displays with monitor instances for devices grouped together under the device name.
  
  - Do one of the following:
    
    - Click the checkbox to the left of the monitor instance(s) you want to add, or
    
    - Click the checked box to the left of the monitor instance(s) you want to remove.
  
  - Click **OK** to accept your changes.

- **Delete**: This feature allows you to permanently remove a graph from a performance view.

  To delete the associated graph, click the icon located to the far right on the graph’s title bar.
  
  - Click **OK** to confirm deletion of the associated graph.
Managing IMC’s performance monitor settings for topology maps

IMC provides you with the ability to customize and view performance reporting on topology maps. Select device(s) in a topology map to view the performance data of the device(s) in a tip. With the Data Shown in Topo feature, you can customize the reports that appear on the topology maps, and add, modify, or remove monitors that are available on the topology map.

Accessing data shown in topo

All reports that are displayed on the topology map are listed in the Data Shown in Topo list. From this list, you can view, add, modify, or remove performance monitors for display on topology maps.

To access the data shown in topo:

1. Navigate to Resource → Data Shown in Topo:
   a. Click the Resource tab from the tabular navigation system on the top.
   b. Click the Performance Management link on the navigation tree on the left.
   c. Click Data Shown in Topo under Performance Management from the navigation system on the left.

The Data Shown in Topo page appears.

Data shown in topo list fields and explanations:

- Performance Index: Contains the name of the index or monitor.
- Applicable To: Identifies which devices on the topology map that the associated monitor can be applied to.
- Time Range: Contains range of data that is provided on the topology map for the associated performance monitor.
- Modify: Contains a link for modifying the topology map settings for the associated monitor.
- Delete: Contains a link for deleting the topology map settings for the associated monitor.

If the Data Shown in Topo list contains multiple entries, the following navigational aids may appear:

- Click to page forward in the Data Shown in Topo List.
- Click to page forward to the end of the Data Shown in Topo List.
- Click to page backward in the Data Shown in Topo List.
- Click to page backward to the front of the Data Shown in Topo List.
2. Click 8, 15, 50, 100, or 200 from the right side of the main pane to configure how many items per page you want to view.

3. For Data Shown in Topo lists that have more than one page, click on 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 … from the bottom right side of the main pane to jump to a particular page of the trap list.

You can sort the Data Shown in Topo list by the Performance Index, Applicable To, and Time Range fields. Click the column label to sort the list by the selected field. The column label is a toggle switch that allows you to toggle between the various sort options specific to each field.

Managing data shown in topo

IMC provides you with the ability to define which performance monitors are displayed on the Network Topology.

Adding a monitor to IMC’s network topology

To add a monitor to the Data Shown in Topo list for display on IMC’s topology maps:

1. Navigate to Resource→Data Shown in Topo:
   a. Click the Resource tab from the tabular navigation system on the top.
   b. Click the Performance Management link on the navigation tree on the left.
   c. Click Data Shown in Topo under Performance Management from the navigation system on the left.

The Data Shown in Topo page appears.

2. Click Add.

The Add/Modify Data Shown in Topo dialog box appears.

3. Select which device type displays the performance monitor from the Applicable to list.

The default device and default link options apply the topology settings to all devices and links regardless of type.

4. Select the performance monitor group you want to display on the topology maps from the first Performance Index list.

The option you select here filters the options available to you in the second Performance Index list to only those monitors that are available under the monitor you select here.

5. Select the individual performance monitor item you want to display on the topology maps from the second Performance Index list.

6. Select the time period you want IMC to display performance statistics for from the Time Range list.

7. Click OK to accept your changes.

Once you have added a performance monitor item to the Data Shown in Topo list, it becomes available for viewing on IMC’s Network Topology.

To view the data of the performance monitor item, click the device, hovering over it and the tip containing the performance data appears.

Modifying a monitor on IMC’s network topology

To modify a monitor on the Data Shown in Topo list:

1. Navigate to Resource→Data Shown in Topo:
   a. Click the Resource tab from the tabular navigation system on the top.
   b. Click the Performance Management link on the navigation tree on the left.
c. Click **Data Shown in Topo** under **Performance Management** from the navigation system on the left.

The **Data Shown in Topo** page appears.

2. Click the icon ⌫ in the **Modify** field for the performance monitor item you want to modify. The **Add/Modify Data Shown in Topo** dialog box appears.

You cannot modify the performance index.

3. Select which device type displays the performance monitor from the **Applicable to** list. The default device and default link options apply the topology settings to all devices and links regardless of type.

4. Select the performance monitor group you want to display on the topology maps from the first **Performance Index** list.

The option you select here filters the options available to you in the second **Performance Index** list to only those monitors that are available under the monitor you select here.

5. Select the individual performance monitor item you want to display on the topology maps from the second **Performance Index** list.

6. Select the time period you want IMC to display performance statistics for from the **Time Range** list.

7. Click **OK** to accept your changes.

**Deleting a monitor from IMC’s network topology**

To delete a monitor from the **Data Shown in Topo** list:

1. Navigate to **Resource** → **Data Shown in Topo**:
   a. Click the **Resource** tab from the tabular navigation system on the top.
   b. Click the **Performance Management** link on the navigation tree on the left.

   c. Click **Data Shown in Topo** under **Performance Management** from the navigation system on the left.

   The **Data Shown in Topo** page appears.

2. Click the icon ⌫ in the **Delete** field for the performance monitor item you want to delete.

3. Click **OK** to confirm the deletion of the selected monitor.

**Managing real-time performance monitor**

IMC provides you with the ability to monitor the real-time performance of key devices.

To display real-time performance data for easy management, IMC manages the data in three hierarchies:

- **Realtime Monitor** window: Provides the whole frame and the main window for displaying performance data. You can create monitors in the frame and view the data of each monitor in the main window.

- **Monitor**: Provides you with the ability to create monitor graphs in the monitor and group the real-time performance data. In a monitor, you can customize the number of monitor graphs to be displayed in a line, maximum number of data records for a monitor graph, data collection interval, and background color.

- **Monitor Graph**: Displays performance data in graphs for one or more devices.
Viewing real-time monitor window

To view the Realtime Monitor window:

1. Navigate to Resource → Real-time Monitor:
   a. Click the Resource tab from the tabular navigation system on the top.
   b. Click the Performance Management link on the navigation tree on the left.
   c. Click Realtime Monitor under Performance Management from the navigation system on the left.

   The Realtime Monitor window appears.

Real-time monitor window

- Monitor/Monitor graphs: The main pane in the Realtime Monitor window displays the history monitor and its monitor graph when you closed the window last time. The monitor graph does not display any history data and displays real-time performance data. The title of the Realtime Monitor window shows the name of the current monitor
- Tool bar: The tool bar is located on the top of the Real-time Monitor window. From the left to the right, the tool bar contains four configuration shortcuts and an icon Add Monitor Graph.

For more information on performing the four configuration options, see "Configuring monitor settings" (page 639).
For more information on adding a monitor graph, see "Adding a monitor graph" (page 640).

- Monitor List:

The Monitor List is located in the upper right corner of the Realtime Monitor window. You can click the Monitor List to add, delete, modify, or switch monitors. For more information, see "Managing Monitors" (page 636).

When you open the Realtime Monitor window that contains no monitor or monitor graph of a monitor, the following dialog box appears:

- If no monitor has been created for the Realtime Monitor window, an Add Monitor dialog box appears when you open the Realtime Monitor window. For more information on adding a monitor, see "Adding a monitor" (page XX).
- If a monitor has no monitor graph created in the Realtime Monitor window, an Add Monitor Graph dialog box appears when you open the Realtime Monitor window. For more information on adding a monitor graph, see "Adding a monitor graph" (page 640).

Managing Monitors

Monitors provide you with the ability to group realtime performance monitor data and view grouped data. The monitor also provides you with the ability to customize the number of monitor graphs to be displayed in a line, maximum number of data records for a monitor graph, data collection interval, and background color.

Viewing a monitor

Open the Realtime Monitor window to view the history monitor as when you closed the window last time. For more information on accessing a monitor, see "Viewing real-time monitor window" (page 636).
To switch to another monitor, click the Monitor List located in the upper right corner of the Realtime Monitor window and select the name of the desired monitor.

When you switch to another monitor, the performance monitor data from the previous monitor is cleared.

Adding a monitor

You can add one or more monitors in the Realtime Monitor window.

To add a Monitor:

1. Navigate to Resource→Realtime Monitor:
   a. Click the Resource tab from the tabular navigation system on the top.
   b. Click the Performance Management link on the navigation tree on the left.
   c. Click Realtime Monitor under Performance Management from the navigation system on the left.
   The Realtime Monitor window appears.

2. Click Monitor List located in the upper right corner of the Realtime Monitor window.

3. Select Add.

4. Enter a name for the monitor in the Monitor Name field.

5. Select an interval from the Poll Interval (sec.) list.
   Performance data of the monitor is collected at the specified interval and displayed in the Realtime Monitor window.

6. Select a record number from the Max. Records list.
   The record number specifies the maximum number of realtime performance data records that a monitor graph can display.

7. Select a color from the Background Color list.
   All monitor graphs in the monitor use the selected background color.

8. Select the column from the Columns list.
   The column specifies how many monitor graphs can be displayed in each line of the monitor.

9. Set the Access Right.

10. Click the checkbox to the left of the operator group(s) you want to add in the Access Right table.

11. Click the list in the Access Right field associated with the operator group.

12. Do one of the following:
    o Select Read Only to allow operators in an operator group only to view the current monitor and change the background color of the monitor graphs, or
    o Select Read/Write Only to allow operators to modify the current monitor and customize the four configuration items.

   You cannot cancel or modify the authorization of the administrator group and the operation group of the current operators for the monitor.

13. Click OK to create the new monitor.

Modifying a monitor

To modify a Monitor:
1. Navigate to Resource → Realtime Monitor:
   a. Click the Resource tab from the tabular navigation system on the top.
   b. Click the Performance Management link on the navigation tree on the left.
   c. Click Realtime Monitor under Performance Management from the navigation system on the left.
      The Realtime Monitor window appears.

2. Click Monitor List located in the upper right corner of the Realtime Monitor window.

3. Select Modify.
   The Modify Monitor dialog box appears.
   You cannot change the name of the Monitor.

4. Select an interval from the Poll Interval (sec.) list.
   Performance data of the monitor is collected at the specified interval and displayed in the Realtime Monitor window.

5. Select a record number from the Max. Records list.
   The record number specifies the maximum number of realtime performance data records that a monitor graph can display.

6. Select the color from the Background Color list.
   All monitor graphs in the monitor use the selected background color.

7. Select the column from the Columns list.
   The column specifies how many monitor graphs can be displayed in each line of the monitor.

8. Set the Access Right.

9. Do one of the following:

10. Click the checkbox [ ] to the left of the operator group(s) you want to add in the Access Right table.
    o Click the checked box [ ] to the left of the operator group(s) you want to cancel in the Access Right table.
    o Click the list in the Access Right field associated with the operator group.

11. Do one of the following:
    o Select Read Only, which allows the operators in an operator group only to view the current monitor and change the background color of the monitor graphs in the monitor, or
    o Select Read/Write, which allows the operators to modify the current monitor and customize the four configuration items.
    You cannot cancel or modify the authorization of the administrator group and the operation group of the current operators for the monitor.

12. Click OK to confirm your change.

Deleting a monitor

To delete a Monitor:

1. Navigate to Resource → Realtime Monitor:
   a. Click the Resource tab from the tabular navigation system on the top.
   b. Click the Performance Management link on the navigation tree on the left.
c. Click Realtime Monitor under Performance Management from the navigation system on the left.
   The Realtime Monitor window appears.

2. Click Monitor List located in the upper right corner of the Realtime Monitor window.
3. Select Delete.
4. Click Yes to confirm the deletion.

Configuring monitor settings

When adding or modifying a monitor, you can customize the number of monitor graphs to be displayed in a line, maximum number of data records for a monitor graph, data collection interval, and background color. The four configuration items are used to adjust the display of the monitor graphs in the monitor.

To configure the settings of a monitor:

1. Navigate to Resource → Realtime Monitor:
   a. Click the Resource tab from the tabular navigation system on the top.
   b. Click the Performance Management link on the navigation tree on the left.
   c. Click Realtime Monitor under Performance Management from the navigation system on the left.
      The Realtime Monitor window displays the history monitor and its monitor graphs as they were when you closed the window the last time.

2. Configure the Monitor:
   a. Specify the interval for refreshing the realtime performance data in monitor graphs by selecting the desired timer from the Poll Interval (sec.) list located in the top tool bar.
      Performance data of all the monitor graphs in the monitor are collected and displayed at the specified interval. The displayed data in the monitor graphs does not change when you are modifying the poll interval.
   b. Modify the maximum number of data records that a monitor graph can display by selecting the desired number from the Max. Records list located in the top tool bar.
      The number specifies the maximum number of realtime performance data records that a monitor graph can display. When the displayed records reach the maximum number, the earliest data is deleted to display new data. If the number of displayed data records in a monitor graph is bigger than the specified number N, the N records display.
   c. Specify the background color for all monitor graphs by selecting the desired color from the Background Color list located in the top tool bar.
      All monitor graphs in the monitor use the selected background color.
   d. Specify the number of monitor graphs displayed in each line of the monitor by selecting the desired number from the Columns list located in the top tool bar.
      The column specifies how many monitor graphs can be displayed in each line of the monitor. The four configuration items take effect for the current monitor only, not for all monitors.
      The settings of the four configuration items are automatically saved when you close and re-open the Realtime Monitor window.
Managing monitor graphs

A monitor graph displays performance monitor data for one or more devices.

Viewing Monitor Graphs

Open the Realtime Monitor window to the history monitor and its monitor graphs when you closed the window last time. For more information on accessing monitor graphs, see “Viewing real-time monitor window” (page 636).

A monitor graph has the graph name located in the upper left corner, buttons for folding up or unfolding the monitor graph in the upper right corner, a tool bar under the graph name, performance data table or graph under the tool bar, and monitor instances at the bottom of the monitor graph.

In the tool bar, you can modify the monitor graph by clicking the button, remove the monitor graph by clicking the button, and display the monitor graph in bar or line graph.

In the bar graph, the X-axis denotes the time, and the Y-axis denotes the performance data. The graph displays the performance data for one or more devices at a specified time.

Under the graph are the items of the monitor instance name, Current Value, Average Value, and Max Value. If there are several instances, the instances are distinguished by colors. If there are two or more monitor graphs in a line, the information of these items cannot be fully displayed. Point to an instance name to view the complete information for the instance.

All the monitor graphs in a monitor have the same poll interval, number of displayed data records, and background color. For more information on these options, see “Configuring monitor settings” (page 639).

Adding a monitor graph

You can add one or more monitor graphs to a monitor.

To add a Monitor Graph:
1. Navigate to Resource→Realtime Monitor:
   a. Click the Resource tab from the tabular navigation system on the top.
   b. Click the Performance Management link on the navigation tree on the left.
   c. Click Realtime Monitor under Performance Management from the navigation system on the left.
      The Realtime Monitor window appears.
2. Click the Add Monitor Graph button located in the top tool bar.
      The Add Monitor Graph dialog box appears.
3. Enter a name for the graph in the Graph Title field.
4. Enter a name for the monitor item of this graph in the Y-axis Name field.
5. Enter a unit for the monitor item of this graph in the Y-axis Unit field.
6. Add the monitor instance:
   a. Click the Add Monitor Instance button located on the top.
      The Monitor dialog box appears.
   b. Click the Select Device button located on the top.
      The Select Devices dialog box appears.
7. Add devices by **View** or by the **Advanced** query option. See "Adding devices by View" (page 85) and "Adding devices by Advanced query" (page 85).
   
a. Click the [Select Index](#) button located on the top.
   
The **Select Index** dialog box appears.

b. Expand the monitor group you want to select monitor items from by clicking the arrow icon  to the left of the monitor group.

c. Click the checkbox  to the left of the monitor item(s) you want to monitor.

d. Click **OK**.
   
A monitor graph can display data measured in one unit only. To display data correctly, select monitor items that are measured in the same unit for each monitor graph.

e. Expand the monitor instance by clicking the arrow icon  to the left of the device name in the **Monitor** dialog box.

f. Confirm that the monitor instances now appear in the **Device Name** field.

g. Click **OK**.

8. Do one of the following:
   
o. Click **OK** to create the new monitor graph, or

o. Click **Continue to Add** to create the new monitor graph and open another **Add Monitor Graph** dialog box.
   
   There is no performance monitor data in a new monitor graph.

**Modifying a monitor graph**

To modify a **Monitor Graph**:

1. Navigate to **Resource**→**Realtime Monitor**:
   
a. Click the **Resource** tab from the tabular navigation system on the top.

b. Click the **Performance Management** link on the navigation tree on the left.

   c. Click [Realtime Monitor](#) under **Performance Management** from the navigation system on the left.
   
   The **Realtime Monitor** window appears.

2. Click [](#) located in the top tool bar of the monitor graph you want to modify.

3. The **Config Monitor Graph** dialog box appears.

4. Enter a new name for the graph in the **Graph Title** field.

5. Enter a new name for the monitor item of this graph in the **Y-axis Name** field.

6. Enter a new unit for the monitor item of this graph in the **Y-axis Unit** field.

7. Do one of the following:
   
o. Click the [Add Monitor Instance](#) button located on the top to add the new monitor instances, or

o. Click the checkbox  of the monitor instance you want to delete.

8. Click the [Delete](#) button located on the top.

9. Click **Yes** to confirm the deletion.

10. Click **OK** to confirm your changes.
If you change the monitor instances in a monitor graph, the existing performance data in the monitor graph is cleared.

Deleting a monitor graph

To delete a Monitor Graph:

1. Navigate to Resource→Realtime Monitor:
   a. Click the Resource tab from the tabular navigation system on the top.
   b. Click the Performance Management link on the navigation tree on the left.
   c. Click Realtime Monitor under Performance Management from the navigation system on the left.
   The Realtime Monitor window appears.

2. Click located in the top tool bar of the monitor graph you want to modify.
   The Config Monitor Graph dialog box appears.

3. Enter a new name for the graph in the Graph Title field.

4. Enter a new name for the monitor item of this graph in the Y-axis Name field.

5. Enter a new unit for the monitor item of this graph in the Y-axis Unit field.

6. Do one of the following:
   o Click the Add Monitor Instance button located on the top to add the new monitor instances, or
   o Click the checkbox of the monitor instance you want to delete.

7. Click the Delete button located on the top.

8. Click Yes to confirm the deletion.

9. Click OK to confirm your changes.

Displaying a monitor graph

To display a monitor graph in bar graph:

   a. Click the Resource tab from the tabular navigation system on the top.
   b. Click the Performance Management link on the navigation tree on the left.
   c. Click Realtime Monitor under Performance Management from the navigation system on the left.
   The Realtime Monitor window appears.

2. Click located in the top tool bar of the monitor graph.

To display a monitor graph in line graph:

3. Navigate to Resource→Realtime Monitor:
   a. Click the Resource tab from the tabular navigation system on the top.
   b. Click the Performance Management link on the navigation tree on the left.
   c. Click Realtime Monitor under Performance Management from the navigation system on the left.
   The Realtime Monitor window appears.
4. Click  located in the top tool bar of the monitor graph.

**Folding up/unfolding a monitor graph**

1. Navigate to Resource→Realtime Monitor:
   a. Click the Resource tab from the tabular navigation system on the top.
   b. Click the Performance Management link on the navigation tree on the left.
   c. Click Realtime Monitor under Performance Management from the navigation system on the left.
      The Realtime Monitor window appears.

2. Do one of the following:
   o Click  located in the upper right corner of the monitor graph to fold up a monitor graph, or
   o Click  located in the upper right corner of the monitor graph to unfold a monitor graph.

**Managing performance option**

The Performance Option includes Display Option and Monitor Option. Display Option allows you to set the data unit. Monitor Option allows you to set which ports are to be monitored.

**Setting display option**

To set the display option:

1. Navigate to Resource→Options:
   a. Click the Resource tab from the tabular navigation system on the top.
   b. Click the Performance Management link on the navigation tree on the left.
   c. Click Performance Option under Performance Management from the navigation system on the left.
      The Performance Option page appears.

2. Click the Display Option tab in the Performance Option page.

3. Select the data unit option from the Data unit of bits/s list.
   The Adapt automatically option can automatically adjust the data unit based on the actual length of the data.

4. Click Set to confirm your change.

**Setting monitor option**

To set the monitor options:

1. Navigate to Resource→Performance Option:
   a. Click the Resource tab from the tabular navigation system on the top.
   b. Click the Performance Management link on the navigation tree on the left.
   c. Click Performance Option under Performance Management from the navigation system on the left.
      The Performance Option page appears:
2. Click the **Monitor Option** tab in the **Performance Option** page.
3. Select the types of interfaces to be monitored.
4. Select the types of interfaces to be monitored.
5. Select the checkbox for the target option.
   The options follow the logical OR rule. If an interface matches one option, the interface is to be monitored.
6. Click **Set** to confirm your change.
ACL Management allows you to view and configure existing ACLs on devices managed by IMC and to import ACLs into ACL Management as templates or resources. Once you have created ACL templates and resources, they can be used to create ACLs for deployment to other managed devices. ACL also has a deployment wizard that allows you to quickly deploy ACLs and ACL uses to manage devices. The deployment task management features allow you to monitor and manage deployment and removal of ACLs and ACL uses.

Rules are the core of an ACL. A rule contains conditions that define whether traffic is forwarded or filtered by a network device and includes a rule number, the action that is taken in the rule - whether traffic is permitted or denied, and a pattern for matching the contents of every packet to determine whether or not the packet is forwarded. The pattern to match can be an IP or MAC address or range of addresses and their masks and can include a Layer 4 TCP, UDP port number, or it can be a hexadecimal string and an offset value that identifies where in the packet to begin the pattern matching. Rules may also include identification of the protocol or type of traffic that the action is taken for and protocol specific configuration options. Rules can also include time ranges and options specific to the protocol identified in the rule or the type of ACL and rule. A rule set is a collection of individual rules that are identified by the rule set name. An ACL is a container for one or more rule sets. In ACL Management, an ACL includes the name or number that identifies the ACL (ACL Identifier), the type of ACL it is, and its name.

There are four types of ACLs that can be created in IMC and therefore also four types of templates:

- **Basic**: Allows you to create rules based on source IP addresses.
- **Advanced**: Allows you to create rules based on Layer 3 and Layer 4 information including IP source and destination addresses, TCP and UDP port information, and protocol specific options.
- **Link**: Allows you to create rules based Layer 2 information including MAC source and destination addresses, source VLAN and VLAN priority information as well as link layer protocol type.
- **User-Defined ACLs**: Enable you to define a hexadecimal pattern and mask and the offset in the packet header where pattern matching begins. When a pattern is matched, the actions specified in the rule in the ACL will be applied.

**ACL Template** in ACL Management is a container for the configuration options required to create an ACL and to maintain the template. An ACL template contains configuration information including the ACL template name and template description, the type of ACL it is, rules that define what actions are taken for each packet examined by the ACL, protocol specific configuration options, and time ranges during which the rules of the ACL are in effect. Once you have created an ACL template, you can import it into an ACL resource. Once ACL resources are created, they can be deployed to devices managed by IMC that support ACLs.

The **ACL Assistant** facilitates ACL template rule creation by modularizing some of the aspects of an ACL rule – services, network address groups, and time ranges. With Services, you define one or more TCP or UDP ports as a named service. With Net Address Groups, you can specify an IP address or range of IP addresses and their subnet mask. With Time Ranges, you specify a fixed or recurring date and time range. Once these are created using the Assistant, they become available for use when configuring rules for templates.

ACL Management offers you a rich feature set for simplifying the task of managing ACLs and their rule sets. Through the **ACL Resource** list, you have a single portal for viewing and managing all of the ACLs that can be deployed to network devices. From this list, you can view, add, rename and delete ACLs.

From the **ACL Resource** list, you can drill down into the **Rule Set List** to view every rule set for a given ACL. From the **Rule Set List** page, you can view information for every rule in a set. From this list, you can also take
action all of the rules in the list, including adding, modifying, copying, deploying, or deleting existing rule sets. From the Rule Set List, you can also import the contents of a template into a new rule set of an existing ACL.

ACL Management also provides features for rule management. You can redefine the order of appearance of rules in a rule set, which can be crucial to its effectiveness when the match order is based on the order of rule appearance. In addition, ACL Management can optimize rules in a rule set by making and implementing recommendations for reducing the effect of ACLs on network performance.

ACL Management also simplifies and streamlines the process of managing ACLs on devices. With ACL Management, you have a single portal for viewing and managing the ACL configurations for all devices that support ACLs. From the ACL Device List, you can view all devices that support ACLs as well as view detailed information the ACL configuration for a single device.

The ACL Device configuration page provides you with features for managing ACL configurations for the selected device. From this page, you can synchronize and refresh the ACL configuration data for the device as well as modify the ACL configuration polling interval. From the configuration page you can access the ACL Definitions tab to add or delete ACL definitions, export an ACL to a text file, and apply an ACL as a packet filter or VLAN packet filter to one or more interfaces on the device.

ACL Management’s ACL Deployment wizard provides you with a step-by-step process for successfully deploying ACLs, ACL uses for packet and VLAN filtering as well as removing ACLs and ACL uses. During the deployment task configuration process for each of these deployment types, IMC evaluates the selected devices and ACLs to determine whether or not the task can be executed successfully. IMC identifies when devices do not match the configuration selections and display warning messages and evaluation results to guide the successful deployment of ACL resources. In addition, ACL Management removes from the deployment configuration devices for which the selected action cannot be successfully executed. Lastly, the ACL Deployment wizard provides you with a facility for viewing and managing all deployment tasks via the ACL Deployment Task List.

The subnet mask inversion function simplifies the task of configuring IP subnets in ACL rules. You can enter an IP address and a subnet mask to identify an IP subnet. ACL Management automatically inverts the subnet mask into a wildcard mask when applying the configuration to devices. This section supposes that the subnet mask inversion function is enabled.

Simplifying ACL rule creation using the assistant

The ACL Assistant facilitates ACL template rule creation by modularizing various aspects of an ACL rule. With the ACL Assistant, you can create services, network address groups, and time ranges consisting of one or more entries. Once created, you can then apply the services, network address groups, and time ranges to one or more rules of any ACL template in ACL Management.

With **Services**, you define one or more ports that constitute a service and assign a name to the list of ports. Then, when creating a rule in a template, you assign the service to one or more rules, which defines the ports that are permitted or denied based on the parameters configured in the rule(s).

With **Net Address Groups**, you define a list of one or more IP address and subnet mask combinations. Then, the address group is assigned to one or more template rules in a template that are imported into ACL rule sets. The addresses specified in the net address groups become the source or destination addresses specified in the rules of an ACL.

With **Time Ranges**, you specify the fixed date and time ranges or recurring or cyclic time ranges specified by one or more days of the week that the rule takes effect. Operators can then assign the specified time range to one or more rules in a template.
With **Wildcard Mask**, or the subnet mask inversion function, you identify an IP subnet by specifying an IP address and a subnet mask. ACL Management automatically inverts the subnet mask into a wildcard mask when applying the configuration to devices.

### Managing services using the ACL assistant

In ACL Management, a service is a mnemonic for the TCP or UDP port configuration of a service, an application, or group of services or applications. Once you create a service in ACL Management using the **ACL Assistant**, you can refer to this service when configuring the port information in a template rule. Each service is comprised of a service name and a set of port numbers. For example, you can define a service called Telnet and specify port 23 as the port for the Telnet service. Or, you can create a service group that specifies one or more ports for one or more services or applications. For example, your organization has a network management application called "WatchIT" and the application uses ports in the range of 1001 to 1010. You can create a service called "WatchIT" and define the ports used by this application in the service. Once you have created the "WatchIT" service, you can specify its name in the **Variable Port** fields of an advanced ACL template rule configuration.

### Viewing the service list

To view the list of services in the ACL Assistant:

1. Navigate to **Service List**.
   a. Click the **Service** tab from the tabular navigation system on the top.
   b. Click the **ACL Management** icon located under the **Resource and Configuration Management** section of the **Service** tab.
   c. Click the **Assistant** link located under **ACL Management** on the navigation tree on the left.
   d. Click the **Service List** option located in the **Assistant Management** portion of the **Service List** page.

The **Service List** displays in the main pane of the page.

### Service list

- **Name**: Contains the name of the service.
  - This field serves as a link for navigating to the **View Service** page for the associated service. For more information the **View Service** option, see "Viewing a service" (page 647).
- **Description**: Contains a description for the associated service.
- **Modify**: Contains a link for modifying the associated service.

2. Click **8, 15, 50, 100**, or **200** from the right side of the main pane to configure the number of items per page you want to view.

You can sort the **Service List** by the **Name** and **Description** fields. Click the column label to sort the list by the selected field. The column label is a toggle switch that allows you to toggle between the various sort options specific to each field.

### Viewing a service

To view the details of a service in the ACL Assistant:

1. Navigate to **Service List**.
   a. Click the **Service** tab from the tabular navigation system on the top.
b. Click the **ACL Management** icon located under the **Resource and Configuration Management** section of the **Service** tab.

c. Click the **Assistant** link located under **ACL Management** on the navigation tree on the left.

d. Click the **Service List** option located in the **Assistant Management** portion of the **Service List** page.
   
The **Service List** displays in the main pane of the page.

2. Click the service name in the **Name** field.
   
The **View Service** page appears.

### Service list

- **Name**: Contains the name of the service.
- **Description**: Contains a description for the associated service.
- **Port List**: Contains a list of all UDP or TCP ports specified for this service.

### Adding a service to the service list

To add a service to the Service List using the ACL Assistant:

1. Navigate to **Service List**.
   
a. Click the **Service** tab from the tabular navigation system on the top.
   
b. Click the **ACL Management** icon located under the **Resource and Configuration Management** section of the **Service** tab.
   
c. Click the **Assistant** link located under **ACL Management** on the navigation tree on the left.
   
d. Click the **Service List** option located in the **Assistant Management** portion of the **Service List** page.
   
The **Service List** displays in the main pane of the page.

2. Click **Add**.
   
The **Add Service** page appears.

3. Enter a name for the service in the **Name** field.
   
   A valid length is 1-32 characters. A service name cannot begin with a number.

4. Enter a brief description for the service in the **Description** field.

5. Enter a port number in the **Port** field.
   
   A valid port entry includes a port number in the range from 0-65535.

6. Click **Add**.

7. Do one of the following:
   
   - To enter more than one port, repeat **Step 5**, or
   - To remove a port number, select the port and click **Delete**, or
   - To remove all ports in the list, click **Delete All**.

8. Click **OK** to create the service.
Once you have created a service, you can enter it in the Variable Port field when you have selected TCP or UDP as the protocol for an Advanced rule when creating an ACL template. For more information using a service when defining a rule in an ACL template, see “Creating ACL templates” (page 661).

Modifying a service in the service list

To modify a service in the Service List using the ACL Assistant:

1. Navigate to Service List.
   a. Click the Service tab from the tabular navigation system on the top.
   b. Click the ACL Management icon located under the Resource and Configuration Management section of the Service tab.
   c. Click the Assistant link located under ACL Management on the navigation tree on the left.
   d. Click the Service List option located in the Assistant Management portion of the Service List page.
      The Service List displays in the main pane of the page.

2. Click the icon in the Modify field associated with the service you want to modify.
   The Modify Service page appears.
   You cannot modify the name of a service once the service has been created.
3. Modify the description for the service as needed in the Description field.
4. To add a port number to the existing list, enter the new port number in the Port field.
   A valid port entry includes port numbers in the range from 0-65535.
5. Click Add.
6. Do one of the following:
   o To enter more than one port, repeat Steps 4-5, or
   o To remove a port number, select the port and click Delete, or
   o To remove all ports in the list, click Delete All, or
   o To enter more than one port, repeat this step, or
   o To remove a port number, select the port. Click Delete, or
   o To remove all ports in the list, click Delete All.
7. Click OK to accept your modifications to the service.

Deleting a service in the service lists

To delete a service using the ACL Assistant:

1. Navigate to Service List.
   a. Click the Service tab from the tabular navigation system on the top.
   b. Click the ACL Management icon located under the Resource and Configuration Management section of the Service tab.
   c. Click the Assistant link located under ACL Management on the navigation tree on the left.
d. Click the Service List option located in the Assistant Management portion of the Service List page.

   The Service List displays in the main pane of the page.

2. Click the checkboxes to the left of the service name for the service(s) you want to delete.
3. Click Delete.
4. Click OK to confirm the deletion of the selected service(s).

Managing net address groups using the ACL assistant

In ACL Management, a Net Address Group is mnemonic for one or more IP address/subnet mask combinations. Once you have created a Net Address Group in ACL Management using the ACL Assistant, you can specify it when configuring source or destination IP addresses and subnet masks in a template rule.

Each Net Address Group is composed of a group name and a set of IP addresses and their subnet masks. For example, you can define a Net Address Group called NetMgmt and specify one or more of the IP addresses for your organization’s network management subnets or servers and their subnet masks in the Net Address Group called NetMgmt. Once you have created the Net Address Group, you can specify its name in ACL resource when use an ACL template to create creating an ACL.

Viewing the net address group list

To view the Net Address Group List in the ACL Assistant:

1. Navigate to Net Address Group List:
   a. Click the Service tab from the tabular navigation system on the top.
   b. Click the ACL Management icon located under the Resource and Configuration Management section of the Service tab.
   c. Click the Assistant link located under ACL Management on the navigation tree on the left.
   d. Click the Net Address Group List option located in the Assistant Management portion of the Service List page.

   The Net Address Group List page displays in the main pane of the page.

Net address group list

   o Name: Contains the name of the Net Address Group.
     This field serves as a link for navigating to the View Network Address Group page for the associated Net Address Group. For more information on the View Network Address Group option, see "Viewing a network address group" (page 651).
   o Description: Contains a description for the associated Net Address Group.
   o Modify: Contains a link for modifying the associated Net Address Group.

2. Click 8, 15, 50, 100, or 200 from the right side of the main pane to configure the number of items per page you want to view.

   You can sort the Net Address Group List by the Name and Description fields. Click the column label to sort the list by the selected field. The column label is a toggle switch that allows you to toggle between the various sort options specific to each field.
Viewing a network address group

To view the details for a Net Address Group in the ACL Assistant:

1. Navigate to **Net Address Group List**:
   a. Click the **Service** tab from the tabular navigation system on the top.
   b. Click the **ACL Management** icon located under the **Resource and Configuration Management** section of the **Service** tab.
   c. Click the **Assistant** link located under **ACL Management** on the navigation tree on the left.
   d. Click the **Net Address Group List** option located in the **Assistant Management** portion of the **Service List** page.

   The **Net Address Group List** page displays in the main pane of the page.

2. Click the Net Address Group name in the **Name** field.

   The **View Network Address Group** page appears.

   **Network address group**
   - Name: Contains the name of the Net Address Group.
   - Description: Contains a description for the associated Net Address Group.
   - IP Address/Mask List: Contains a list of all of the IP addresses and their subnet masks in the Net Address Group.

Adding a network address group:

To add a Net Address Group:

1. Navigate to **Net Address Group List**:
   a. Click the **Service** tab from the tabular navigation system on the top.
   b. Click the **ACL Management** icon located under the **Resource and Configuration Management** section of the **Service** tab.
   c. Click the **Assistant** link located under **ACL Management** on the navigation tree on the left.
   d. Click the **Net Address Group List** option located in the **Assistant Management** portion of the **Service List** page.

   The **Net Address Group List** page displays in the main pane of the page.

2. Click **Add**.

   The **Add Network Address Group** page appears.

3. Enter a name for the Net Address Group in the **Name** field.
   A valid length is 1-32 characters. A Net Address Group name cannot begin with a number.

4. Enter a brief description for the Network Address Group in the **Description** field.

5. Enter an IP address/subnet mask combination in the **IP Address/Mask** field.
   The subnet mask must be entered using either CIDR or dotted decimal notation. A valid IP address/subnet mask using dotted decimal notation would be 192.168.1.0/255.255.255.0
A valid IP address/subnet mask using CIDR would be 192.168.1.0/24

6. Click Add.

7. Do one of the following:
   o To add more than one IP address/subnet mask combinations, repeat Step 5-6, or
   o To remove an IP address/subnet mask combination, select the Net Address Group and click Delete, or
   o To remove all IP address/subnet mask combinations in the list, click Delete All.

8. Click OK to create the Net Address Group.

Once you have created a Net Address Group, you can enter it in the Variable Address field of a rule configuration when creating an ACL template. For more information using a Net Address Group when defining a rule in an ACL template, see "Creating ACL templates" (page 661).

Modifying a network address group

To modify a Net Address Group:

1. Navigate to Net Address Group List:
   a. Click the Service tab from the tabular navigation system on the top.
   b. Click the ACL Management icon located under the Resource and Configuration Management section of the Service tab.
   c. Click the Assistant link located under ACL Management on the navigation tree on the left.
   d. Click the Net Address Group List option located in the Assistant Management portion of the Service List page.

   The Net Address Group List page displays in the main pane of the page.

2. Click the icon in the Modify field associated with the Net Address Group you want to modify.

   The Modify Network Address Group page appears.

   You cannot modify the name of a Net Address Group once it has been created.

3. Modify the description for the Net Address Group in the Description field.

4. To add a new IP address/subnet mask combination, enter it in the IP Address/Mask field.

   The subnet mask must be entered using either CIDR or dotted decimal notation. A valid IP address/subnet mask using dotted decimal notation would be 192.168.1.0/255.255.255.0

   A valid IP address/subnet mask using CIDR would be 192.168.1.0/24

5. Click Add.

6. Do one of the following:
   o To add more than one IP address/subnet mask combinations, repeat Steps 4 – 5, or
   o To remove an IP address/subnet mask combination, select the IP address/subnet mask combination and click Delete, or
   o To remove all IP address/subnet mask combinations in the list, click Delete All.
7. Click OK to modify the Net Address Group.
   Once you have created or modified a Net Address Group, you can enter it in the Variable Address field of a rule configuration when creating an ACL template. For more information using a Net Address Group when defining a rule in an ACL template, see "Creating ACL templates" (page 661).

Deleting a network address group

To delete a Net Address Group:
1. Navigate to Net Address Group List:
   a. Click the Service tab from the tabular navigation system on the top.
   b. Click the ACL Management icon located under the Resource and Configuration Management section of the Service tab.
   c. Click the Assistant link located under ACL Management on the navigation tree on the left.
   d. Click the Net Address Group List option located in the Assistant Management portion of the Service List page.
      The Net Address Group List page displays in the main pane of the page.
2. Click the checkboxes to the left of the Net Address Groups you want to delete.
3. Click Delete.
4. Click OK to confirm the deletion of the selected Net Address Groups.

Managing time ranges using the ACL assistant

In ACL Management, a Time Range is a mnemonic for a time range definition that you can apply to a rule in an ACL template. Once you have created a time range using the ACL Assistant, you can refer to this named time range when configuring the time range for a rule.

Each time range is comprised of a name, a description and a starting and ending date and time. For example, you can define a time range called "workweek" and specify the days Monday through Friday. Once you have created the named time range, you can specify its name in the Time Range field of an ACL template rule configuration.

Viewing the time range list

To view the Time Range List in the ACL Assistant:
1. Navigate to Time Range List:
   a. Click the Service tab from the tabular navigation system on the top.
   b. Click the ACL Management icon located under the Resource and Configuration Management section of the Service tab.
   c. Click the Assistant link located under ACL Management on the navigation tree on the left.
   d. Click the Time Range List option located in the Assistant Management portion of the Service List page.
      The Time Range List displays in the main pane of the page.

Time Range List
To view the details of an individual Time Range:

1. Navigate to Time Range List:
   a. Click the Service tab from the tabular navigation system on the top.
   b. Click the ACL Management icon located under the Resource and Configuration Management section of the Service tab.
   c. Click the Assistant link located under ACL Management on the navigation tree on the left.
   d. Click the Time Range List option located in the Assistant Management portion of the Service List page.

   The Time Range List displays in the main pane of the page.

2. Click the Time Range name in the Name field for the time range for which you want to view individual details.

The View Time Range page appears.

Time Range field

- **Name**: Contains the name assigned to this time range.
- **Description**: Contains a description for the associated time range.
- **Start Time**: Contains the date and time stamp for the time at which the rule configured with this time range takes effect.
- **End Time**: Contains the date and time stamp for the time at which the rule configured with this time range is no longer in effect.
- **Type**: Identifies the type of time range. There are two types of time ranges, Fixed and Cyclic.
- **Execution Period**: For Cyclic time ranges, identifies the recurring days during which the time range is in effect. If the time range is Fixed, this field is empty.

Adding a time range

To add a Time Range:

1. Navigate to Time Range List:
   a. Click the Service tab from the tabular navigation system on the top.
b. Click the ACL Management icon located under the Resource and Configuration Management section of the Service tab.

c. Click the Assistant link located under ACL Management on the navigation tree on the left.

d. Click the Time Range List option located in the Assistant Management portion of the Service List page. The Time Range List displays in the main pane of the page.

2. Click Add. The Add Time Range page appears.

3. Enter a name for the Time Range in the Name field. A valid length is 1 – 32 characters. The name must begin with a letter (A-Z, a-z). Spaces and question marks are not permitted in a Time Range name.

4. Enter a brief description for the time range in the Description field.

5. Click Add to enter the time range. The Add Time Range dialog box appears.

6. Select the type of time range you want to create by clicking the radio button ☐ to the left of the desired time range type:
   o Fixed if you want to identify a specific and finite start and end date and time, or
   o Cyclic if you want the time range to recur for selected days of the week.

7. See "Configuring fixed time ranges" (page 655) to configure fixed time ranges and "Configuring cyclic time ranges" (page 656) to configure cyclic time ranges.

**Configuring fixed time ranges**

1. Do one of the following to populate the start time field:
   o Enter the start time for the time range in the From field. A valid format for date and time is YYYY-MM-DD hh:mm where YYYY refers to the four-digit year, MM refers two-digit month, DD refers to the two-digit day, hh refers to the two-digit hour, and mm refers to the two-digit minute values.

   b. Click the calendar icon ☑ located to the right. A popup calendar appears.
      o Select the start date from the calendar.
      o Enter the time in the Time fields provided below the calendar.

2. Do one of the following to populate the end time field:
   o Enter the end time for the time range in the To field, or
     A valid format for date and time is YYYY-MM-DD hh:mm where YYYY refers to the four-digit year, MM refers two-digit month, DD refers to the two-digit day, hh refers to the two-digit hour, and mm refers to the two-digit minute values.

   o Click the calendar icon ☑ located to the right.
     A popup calendar appears.
   o Select the end date from the calendar.
Enter the time in the **Time** fields provided below the calendar.

3. Click **OK**.

4. To add more **Fixed** time ranges, repeat Steps 1 - 3 for each time range you want to add.

**Configuring cyclic time ranges**

1. If you selected **Cyclic** as the time range type, select from the following:
   - **All Time**: Includes every day of the week.
   - **Workday**: Includes days of the work week only, which includes Monday, Tuesday, Wednesday, Thursday, and Friday.
   - **Weekend**: Excludes days of the work week and includes the weekend days only, Saturday and Sunday.
   - **Customizing Time**: Allows you to select one or more days of the week, by clicking the checkbox □ to the left of the each day.

2. Enter the start time for the time range in the **From** field.
   
   A valid format for time is hh:mm where hh refers to the two-digit hour and mm refers to the two-digit minute values.

3. Enter the end time for the time range in the **To** field.
   
   A valid format for time is hh:mm where hh refers to the two-digit hour and mm refers to the two-digit minute values.

4. Click **OK**.

5. To add more **Cyclic** time ranges, repeat Steps 1-4 for each time range you want to add.
   
   Up to twelve time periods are allowed for Fixed time ranges. Thirty-two time periods are permitted for Cyclic time ranges.

6. To remove a time range, do one of the following:
   
   o To remove a time range, click on the checkbox □ to the left of the time range name and click **Delete**, or
   
   o To delete all time ranges, click on the checkbox □ to the left of **Start Time** and click **Delete**.

7. Click **OK** to create the Time Range.

   Once you have created a Time Range, you can enter it in the **Time Range** field of a rule configuration when creating an ACL template. For more information using a Time Range when defining a rule in an ACL template, see “Creating ACL templates” (page 661).

**Modifying time range**

To modify a Time Range:

1. Navigate to **Time Range List**.
   
   a. Click the **Service** tab from the tabular navigation system on the top.

   b. Click the **ACL Management** icon located under the **Resource and Configuration Management** section of the **Service** tab.

   c. Click the **Assistant** link located under **ACL Management** on the navigation tree on the left.

   d. Click the **Time Range List** option located in the **Assistant Management** portion of the **Service List** page.

   The **Time Range List** displays in the main pane of the page.
2. Click the icon in the Modify field associated with the Time Range you want to modify. The Modify Time Range page appears.

You cannot modify the name of a Time Range once it has been created.

3. Modify the description for the time range as needed in the Description field.

4. To add a new time range to the existing list, click Add. The Add Time Range dialog box appears.

5. Do one of the following:
   - Select Fixed if you want to identify a specific and finite start and end date and time, or
   - Select Cyclic if you want the time range to recur for selected days of the week.

6. See "Configuring fixed time ranges" (page 655) to configure fixed time ranges and "Configuring cyclic time ranges" (page 656) to configure cyclic time ranges.

Deleting a time range

To delete one or more Time Ranges:

1. Navigate to Time Range List:
   a. Click the Service tab from the tabular navigation system on the top.
   b. Click the ACL Management icon located under the Resource and Configuration Management section of the Service tab.
   c. Click the Assistant link located under ACL Management on the navigation tree on the left.
   d. Click the Time Range List option located in the Assistant Management portion of the Service List page. The Time Range List displays in the main pane of the page.

2. Click the checkboxes to the left of the Time Ranges you want to delete.

3. Click Delete.

4. Click OK to confirm the deletion of the selected Time Ranges.

Configuring subnet mask type for ACL management

In ACL Management, the subnet mask inversion function allows you to identify an IP subnet by entering an IP address and a subnet mask. ACL Management automatically inverts the subnet mask into a wildcard mask when applying the ACL configuration to devices. You can select subnet mask types as needed, including Enable Subnet Mask Inversion and Enable Wildcard Mask.

To configure subnet mask type for ACL management:

1. Click the Service tab from the tabular navigation system on the top.

2. Click the ACL Management icon located under the Resource and Configuration Management section of the Service tab.

3. Click the Options link located under ACL Management on the navigation tree on the left.

4. Check the radio button to the left of Enable Subnet Mask Inversion and Enable Wildcard Mask to select the option you want to apply. (The default option is Enable Wildcard Mask.)
Enable Subnet Mask Inversion: When this option is selected, ACL management inverts the wildcards configured on devices into subnet masks for display in IMC. During device configuration, ACL management inverts an input subnet mask into a wildcard mask. The subnet mask is a 32-bit binary represented in dotted decimal notation, where the 1 bits represent do care bits and the 0 bits represent don’t care bits.

Enable Wildcard Mask: When this option is selected, ACL management displays wildcards as configured on the device in IMC. During device configuration, ACL management applies the mask specified during ACL configuration as is, without inversion. Also called represent do care bits, and the 1 bits represent don’t care bits.

After you change the options, go to the ACL device page to synchronize ACL devices.

5. Click OK.

Managing ACL templates in IMC

ACL Templates in ACL Management are a container for the configuration options required to create an ACL or to maintain the template. The ACL template contains configuration and can be imported into an ACL resource. Resources are ACLs that contain one or more rule sets and can be deployed to devices managed by IMC that support ACLs.

Rules, which are grouped to form rule sets, are the core of an ACL. A rule contains conditions that define whether or not traffic is forwarded by a device or not. A rule includes a rule number, the action that to be taken in the rule- whether traffic is permitted or denied, and a pattern for matching against the contents of every packet to determine whether or not the packet is forwarded. The pattern to match can be an IP or MAC address, range of addresses and their masks or a Layer 4 port number, or a hexadecimal string and an offset value that identifies where in the packet to begin the pattern matching. Rules may also include identification of the protocol or type of traffic that the action to be taken for and protocol specific configuration options. Rules can also include time ranges and options specific to the protocol identified in the rule or the type of ACL and rule.

There are four types of ACLs that can be created in IMC and therefore four types of templates:

- **Basic**: Allows you to create rules based on source IP addresses.
- **Advanced**: Allows you to create rules based on Layer 3 and Layer 4 information including IP source and destination addresses, TCP and UDP port information, and protocol specific options.
- **Link**: Allows you to create rules based on Layer 2 information including MAC source and destination addresses, VLAN priority information as well as link layer protocol type.
- **User-Defined**: Allows you to define a hexadecimal pattern and mask and the offset in the packet header where pattern matching begins. When a pattern is matched, the actions specified in the rule in the ACL template are applied. A valid numeric range for assigning ACL Identifiers to user-defined ACLs is 5000-5999.

Creating templates in ACL management

To create templates in ACL Management:

1. Define the Services, Net Address Groups, and Time Ranges using the Assistant in the configuration ACL templates.
2. Create an ACL template using the services, Net Address Groups and Time Ranges created in the Assistant to configure many of the template’s options, including rule sets in the template.
3. Modify options, copy templates, import into an existing ACL.
4. Deploy to one or more devices using the ACL Deployment wizard.
Viewing ACL templates

The ACL Management provides you with a single portal for accessing all ACL templates. From the Template List, you can view a list of all ACL templates as well as navigate to the View Template page for viewing detailed information for each ACL template. From this page, you can navigate to the View Rule page for viewing detailed information for every rule in an ACL template.

Viewing the template list

To view the list of ACL templates:

1. Navigate to ACL Template:
   a. Click the Service tab from the tabular navigation system on the top.
   
   b. Click the ACL Management icon located under the Resource and Configuration Management section of the Service tab.
   
   c. Click the ACL Template link located under ACL Management on the navigation tree on the left. The Template List displays in the main pane of the page.

2. To filter the Template List by template type, select the template type you want to filter for from the Template Type list located in the upper right corner of the Template List.

Template list

- **Template Name**: Contains the name for the ACL template. The template name serves as a link for navigating to the View Template page for the associated template. For more information on the viewing the details of a template, see "Viewing ACL templates" (page 659).
- **Type**: Contains the ACL template type for the associated template. There are four types of templates in IMC: Basic, Advanced, Link, or User-Defined.
- **Template Description**: Contains a description for the associated template.
- **Match Order**: Contains the match order type for the associated Rule. The Match Order can either be Config or Auto.

- **Modify**: Contains a link for modifying the associated ACL.
- **Copy**: Contains a link for copying the associated ACL.
- **Export**: Contains a link for exporting the associated ACL.

If the Template List contains multiple entries, the following navigational aids may appear:

- Click \[
\]
  to page forward in the Template List.

- Click \[
\]
  to page forward to the end of the Template List.

- Click \[
\]
  to page backward in the Template List.

- Click \[
\]
  to page backward to the front of the Template List.

3. Click 8, 15, 50, 100, or 200 from the right side of the main pane to configure how many items per page you want to view.

You can sort the Template List by the Template Name, Type, Template Description and Match Order fields. Click the column label to sort the list by the selected field. The column label is a toggle switch that allows you to toggle between the various sort options specific to each field.
Viewing an ACL template

To view the contents of an individual template:

1. Navigate to ACL Template:
   a. Click the Service tab from the tabular navigation system on the top.
   b. Click the ACL Management icon located under the Resource and Configuration Management section of the Service tab.
   c. Click the ACL Template link located under ACL Management on the navigation tree on the left. The Template List displays in the main pane of the page.

2. Click the name in the Template Name field.
   The View Template page appears. The content of the page varies based on the template style.

Basic info
   - Template Name: Contains the name for the ACL template.
   - Type: Contains the ACL template type for the associated template. There are four types of templates in IMC: Basic, Advanced, Link, or User-Defined.
   - Match Order: Contains the match order type for the associated rule. The Match Order can either be Config or Auto.
   - Template Description: Contains a description for the associated template.

Rule maintenance field names and explanations:
   - No.: Contains the sequence or rule number for the associated rule in the Rule Set. The value in the sequence field serves as a link for navigating to the View Rule page for the associated rule. This page displays rule configuration information for the associated rule. For more information viewing rule information, see "Viewing ACL templates" (page 659).
   - Action: Contains the access control action specified in the associated rule. Actions include permit and deny.
   - Time Range: Contains the name assigned to the Time Range specified for the associated rule.
   - Source Address: Contains the source address specified in the associated rule for which the action is taken. For example, if the action is to permit IP traffic, this field identifies the source IP address from which IP traffic is permitted. Source Address is available for basic and advanced ACL templates.
   - Protocol: Contains the protocol specified in the associated rule for which the action is taken. Protocol is available for advanced ACL templates.
   - Destination Address: Contains the destination address specified in the associated rule for which the action is taken. For example, if the action is to permit IP traffic, this field identifies the destination IP address to which IP traffic is permitted. Destination Address is available for advanced ACL templates.
   - Source Mac Addr: Contains the source MAC address specified in the associated rule for which the action is taken. For example, if the action is to permit traffic, this field identifies the source MAC address from which traffic is permitted. Source Mac Addr is available for link ACL templates.
   - Destination Mac Addr: Contains the destination MAC address specified in the associated rule for which the action is taken. For example, if the action is to permit traffic, this field identifies the destination MAC address from which traffic is permitted. Destination Mac Addr is available for link ACL templates.
Matching String: Contains the hexadecimal string to be matched in a packet, the mask, and the offset values for a user-defined pattern-matching rule. Matching String is available for user-defined ACL templates.

Creating ACL templates

ACL templates enable you to create containers for the configuration options of an ACL. ACLs contain rules sets and other ACL attributes that define whether or not packets are forwarded or dropped by network devices. Once a template is created, you can import templates into existing ACLs for simplifying the process of ACL creation and management. Once an ACL has been created in ACL Management, it can then be deployed to one or more devices using the ACL Deployment wizard. For more information, see “Managing ACL templates in IMC” (page 658).

Creating a basic ACL template

Basic ACLs enable you to create one or more rules based on source IP addresses and subnet masks. A valid numeric range for assigning ACL Identifiers to basic ACLs is 1-99, 1300-1999, or 2000-2999.

To create a basic ACL template:

1. Navigate to ACL Template:
   a. Click the Service tab from the tabular navigation system on the top.
   b. Click the ACL Management icon located under the Resource and Configuration Management section of the Service tab.
   c. Click the ACL Template link located under ACL Management on the navigation tree on the left. The Template List displays in the main pane of the page.

2. Click Add.

3. Enter the name for the template in the Template Name field.
   A valid length for a template name is 1-32 characters. A template name cannot begin with a number or a space.

4. Select a Type field to define the type of ACL template to create.
   Options include Basic, Advanced, Link, and User-Defined. Select Basic from the Type list.

5. Select the match order you want to apply to this ACL template by clicking the radio button to the left of the Match Order option you want to use. Options include Config and Auto.
   If you select Config, IMC matches rules in the order in which they were configured. This feature works only for the devices that support it. If you select Auto, IMC matches rules based on the principle of depth priority.

6. Enter a brief description for this ACL template in the Template Description field.

7. Click Add Rule to add a rule to the ACL template.
   The Add Basic Rule page appears.

8. Select the action you want to take by clicking the radio button to the left of the option you want to apply to this rule:
   o Select permit if, upon matching the specified conditions, the packet should be forwarded, or
   o Select deny if, upon matching the specified conditions, the packet should be discarded.

9. Enter a named variable for this ACL template in the Time Range field which allows you to create a named variable without requiring you enter the time range in the template.
The named variable then serves as a placeholder for **Time Range** you created using the **Assistant** combination when you import the template as a rule set into an existing ACL.

10. Select the source IP address option you want to use by clicking the radio button ○ to the left of the desired option in the **Source Address** field of the **Basic Info** section.

This option specifies where the pattern matching occurs in this template rule. In this case, then pattern matching is applied to the source IP address.

Options include:

- **All**: Allows you to permit or deny traffic from all IP addresses.
- **IP Address/Mask**: Allows you to enter a specific IP address and its subnet mask from which you want to either permit or deny traffic for.

a. Enter an IP address/subnet mask combination in the **IP Address/Mask** field.

The subnet must be entered using either CIDR or dotted decimal notation. A valid IP address/subnet mask using dotted decimal notation would be 192.168.1.0/255.255.255.0

A valid IP address/subnet mask using CIDR would be 192.168.1.0/24

A forward slash "/" must be used to separate the IP address from the subnet mask.

- **Variable Address**: Allows you to create a named variable without requiring you to enter the IP addresses/subnet masks in the template. The named variable then serves as a placeholder for **Net Address Group** you created using the **Assistant** combination when you import the template as a rule set into an existing ACL.

b. Enter a name for this variable in the field to the right.

11. Do one of the following:

- Click the radio button ○ to the left of **Yes** in the **Fragment** option if you want to apply the rule to each fragment, or
- Click the radio button ○ to the left of **No** in the **Fragment** option if you want to apply the rule to first fragments.

Traditional packet filtering matched only first fragments of IPv4 packets and allowed all subsequent non-first fragments to pass through. This resulted in security risks as hackers can fabricate non-first fragments to attack networks.

12. Click the radio button ○ to the left of **Yes** in the **Logging** option if you want to enable logging for this rule.

This feature enables the logging of packet filtering only when a module (for example, a firewall) using the ACL supports logging.

13. Enter the VPN instance you want to apply to this rule by entering the VPN-instance-name in the **VPN Instance** field.

A valid entry must be 0-31 characters that cannot contain question marks or blank spaces. This field is case sensitive. If no VPN instance is specified in this field, the rule applies only to non-VPN packets.

14. Click **OK** to create the rule you have just configured.

15. Do one of the following:

- To add more rules to the ACL template, repeat **Steps 7-17**, or
To delete one or more rules from the ACL template, click the checkbox to the left of the sequence number of the rule(s) you want to delete and click the **Delete** button located above the rule table. Click **OK** to confirm the deletion of the selected rule(s), or

To modify the rules you have already created, click the **Modify** icon associated with the rule sequence you want to modify. For more information modifying a rule set, see "Adding or modifying a basic rule in a basic ACL rule set" (page 744), or

To copy rules you have already created, click the **Copy** icon associated with the rule sequence you want to copy. For more information copying a rule set, see "Copying a rule in a template" (page XX).

Rules that belong to a rule set that is configured with a **Match Order** of 'Config' are executed in the order in which they appear in the rule set.

The order in which rules appear in a rule set is initially defined by the order in which they are created. You can, however, reorder the rules in a rule set using the **Sort** feature. For more information using **Sort** to redefine the order of appearance of rules in a rule set, see "Using sort to reorder the rules in an ACL rules set" (page 752).

16. Click **OK** to create the ACL template.

Once you have created an ACL template, you can import the template into one or more ACLs. For more information importing into ACLs, see "Importing rule sets" (page 729).

**Creating an advanced ACL template**

Advanced ACLs enable you to define rules based on Layer three and Layer four information including IP source and destination addresses, protocol and TCP and UDP port information, as well as protocol specific features. A valid numeric range for assigning ACL Identifiers to Advanced ACLs is 100-199, 2000-2699, or 3000-3999.

To create an advanced ACL template:

1. **Navigate to ACL Template:**
   a. Click the **Service** tab from the tabular navigation system on the top.
   b. Click the **ACL Management** icon located under the **Resource and Configuration Management** section of the **Service** tab.
   c. Click the **ACL Template** link located under **ACL Management** on the navigation tree on the left. The **Template List** displays in the main pane of the page.

2. **Click Add.**

3. Enter the name for the template in the **Template Name** field. A valid length for a template name is 1 – 32 characters. A template name cannot begin with a number or a space.

4. Select the **Type** field to define the type of ACL template you want to create. Options include **Basic**, **Advanced**, **Link**, and **User-Defined**. Select **Advanced** from the **Type** list. If you change the type, the added rules are deleted.

5. Select the match order you want to apply to this ACL template by clicking the radio button to the left of the **Match Order** option you want to use. Options include **Config** and **Auto**.
   o If you select **Config**, IMC matches rules in the order in which they were configured.
If you select **Auto**, IMC matches rules based on the principle of depth priority. This feature works only for devices that support it.

6. Enter a brief description for this ACL template in the **Template Description** field.

7. Click **Add Rule** to add a rule to the ACL template.

The **Add Advanced Rule** page appears.

8. Select the protocol for which you want to permit or deny traffic from the **Protocol** list.

9. Select the action you want to take by clicking the radio button to the left of the option you want to apply to this rule.

   - Select **permit** if, upon matching the specified conditions, the packet should be forwarded, or
   - Select **deny** if, upon matching the specified conditions, the packet should be discarded.

10. Enter a named variable for this ACL template in the **Time Range** field, allowing you to create a named variable without requiring you enter the time range in the template.

    The named variable then serves as a placeholder for **Time Range** you created using the **Assistant** combination when you import the template as a rule set into an existing ACL.

    The string entered in the **Time Range** field must start with a letter and have a length of 1-32 characters. Blank spaces [ ] and question marks [?] are not permitted.

11. Select the source IP address option you want to use by clicking the radio button to the left of the desired option in the **Source Address** field in **Basic Info** section.

    This option specifies where the pattern matching occurs in this template rule. In this case, the pattern matching is applied to the source IP address.

    - **All**: Allows you to permit or deny traffic for all IP addresses.
    - **IP Address/Mask**: Allows you to enter a specific IP address and its subnet mask for which you want to either permit or deny traffic for.

    a. Enter an IP address/subnet mask combination in the **IP Address/Mask** field.

    The subnet mask must be entered in dotted decimal notation. A valid IP address/subnet mask using dotted decimal notation would be:

    192.168.1.0/255.255.255.0

    A forward slash "/" must be used to separate the IP address from the subnet mask.

    - **Variable Address**: Enter a name for this variable in the field to the right, allowing you to create a named variable without requiring you to enter the IP addresses/subnet masks in the template. The named variable then serves as a placeholder for **Net Address Group** you created using the **Assistant** combination when you import the template as a rule set into an existing ACL.

12. Select the destination IP address option you want to use by clicking the radio button to the left of the desired option in the **Destination Address** field in **Basic Info** section.

    This option specifies where the pattern matching occurs in this template rule. In this case, the pattern matching is applied to the destination IP address.

    - **All**: Allows you to permit or deny traffic for all IP addresses.
    - **IP Address/Mask**: Allows you to enter a specific IP address and its subnet mask for which you want to either permit or deny traffic.

    a. Enter an IP address/subnet mask combination in the **IP Address/Mask** field.

    This option specifies where the pattern matching occurs in this template rule. In this case, the pattern matching is applied to the destination IP address.
The subnet mask must be entered in dotted decimal notation. A valid IP address/subnet mask using dotted decimal notation would be 
192.168.1.0/255.255.255.0
A forward slash "/" must be used to separate the IP address from the subnet mask.

- **Variable Address**: Enter a name for this variable in the field to the right, allowing you to create a named variable without requiring you to enter the IP addresses/subnet masks in the template. The named variable then serves as a placeholder for **Net Address Group** you created using the **Assistant** combination when you import the template as a rule set into an existing ACL.

b. If you selected **tcp** or **udp** as the protocol you want to apply this ACL rule to in **Step 8**, you must also specify the source TCP or UDP port numbers, as follows:

- Select the source TCP or UDP port option by clicking the radio button ◐ to the left of the port option you want to apply in the Source Port field of the Advanced Settings section.
  - **Undefined**: Allows you to permit or deny traffic for all TCP or UDP port numbers.
  - **Specified Port**: Allows you to identify a specific TCP or UDP port number or range of numbers.

c. Click the radio button ◐ to the left of Specified Port and select the operator you want to use from the list located to the right of the Specified Port option.

d. Enter the TCP or UDP port number in the Port field.

- **Variable Port**: Enter a name for this variable in the field to the right. This option allows you to create a named variable without requiring you to enter the port(s) in the template. The named variable then serves as a placeholder for **Service** you creating using the **Assistant** combination when you import the template as a rule set into an existing ACL.

13. If you selected **tcp** or **udp** as the protocol you want to apply this ACL rule to in **Step 8**, you must also specify the destination TCP or UDP port numbers, as follows:

- Select the destination TCP or UDP port option by clicking the radio button ◐ to the left of the port option you want to apply in the Destination Port field of the Advanced Settings section of the page.
  - **Undefined**: This option allows you to permit or deny traffic for all TCP or UDP port numbers.
  - **Specified Port**: This option allows you to identify a specific TCP or UDP port number or range of numbers.

c. Click the radio button ◐ to the left of Specified Port and select the operator you want to use from the list located to the right of the Specified Port option.

c. Enter the TCP or UDP port number in the Port field.

- **Variable Port**: Enter a name for this variable in the field to the right. This option allows you to create a named variable without requiring you to enter the port(s) in the template. The named variable then serves as a placeholder for **Service** you creating using the **Assistant** combination when you import the template as a rule set into an existing ACL.

14. If you selected **tcp** or **udp** as the protocol you want to apply this ACL rule to in **Step 8**, you may be promoted to select these options:

- Click the radio button ◐ to the left of **Yes** in the **HP ACK** option if you want to apply the rule to match the TCP ACK, otherwise click on the radio button to the left of **No**.
- Click the radio button ◐ to the left of **Yes** in the **HP FIN** option if you want to apply the rule to match the TCP FIN, otherwise click on the radio button to the left of **No**.
- Click the radio button ◐ to the left of **Yes** in the **HP RST** option if you want to apply the rule to match the TCP RST, otherwise click on the radio button to the left of **No**.
• Click the radio button ☐ to the left of Yes in the HP SYN option if you want to apply the rule to match the TCP SYN, otherwise click on the radio button to the left of No.

The HP ACK, HP FIN, HP RST, and HP SYN settings are valid only for the HP E series devices.

15. Select the IP priority you want to apply to ACL template from the IP Priority list.

16. Select the Type of Service for this ACL template from the ToS Value list.

17. Select the DSCP value you want to apply to this ACL template from the DSCP Value list.

18. Do one of the following:
   o Click the radio button ☐ to the left of Yes in the Fragment option if you want to apply the rule to each fragment, or
   o Click the radio button ☐ to the left of No in the Fragment option if you want to apply the rule first fragments.

Traditional packet filtering matched only first fragments of IPv4 packets and allowed all subsequent non-first fragments to pass through. This resulted in security risks as hackers can fabricate non-first fragments to attack networks.

19. Click the radio button ☐ to the left of Yes in the Logging option if you want to enable logging for this rule.

This feature enables the logging of packet filtering only when a module (for example, a firewall) using the ACL supports logging.

20. Enter the VPN instance you want to apply to this rule by entering the VPN-instance-name in the VPN Instance field.

A valid entry must be 0 – 31 characters that cannot contain question marks or blank spaces. This field is case sensitive. If no VPN instance is specified in this field, the rule applies only to non-VPN packets.

21. Click OK to create the rule you have just configured.

22. Do one of the following to add more rules, delete, modify or copy existing rules:
   o To add more rules to the ACL template, repeat Steps 7-21, or
   o To delete one or more rules from the ACL template, click the checkbox ☐ to the left of the No. of the rule(s) you want to delete and click on the Delete button located above the rule table. Click OK to confirm the deletion of the selected rule(s), or
   o To modify a rule you already created, click the Modify icon associated with the rule sequence you want to modify. For more information modifying a rule set, see “Modifying the rules in an ACL template” (page 689), or
   o To copy rules you have already created, click the Copy icon associated with the rule sequence you want to copy. For more information copying a rule set, “Copying a rule in a template” (page 696).

Rules that belong to a rule set that is configured with a Match Order of ‘Config’ are executed in the order in which they appear in the rule set. The order in which rules appear in a rule set is initially defined by the order in which they are created. You can, however, reorder the rules in a rule set using the Sort feature. For more information using Sort to redefine the order of appearance of rules in a rule set, see "Using sort to reorder the rules in an ACL rules set" (page 752).

23. Click OK to create the ACL template.

Once you have created an ACL template, you are ready to import the template into one or more ACLs. For more information importing into ACLs, see "Importing rule sets" (page 729).
Creating a link ACL template

Link ACLs enable you to define rules based on Layer 2 information including MAC source and destination addresses and masks, VLAN priority information, as well as link layer protocol type. A valid numeric range for assigning ACL Identifiers to Link ACLs is 4000-4999.

To create a link ACL template:

1. Navigate to ACL Template:
   a. Click the Service tab from the tabular navigation system on the top.
   b. Click the ACL Management icon located under the Resource and Configuration Management section of the Service tab.
   c. Click the ACL Template link located under ACL Management on the navigation tree on the left. The Template List displays in the main pane of the page.

2. Click Add.

3. Enter the name for the template in the Template Name field. A valid length for a template name is 1 – 32 characters. A template name cannot begin with a number or a space.

4. Select one of the options in the Type field list to define the type of ACL template you want to create. If you change the type, the added rules are deleted.

5. Select the match order you want to apply to this ACL template by clicking the radio button to the left of the Match Order option you want to use.
   o If you select Config, IMC matches rules in the order in which they were configured.
   This feature works only for devices that support it.
   If you select Auto, IMC matches rule based on the principle of depth priority.

6. Enter a brief description for this ACL template in the Template Description field.

7. Click Add Rule to add a rule to the ACL template.

8. Select the action you want to take by clicking the radio button to the left of the option you want to apply to this rule.
   o Select permit if, upon matching the specified conditions, the packet should be forwarded, or
   o Select deny if, upon matching the specified conditions, the packet should be discarded.

9. Enter a named variable for this ACL template in the Time Range field, allowing you to create a named variable without requiring you enter the Time Range in the template.
   The named variable then serves as a placeholder for Time Range you created using the Assistant combination when you import the template as a rule set into an existing ACL.

10. Select the source MAC address option you want to use by clicking the radio button to the left of the desired option in the Source MAC Addr field of the Basic Info section.
    This option specifies where the pattern matching occurs in this template rule. In this case, the pattern matching is applied to the source MAC address.
    o All: Allows you to permit or deny traffic for all MAC addresses.
    o MAC Address/Mask: Allows you to enter a specific MAC address and mask for which you want to either permit or deny traffic.

667
A Valid MAC address format for IMC consists of three sets of four hexadecimal characters separated by a dash, ":". For example:

```
0014-2ad9-05f7
```

would be a valid entry for a MAC address in IMC.

Similarly, the format for a MAC address mask consists of three sets of four hexadecimal characters separated by a dash, ":". For example:

```
ffff-ffff-ffff
```

would be a valid entry for a MAC address mask in IMC.

The MAC address and its mask must be separated by a forward slash, "/".

A valid entry for a MAC Address/Mask would be:

```
0014-2ad9-05f7/ffff-ffff-ffff
```

- **Variable Address**: Enter a name for this variable in the field to the right allowing you to create a named variable without requiring you to enter the MAC addresses/masks in the template. The named variable then serves as a placeholder for entering a MAC address/mask combination when you import the template as a rule set into an existing ACL.

11. Select the destination MAC address option you want to use by clicking the radio button to the left of the desired option in the **Destination MAC Address** field of the **Basic Info** section.

This option specifies where the pattern matching occurs in this template rule. In this case, the pattern matching is applied to the source MAC address.

- **All**: Allows you to permit or deny traffic for all MAC addresses.
- **MAC Address/Mask**: Allows you to identify a specific MAC address and mask for which you want to either permit or deny traffic.

A valid MAC address format for IMC consists of three sets of four hexadecimal characters separated by a dash, ":". For example,

```
0014-2ad9-05f7
```

would be a valid entry for a MAC address in IMC.

Similarly, the format for a MAC address mask consists of three sets of four hexadecimal characters separated by a dash, ":". For example,

```
ffff-ffff-ffff
```

would be a valid entry for a MAC address mask in IMC.

The MAC address and its mask must be separated by a forward slash, "/".

A valid entry for a MAC Address/Mask would be

```
0014-2ad9-05f7/ffff-ffff-ffff
```

- **Variable Address**: Enter a name for this variable in the field to the right allowing you to create a named variable without requiring you to enter the MAC addresses/masks in the template. The named variable then serves as a placeholder for entering a MAC address/mask combination when you import the template as a rule set into an existing ACL.

12. Select the 802.1 priority you want to apply to this ACL rule from the **802.1 Priority** list.

13. Select the Layer 2 encapsulation type you want to apply to this ACL rule from the **Encapsulation Type** list.

14. Enter the Source VLAN ID by entering it in the **Source VLAN ID** field.

This field cannot contain question marks (?) or spaces [ ].

15. Select the Layer 2 frame type from the **Based Frame Type** list.
16. If you selected Ethernet Frame or 802.2 Ethernet Frame in the Base Frame Type list, you must specify a code in the Code field.
   A valid entry for this field includes any four character hexadecimal value.

17. If you selected Ethernet Frame or 802.2 Ethernet Frame in the Base Frame Type list, you must also specify a mask in the Mask field.
   A valid entry for this field includes any four character hexadecimal value.

18. Click OK to create the rule you have just configured.

19. To add more rules, delete, modify, or copy existing rules, do one of the following:
   o To add more rules to the ACL template, repeat Steps 7-18, or
   o To delete one or more rules from the ACL template, click the checkbox to the left of the No. of the rules you want to delete, click the Delete button located above the rule table and then OK to confirm the deletion of the selected rules, or
   o To modify rules you have already created, click the Modify icon associated with the rule sequence you want to modify. For more information modifying a rule set, see "Adding or modifying a basic rule in a basic ACL rule set" (page 744), or
   o To copy rules you have already created, click the Copy icon associated with the rule sequence you want to copy. For more information copying a rule set, see "Copying a rule in an ACL rule set" (page 750).

20. Click OK to create the ACL template.

Once you have created an ACL template, you are ready to import the template into one or more ACLs. For more information importing into ACLs, see "Importing rule sets" (page 729).

Creating a user-defined ACL template

User-Defined ACLs enable you to define a hexadecimal pattern and mask and the offset in the packet header to begin the pattern matching. When a pattern is matched, the conditions of the rule in the ACL template are applied. A valid numeric range for assigning ACL Identifiers to user-defined ACLs is 5000-5999.

To create a user-defined ACL template:
1. Navigate to ACL Template:
   a. Click the Service tab from the tabular navigation system on the top.
   b. Click the ACL Management icon located under the Resource and Configuration Management section of the Service tab.
   c. Click the ACL Template link located under ACL Management on the navigation tree on the left.
      The Template List displays in the main pane of the page.
2. Click Add.
3. Enter the name for the template in the Template Name field.
A valid length for a template name is 1 – 32 characters. A template name cannot begin with a number or a space.

4. Select **User-Defined** from the **Type** list to define the type of ACL template you want to create. A User-Defined template can only have a **Match Order** of **Config**.

5. Enter a brief description for this ACL template in the **Template Description** field.

6. Click **Add Rule** to add a rule to the ACL template. The **Add User-Defined Rule** page appears.

7. Select the action you want to take by clicking the radio button ☑️ to the left of the option you want to apply to this rule:
   - Select **permit** if, upon matching the specified conditions, the packet should be forwarded, or
   - Select **deny** if, upon matching the specified conditions, the packet should be discarded.

8. Enter a named variable for this ACL template in the **Time Range** field, allowing you to create a named variable without requiring you enter the **Time Range** in the template. The named variable then serves as a placeholder for Time Range you created using the Assistant combination when you import the template as a rule set into an existing ACL.

9. Enter up to eight hexadecimal patterns, masks, and offsets for matching the contents of a packet and applying the actions specified in the rule when a hexadecimal pattern is matched. The following rules and guidelines apply to constructing a valid hexadecimal string, mask, and offset value:
   - A rule string must be expressed in hexadecimal only
   - A mask must be expressed in hexadecimal only
   - A rule string length must be equal to its mask length
   - Rule string and mask length must be in multiples of 2
   - The minimum length of a rule string and mask is 2
   - The maximum length of a rule string and mask is 160
   - Offsets must be expressed as a decimal integer
   - Offset range varies by the mask length
   - The minimum value for an offset is 0
   - The maximum value for an offset is 79
   - The offset must increase progressively
     - a. Enter a hexadecimal pattern to be matched in the **Rule String** field.
     - b. Enter a mask in the **Mask** field.
     - c. Enter the offset in the **Excursion** field.
     - d. Enter up to eight **Rule String/Mask/Excursion** combinations.

10. Click **OK** to create the rule you have just configured.

11. To add more rules, delete, modify, or copy an existing rule, do one of the following:
   - To add more rules to the ACL template, repeat **Steps 7-10**, or
   - To delete one or more rules from the ACL template, click on the checkbox ☐️ to the left of the **No.** of the rules you want to delete, click **Delete** located above the rule table, and click **OK** to confirm the deletion of the selected rules, or
To modify rules you have already created, click the Modify icon associated with the rule sequence you want to modify. For more information modifying a rule set, see "Adding or modifying a basic rule in a basic ACL rule set" (page 744), or

To copy rules you have already created, click the Copy icon associated with the rule sequence you want to copy. For more information copying a rule set, see "Copying a rule in an ACL rule set" (page 750).

Rules that belong to a rule set that is configured with a Match Order of ‘Config’ are executed in the order in which they appear in the rule set. The order in which rules appear in a rule set is initially defined by the order in which they are created. You can, however, reorder the rules in a rule set using the Sort feature. For more information using Sort to redefine the order of appearance of rules in a rule set, see "Using sort to reorder the rules in an ACL rules set" (page 752).

12. Click OK to create the ACL template.

Once you have created an ACL template, you are ready to import the template into one or more ACLs. For more information importing into ACLs, see "Importing rule sets" (page 729).

## Modifying ACL templates

Many of the parameters used to configure an ACL template can be changed using the modify option for each of the ACL template types.

### Modifying a basic ACL template

To modify a basic ACL template:

1. Navigate to ACL Template:
   a. Click the Service tab from the tabular navigation system on the top.
   b. Click the ACL Management icon located under the Resource and Configuration Management section of the Service tab.
   c. Click the ACL Template link located under ACL Management on the navigation tree on the left. The Template List displays in the main pane of the page.

2. Click the icon in the Modify field associated with the template you want to modify. The Modify Template page appears.

   You cannot change the Template Name, template Type, or Match Order of an ACL template once you have created it.

3. Modify the description for this ACL template as needed in the Template Description field.

4. To add a new rule to the existing rule set, click Add Rule to add a rule to the ACL template. The Add Basic Rule page appears.

5. Select the action you want to take by clicking the radio button to the left of the option you want to apply to this rule:
   - Select permit if, upon matching the specified conditions, the packet should be forwarded, or
   - Select deny if, upon matching the specified conditions, the packet should be discarded.

6. Enter a named variable for this ACL template in the Time Range field, allowing you to create a named variable without requiring you enter the time range in the template.
The named variable then serves as a placeholder for **Time Range** you created using the **Assistant**
combination when you import the template as a rule set into an existing ACL.

7. Select the source IP address option you want to use by clicking the radio button **☐** to the left of the desired option in the **Source Address** field in **Basic Info** section.

This option specifies where the pattern matching occurs in this template rule. In this case, the pattern matching is applied to the source IP address.

- **All**: Allows you to permit or deny traffic for all IP addresses.
- **IP Address/Mask**: Allows you to enter a specific IP address and its subnet mask for which you want to either permit or deny traffic for.
  a. Enter an IP address/subnet mask combination in the **IP Address/Mask** field.

The subnet mask must be entered in dotted decimal notation. A valid IP address/subnet mask using
dotted decimal notation would be

```
192.168.1.0/255.255.255.0
```

A forward slash “/” must be used to separate the IP address from the subnet mask.

- **Variable Address**: Allows you to create a named variable without requiring you to enter the IP addresses/masks in the template. The named variable then serves as a placeholder for **Net Address Group** you created using the **Assistant** combination when you import the template as a rule set into an existing ACL.

b. Enter a name for this variable field to the right.

8. Do one of the following:

- Click the radio button **☐** to the left of **Yes** in the **Fragment** option if you want to apply the rule to each fragment, or
- Click the radio button **☐** to the left of **No** in the **Fragment** option if you want to apply the rule to first fragments.

Traditional packet filtering matched only first fragments of IPv4 packets and allowed all subsequent non-first fragments to pass through. This resulted in security risks as hackers can fabricate non-first fragments to attack networks.

9. Click the radio button **☐** to the left of **Yes** in the **Logging** option if you want to enable logging for this rule.

This feature enables the logging of packet filtering only when a module (for example, a firewall) is using the ACL supports logging.

10. Enter the **VPN instance** you want to apply to this rule by entering the VPN-instance-name in the **VPN Instance** field.

A valid entry must be 0 – 31 characters that cannot contain question marks or blank spaces. This field is also case sensitive. If no VPN instance is specified in this field, the rule applies only to non-VPN packets.

11. Click **OK** to create the rule you have just configured.

12. Select from the following options to add more rules, delete, modify, or copy existing rules.

a. To add more rules to the ACL template, repeat **Steps 4-11**, or

b. To delete one or more rules from the ACL template, click the checkbox **☐** to the left of the **No.** of the rules you want to delete, click **Delete** located above the rule table and then click **OK** to confirm the deletion of the selected rules, or
c. To modify rules you have already created, click the Modify icon associated with the rule sequence you want to modify. For more information modifying a rule set, see “Adding or modifying a basic rule in a basic ACL rule set” (page 744), or

d. To copy rules you have already created, click the Copy icon associated with the rule sequence you want to copy. For more information copying a rule set, see “Copying a rule in an ACL rule set” (page 750).

Rules that belong to a rule set that is configured with a Match Order of ‘Config’ are executed in the order in which they appear in the rule set. The order in which rules appear in a rule set is initially defined by the order in which they are created. You can, however, reorder the rules in a rule set using the Sort feature. For more information using Sort to redefine the order of appearance of rules in a rule set, see “Using sort to reorder the rules in an ACL rules set” (page 752).

13. Click OK to accept your modifications to the ACL template.

Once you finished modifying an ACL template, you can import the template into one or more ACLs. For more information importing into ACLs, see “Importing rule sets” (page 729).

Modifying an advanced ACL template

To modify an advanced ACL template:

1. Navigate to ACL Template:
   a. Click the Service tab from the tabular navigation system on the top.
   
   b. Click the ACL Management icon located under the Resource and Configuration Management section of the Service tab.
   
   c. Click the ACL Template link located under ACL Management on the navigation tree on the left. The Template List displays in the main pane of the page.

2. Click the icon in the Modify field associated with the template you want to modify. The Modify Template page appears.

   You cannot change the Template Name, template Type, or Match Order of an ACL template once you have created it.

3. Modify the description for this ACL template as needed in the Template Description field.

4. To add a new rule to the existing rule set, click Add Rule to add a rule to the ACL template. The Add Advanced Rule page appears.

5. Select the protocol for which you want to permit or deny traffic from the Protocol list.

6. Select the action you want to take by clicking the radio button to the left of the option you want to apply to this rule.

   o Select permit if, upon matching the specified conditions, the packet should be forwarded, or
   
   o Select deny if, upon matching the specified conditions, the packet should be discarded.

7. Enter a named variable for this ACL template in the Time Range field, allowing you to create a named variable without requiring you enter the time range in the template. The named variable then serves as a placeholder for Time Range you created using the Assistant combination when you import the template as a rule set into an existing ACL.
8. Select the source IP address option you want to use by clicking the radio button to the left of the desired option in the **Source Address** field in **Basic Info** section.

This option specifies where the pattern matching occurs in this template rule. In this case, the pattern matching is applied to the source IP address.

- **All**: Allows you to permit or deny traffic for all IP addresses.
- **IP Address/Mask**: Allows you to enter a specific IP address and its subnet mask for which you want to either permit or deny traffic for.
  
  a. Enter an IP address/subnet mask combination in the **IP Address/Mask** field.

  The subnet mask must be entered in dotted decimal notation. A valid IP address/subnet mask using dotted decimal notation would be

  192.168.1.0/255.255.255.0

  A forward slash "/" must be used to separate the IP address from the subnet mask.

  **Variable Address**: This option allows you to create a named variable without requiring you to enter the IP addresses/masks in the template. The named variable then serves as a placeholder for **Net Address Group** you created using the **Assistant** combination when you import the template as a rule set into an existing ACL.

  b. Enter a name for this variable in the field to the right.

9. Select the destination IP address option you want to use by clicking the radio button to the left of the desired option in the **Destination Address** field in **Basic Info** section.

This option specifies where the pattern matching occurs in this template rule. In this case, the pattern matching is applied to the source IP address.

- **All**: Allows you to permit or deny traffic for all IP addresses.
- **IP Address/Mask**: Allows you to enter a specific IP address and its subnet mask for which you want to either permit or deny traffic.

  a. Enter an IP address/subnet mask combination in the **IP Address/Mask** field.

  The subnet mask must be entered in dotted decimal notation. A valid IP address/subnet mask using dotted decimal notation would be

  192.168.1.0/255.255.255.0

  A forward slash "/" must be used to separate the IP address from the subnet mask.

  **Variable Address**: This option allows you to create a named variable without requiring you to enter the IP addresses/masks in the template. The named variable then serves as a placeholder for **Net Address Group** you created using the **Assistant** combination when you import the template as a rule set into an existing ACL.

  b. Enter a name for this variable in the field to the right.

10. If you selected TCP or UDP as the protocol you want to apply this ACL rule to in **Step 5**, you must also specify the source TCP or UDP port numbers:

  a. Select the source TCP or UDP port option by clicking the radio button to the left of the port option you want to apply in the **Source Port** field of the **Advanced Settings** section:

  o **Undefined**: Allows you to permit or deny traffic for all TCP or UDP port numbers.

  o **Specified Port**: Allows you to identify a specific TCP or UDP port number or range of numbers. Click the radio button to the left of **Specified Port** and select the operator you want to use from the list located to the right of the **Specified Port** option. Enter the TCP or UDP port number in the **Port** field.
**Variable Port**: Allows you to create a named variable without requiring you to enter the ports in the template. The named variable then serves as a placeholder for the **Service** you creating using the **Assistant** combination when you import the template as a rule set into an existing ACL.

**b.** Enter a name for this variable in the field to the right.

11. If you selected TCP or UDP as the protocol you want to apply this ACL rule to in **Step 5**, you must also specify the destination TCP or UDP port numbers:
   
a. Select the destination TCP or UDP port option by clicking the radio button (☑) to the left of the port option you want to apply in the **Destination Port** field of the **Advanced Settings** section:
   
   - **Undefined**: Allows you to permit or deny traffic for all TCP or UDP port numbers.
   - **Specified Port**: Allows you to identify a specific TCP or UDP port number or range of numbers. Click the radio button (☑) to the left of **Specified Port** and select the operator you want to use from the list located to the right of the **Specified Port** option. Enter the TCP or UDP port number in the **Port** field.
   
   - **Variable Port**: Allows you to create a named variable without requiring you to enter the ports in the template. The named variable then serves as a placeholder for **Service** you creating using the **Assistant** combination when you import the template as a rule set into an existing ACL.

   **b.** Enter a name for this variable in the field to the right.

12. If you selected TCP or UDP as the protocol you want to apply this ACL rule to in **Step 5**, you may be promoted to select these options:
   
   - Click the radio button (☑) to the left of **Yes** in the **HP ACK** option if you want to apply the rule to match the TCP ACK, otherwise click on the radio button to the left of **No**.
   
   - Click the radio button (☑) to the left of **Yes** in the **HP FIN** option if you want to apply the rule to match the TCP FIN, otherwise click on the radio button to the left of **No**.
   
   - Click the radio button (☑) to the left of **Yes** in the **HP RST** option if you want to apply the rule to match the TCP RST, otherwise click on the radio button to the left of **No**.
   
   - Click the radio button (☑) to the left of **Yes** in the **HP SYN** option if you want to apply the rule to match the TCP SYN, otherwise click on the radio button to the left of **No**.

   The **HP ACK**, **HP FIN**, **HP RST**, and **HP SYN** settings are valid only for the HP E series devices.

13. Select the IP priority you want to apply to ACL template from the **IP Priority** list.

14. Select the Type of Service for this ACL template from the **ToS Value** list.

15. Select the DSCP value you want to apply to this ACL template from the **DSCP Value** list.

16. Do one of the following:
   
   - Click the radio button (☑) to the left of **Yes** in the **Fragment** option if you want to apply the rule to each fragment, or
   
   - Click the radio button (☑) to the left of **Yes** in the **Fragment** if you want to apply the rule to first fragments.

   Traditional packet filtering matched only first fragments of IPv4 packets and allowed all subsequent non-first fragments to pass through. This resulted in security risks as hackers can fabricate non-first fragments to attack networks.

17. Click the radio button (☑) to the left of **Yes** in the **Logging** option if you want to enable logging for this rule.

   This feature enables the logging of packet filtering only when a module (for example, a firewall) using the ACL supports logging.

18. Enter the VPN instance you want to apply to this rule by entering the VPN-instance-name in the **VPN Instance** field.
A valid entry must be 0-31 characters that cannot contain question marks or blank spaces. This field is case sensitive. If no VPN instance is specified in this field, the rule will apply only to non-VPN packets.

19. Click **OK** to create the rule you have just configured.

20. Select from the following to delete, modify, or copy rules that you have just configured:

   - To delete one or more rules from the ACL template, click the checkbox □ to the left of the No. of the rules you want to delete, click **Delete** located above the rule table, and then click **OK** to confirm the deletion of the selected rules, or

   - To modify rules you have already created, click the **Modify** icon associated with the rule sequence you want to modify. For more information modifying a rule set, see "Adding or modifying a basic rule in a basic ACL rule set" (page 744), or

   - To copy rules you have already created, click the **Copy** icon associated with the rule sequence you want to copy. For more information copying a rule set, see "Copying a rule in an ACL rule set" (page 750).

Rules that belong to a rule set that is configured with a Match Order of ‘Config’ are executed in the order in which they appear in the rule set. The order in which rules appear in a rule set is initially defined by the order in which they are created. You can, however, reorder the rules in a rule set using the **Sort** feature. For more information using **Sort** to redefine the order of appearance of rules in a rule set, see "Using sort to reorder the rules in an ACL rules set" (page 752).

21. Click **OK** to accept your modifications to the ACL template.

   Once you finished modifying an ACL template, you can import the template into one or more ACLs. For more information importing into ACLs, see "Importing rule sets" (page 729).

**Modifying a link ACL template**

To modify a link ACL template:

1. Navigate to **ACL Template**:
   a. Click the **Service** tab from the tabular navigation system on the top.

   b. Click the **ACL Management** icon located under the **Resource and Configuration Management** section of the **Service** tab.

   c. Click the **ACL Template** link located under **ACL Management** on the navigation tree on the left. The **Template List** displays in the main pane of the page.

2. Click the icon in the **Modify** field associated with the template you want to modify.

   The **Modify Template** page appears.

   You cannot change the **Template Name**, template **Type**, or **Match Order** of an ACL template once you have created it.

3. Modify the description for this ACL template as needed in the **Template Description** field.

4. To add a new rule to the existing rule set, click **Add Rule** to add a rule to the ACL template.

   The **Add Link Rule** page appears.

5. Select the action you want to take by clicking the radio button ○ to the left of the option you want to apply to this rule.
Select **permit** if, upon matching the specified conditions, the packet should be forwarded, or

Select **deny** if, upon matching the specified conditions, the packet should be discarded.

6. Enter a named variable for this ACL template in the **Time Range** field allowing you to create a named variable without requiring you enter the **Time Range** in the template.

The named variable then serves as a placeholder for Time Range you created using the Assistant combination when you import the template as a rule set into an existing ACL.

7. Select the source MAC address option you want to use by clicking the radio button ☐ to the left of the desired option in the **Source MAC Addr** field of the **Basic Info** section.

This option specifies where the pattern matching occurs in this template rule. In this case, the pattern matching is applied to the source MAC address.

   - **All**: Allows you to permit or deny traffic for all MAC addresses.
   - **MAC Address/Mask**: Allows you to enter a specific MAC address and mask for which you want to either permit or deny traffic for.

A valid MAC address format for IMC consists of three sets of four hexadecimal characters separated by a dash, "-". For example,

```
0014-2ad9-05f7
```

would be a valid entry for a MAC address in IMC.

Similarly, the format for a MAC address mask consists of three sets of four hexadecimal characters separated by a dash, "-". For example,

```
ffff-ffff-ffff
```

would be a valid entry for a MAC address mask in IMC.

The MAC address and its mask must be separated by a forward slash, "/".

A valid entry for a MAC Address/Mask would be

```
0014-2ad9-05f7/ffff-ffff-ffff
```

   - **Variable Address**: Allows you to create a named variable without requiring you to enter the MAC addresses/masks in the template. The named variable then serves as a placeholder for entering a MAC address/mask combination when you import the template as a rule set into an existing ACL.

   a. Enter a name for this variable in the field to the right.

8. Select the destination MAC address option you want to use by clicking the radio button ☐ to the left of the desired option in the **Destination MAC Address** section of the page.

This option specifies where the pattern matching occurs in this template rule. In this case, the pattern matching is applied to the source MAC address.

   - **All**: Allows you to permit or deny traffic for all MAC addresses.
   - **MAC Address/Mask**: Allows you to identify a specific MAC address and its mask for which you want to either permit or deny traffic.

   a. Select the destination MAC address option you want to use by clicking the radio button ☐ to the left of the desired option in the **Source MAC Addr** field of the **Basic Info** section.

This option specifies where the pattern matching occurs in this template rule. In this case, the pattern matching is applied to the source MAC address.

   - **All**: Allows you to permit or deny traffic to all MAC addresses.
   - **MAC Address/Mask**: Allows you to enter a specific MAC address and mask to which you want to either permit or deny traffic.
A valid MAC address format for IMC consists of three sets of four hexadecimal characters separated by a dash, ".". For example,

```
0014-2ad9-05f7
```

would be a valid entry for a MAC address in IMC.

Similarly, the format for a MAC address mask consists of three sets of four hexadecimal characters separated by a dash, ".". For example,

```
ffff-ffff-ffff
```

would be a valid entry for a MAC address mask in IMC.

The MAC address and its mask must be separated by a forward slash, "/".

A valid entry for a MAC Address/Mask would be

```
0014-2ad9-05f7/ffff-ffff-ffff
```

**Variable Address:** Allows you to create a named variable without requiring you to enter the MAC addresses/masks in the template. The named variable then serves as a placeholder for entering a MAC address/mask combination when you import the template as a rule set into an existing ACL.

b. Enter a name for this variable in the field to the right.

9. Select the 802.1 priority you want to apply to this ACL rule from the **802.1 Priority** list.

10. Select the Layer 2 encapsulation type you want to apply to this ACL rule from the **Encapsulation Type** list.

11. Enter the Source VLAN ID by entering it in the **Source VLAN ID** field.

   This field cannot contain question marks or blank spaces.

12. Select the Layer 2 frame type from the **Based Frame Type** list.

13. If you selected **Ethernet Frame** or **802.2 Ethernet Frame** in the **Base Frame Type** list, you must specify a code in the **Code** field.

   A valid entry for this includes any four character hexadecimal value.

14. Click **OK** to create the rule you have just configured.

15. Do one of the following to add more rules, delete, modify, or copy an existing rule:

   a. To add more rules to the ACL template, repeat **Steps 4-14**, or

   b. To delete one or more rules from the ACL template, click the checkbox to the left of the **No.** of the rules you want to delete, click **Delete** located above the rule table and then click **OK** to confirm the deletion of the selected rules, or

   c. To modify rules you have already created, click the **Modify** icon associated with the rule sequence you want to modify. For more information modifying a rule set, see "Modifying the rules in an ACL template" (page 689), or

   d. To copy rules you have already created, click the **Copy** icon associated with the rule sequence you want to copy. For more information copying a rule set, see "Copying a rule in a template" (page 696).

Rules that belong to a rule set that is configured with a **Match Order** of ‘Config’ are executed in the order in which they appear in the rule set. The order in which rules appear in a rule set is initially defined by the order in which they are created. You can, however, reorder the rules in a rule set using the **Sort** feature. For more information using Sort to redefine the order of appearance of rules in a rule set, see "Using sort to reorder the rules in an ACL rules set" (page 752).

16. Click **OK** to accept your modifications to the ACL template.
Once you finish modifying an ACL template, you can import the template into one or more ACLs. For more information importing into ACLs, see "Importing rule sets" (page 729).

Modifying a user-defined ACL template

To modify a User-Defined ACL template:

1. Navigate to **ACL Template**:
   a. Click the **Service** tab from the tabular navigation system on the top.
   b. Click the **ACL Management** icon located under the **Resource and Configuration Management** section of the **Service** tab.
   c. Click the **ACL Template** link located under **ACL Management** on the navigation tree on the left. The Template List displays in the main pane of the page.

2. Click the icon in the **Modify** field associated with the template you want to modify.
   The **Modify Template** page appears.
   You cannot change the **Template Name**, template **Type**, or **Match Order** of an ACL template once you have created it.

3. Modify the description for this ACL template as needed in the **Template Description** field.

4. To add a new rule to the existing rule set, click **Add Rule** to add a rule to the ACL template.
   The **Add User-Defined Rule** page appears.

5. Select the action you want to take by clicking the radio button ☐ to the left of the option you want to apply to this rule:
   o Select **permit** if, upon matching the specified conditions, the packet should be forwarded, or
   o Select **deny** if, upon matching the specified conditions, the packet should be discarded.

6. Enter a named variable for this ACL template in the **Time Range** field allowing you to create a named variable without requiring you enter the **Time Range** in the template.
   The named variable then serves as a placeholder for Time Range you created using the Assistant combination when you import the template as a rule set into an existing ACL.

7. Enter up to eight hexadecimal patterns, masks, and offsets for matching the contents of a packet and applying the actions specified in the rule when a hexadecimal pattern is matched.
   The following rules and guidelines apply to constructing a valid hexadecimal string, mask, and offset value:
   o A rule string must be expressed in hexadecimal only
   o A mask must be expressed in hexadecimal only
   o A rule string length must be equal to its mask length
   o Rule string and mask length must be in multiples of 2
   o The minimum length of a rule string and mask is 2
   o The maximum length of a rule string and mask is 160
   o Offsets must be expressed as a decimal integer
   o Offset range varies by the mask length
   o The minimum value for an offset is 0
   o The maximum value for an offset is 79
The offset must increase progressively
a. Enter a hexadecimal pattern to be matched in the **Rule String** field.
b. Enter a mask in the **Mask** field.
c. Enter the offset in the **Excursion** field.
d. Enter up to eight **Rule String/Mask/Excursion** combinations.

8. Click **OK** to create the rule you have just configured or to accept the modifications.

9. Do one of the following to add more rules, delete, modify or copy existing rules:
   a. To add more rules to the ACL template, repeat **Steps 4-8**, or
   b. To delete one or more rules from the ACL template, click the checkbox to the left of the **No.** of the rules you want to delete, click **Delete** located above the rule table and then **OK** to confirm the deletion of the selected rules, or
   c. To modify rules you have already created, click the **Modify** icon associated with the rule sequence you want to modify. For more information modifying a rule set, see “Adding or modifying a basic rule in a basic ACL rule set” (page 744), or
   d. To copy rules you have already created, click the **Copy** icon associated with the rule sequence you want to copy. For more information copying a rule set, see "Copying a rule in an ACL rule set" (page 750).

Rules that belong to a rule set that is configured with a **Match Order** of ‘Config’ are executed in the order in which they appear in the rule set. The order in which rules appear in a rule set is initially defined by the order in which they are created. You can, however, reorder the rules in a rule set using the **Sort** feature. For more information using Sort to redefine the order of appearance of rules in a rule set, see "Using sort to reorder the rules in an ACL rules set" (page 752).

10. Click **OK** to accept your modifications to the ACL template.

   Once you are finished modifying an ACL template, you can import the template into one or more ACLs. For more information importing into ACLs, see "Importing rule sets" (page 729).

### Copying an ACL template

ACL Management provides you with the ability to copy an existing ACL template to a new template and change some of the configuration parameters to adapt it to meet other needs. While you can change many of the configuration options using the copy feature, you cannot change the ACL template type or match order of a template using the **Copy** option. Therefore, copying an existing ACL template limits you to creating rules for the same template type as was used for the original ACL template that was copied.

To copy an existing ACL template:

1. **Navigate to ACL Template**:
   a. Click the **Service** tab from the tabular navigation system on the top:
   b. Click the **ACL Management** icon located under the **Resource and Configuration Management** section of the **Service** tab.
   c. Click the **ACL Template** link located under **ACL Management** on the navigation tree on the left.
   The **Template List** displays in the main pane of the page.
2. Click the icon in the Copy field associated with the template you want to copy.

3. Enter a new name for the ACL template in the Template Name field.
   You cannot change the template Type or Match Order of an ACL template when copying an existing
   template to a new template.

4. Enter a template description in the Template Description field.

5. You can create, modify, copy, or delete the rules of a copied template based on the existing ACL
   template type.
   For more information creating rules, see the sections of this manual on creating or modifying ACLs and
   specifically the steps for creating rules for the ACL template type you have copied. The steps for
   creating rules vary by template type.

6. Click OK to create a copy of the ACL template.
   Once you finished copying an ACL template, you can import the template into one or more ACLs. For
   more information importing into ACLs, see "Importing rule sets" (page 729).

Exporting an ACL template

IMC provides you with the ability to export the contents of an ACL template for import into an ACL resource.
Or rather, you can import the contents of an ACL template into an existing ACL in ACL Management. There
are two paths for accessing this option. The first is by clicking the Export icon associated with the ACL
template you want to import and the second is by clicking Import from the Rule Set List of an existing ACL
Resource. Both paths lead to the same feature in ACL Management, the Import ACL Template to ACL
Resource feature. For more information importing the contents of an ACL template into an ACL resource, see
"Importing rule sets" (page 729).

Deleting ACL templates

You can manage the ACL template list by deleting templates that are no longer used.

To delete one or more templates:

1. Navigate to ACL Template:
   a. Click the Service tab from the tabular navigation system on the top.

   b. Click the ACL Management icon located under the Resource and Configuration Management
      section of the Service tab.

   c. Click the ACL Template link located under ACL Management on the navigation tree on the left.
      The Template List displays in the main pane of the page.

2. Click the checkboxes to the left of the Template Names for the templates you want to delete.

3. Click Delete.

4. Click OK to confirm the deletion of the selected templates.
Managing the rules in a template

Effective template management requires effective rule management. ACL Management provides you with the ability to manage the rules within the rule set of a template. This includes adding, modifying, copying, deleting, and sorting the rules in a rules set.

Adding rules to a template

Once a template has been created, you can add rules to it. You can only add rules of the same type as the ACL.

To add a basic rule to a basic ACL template:

1. Navigate to ACL Template:
   a. Click the Service tab from the tabular navigation system on the top.
   b. Click the ACL Management icon located under the Resource and Configuration Management section of the Service tab.
   c. Click the ACL Template link located under ACL Management on the navigation tree on the left.
   
   The Template List displays in the main pane of the page.

2. Click the icon in the Modify field associated with the basic template you want to modify.
   
   The Modify Template page appears.

3. Click Add Rule to add a rule to the ACL template.
   
   The Add Basic Rule page appears.

4. Select the action you want to take by clicking the radio button to the left of the option you want to apply to this rule:
   - Select permit if, upon matching the specified conditions, the packet should be forwarded, or
   - Select deny if, upon matching the specified conditions, the packet should be discarded.

5. Enter a named variable for this ACL template in the Time Range field allowing you to create a named variable without requiring you enter the time range in the template. The named variable then serves as a placeholder for Time Range you created using the Assistant combination when you import the template as a rule set into an existing ACL.

6. Select the source IP address option you want to use by clicking the radio button to the left of the desired option in the Source Address field in Basic Info section.
   
   This option specifies where the pattern matching occurs in this template rule. In this case, pattern matching is applied to the source IP address.
   - All: Allows you to permit or deny traffic for all IP addresses.
   - IP Address/Mask: Allows you to enter a specific IP address and its subnet mask for which you want to either permit or deny traffic for.

   a. Enter an IP address/subnet mask combination in the IP Address/Mask field.
   
   The subnet mask must be entered in dotted decimal notion. A valid IP address/subnet mask using dotted decimal notation would be 192.168.1.0/255.255.255.0.

   A forward slash "/" must be used to separate the IP address from the subnet mask.
Variable Address: Allows you to create a named variable without requiring you to enter the IP addresses/masks in the template. The named variable then serves as a placeholder for Net Address Group you created using the Assistant combination when you import the template as a rule set into an existing ACL.

b. Enter a name for this variable in the field to the right.

7. Do one of the following:
   o Click the radio button to the left of Yes in the Fragment option if you want to apply the rule to each fragment, or
   o Click the radio button to the left of No in the Fragment option if you want the rule to apply to first fragments.

Traditional packet filtering matched only first fragments of IPv4 packets and allowed all subsequent non-first fragments to pass through. This resulted in security risks as hackers can fabricate non-first fragments to attack networks.

8. Click the radio button to the left of Yes in the Logging option if you want to enable logging for this rule.

This feature enables the logging of packet filtering only when a module (for example, a firewall) using the ACL supports logging.

9. Enter the VPN instance you want to apply to this rule by entering the VPN-instance-name in the VPN Instance field.

   A valid entry must be 0-31 characters that cannot contain question marks or blank spaces. Note also that this field is case sensitive. If no VPN instance is specified in this field, the rule applies only to non-VPN packets.

10. Click OK to create the rule you have just configured.

11. Click OK to add the rule to the ACL template.

Adding an advanced rule to an advanced template

To add an advanced rule to an advanced ACL template:

1. Navigate to ACL Template:
   a. Click the Service tab from the tabular navigation system on the top.

   b. Click the ACL Management icon located under the Resource and Configuration Management section of the Service tab.

   c. Click the ACL Template link located under ACL Management on the navigation tree on the left.

   The Template List displays in the main pane of the page.

2. Click the icon in the Modify field associated with the advanced template you want to modify. The Modify Template page appears.

3. Click Add Rule to add a rule to the ACL template. The Add Advanced Rule page appears.

4. Select the protocol for which you want to permit or deny traffic from the Protocol list.

5. Select the action you want to take by clicking the radio button to the left of the option you want to apply to this rule:
   o Select permit if, upon matching the specified conditions, the packet should be forwarded, or
Select deny if, upon matching the specified conditions, the packet should be discarded.

6. Enter a named variable for this ACL template in the Time Range field allowing you to create a named variable without requiring you to enter the time range in the template.

The named variable then serves as a placeholder for Time Range you created using the Assistant combination when you import the template as a rule set into an existing ACL.

7. Select the source IP address option you want to use by clicking the radio button to the left of the desired option in the Source Address field in Basic Info section.

This option specifies where the pattern matching occurs in this template rule. In this case, the pattern matching is applied to the source IP address.

- All: Allows you to permit or deny traffic for all IP addresses.
- IP Address/Mask: Allows you to enter a specific IP address and its subnet mask for which you want to either permit or deny traffic for.

   a. Enter an IP address/subnet mask combination in the IP Address/Mask field.

   The subnet mask must be entered in dotted decimal notation. A valid IP address/subnet mask using dotted decimal notation would be

   

   A forward slash "/" must be used to separate the IP address from the subnet mask.

   - Variable Address: Allows you to create a named variable without requiring you to enter the IP addresses/masks in the template. The named variable then serves as a placeholder for Net Address Group you created using the Assistant combination when you import the template as a rule set into an existing ACL.

   b. Enter a name for this variable in the field to the right.

8. Select the destination IP address option you want to use by clicking the radio button to the left of the desired option in the Destination Address field in Basic Info section.

This option specifies where the pattern matching occurs in this template rule. In this case, the pattern matching is applied to the source IP address.

- All: Allows you to permit or deny traffic for all IP addresses.
- IP Address/Mask: Allows you to enter a specific IP address and its subnet mask for which you want to either permit or deny traffic.

   a. Enter an IP address/subnet mask combination in the IP Address/Mask field.

   The subnet mask must be entered in dotted decimal notation. A valid IP address/subnet mask using dotted decimal notation would be

   

   A forward slash "/" must be used to separate the IP address from the subnet mask.

   - Variable Address: Allows you to create a named variable without requiring you to enter the IP addresses/masks in the template. The named variable then serves as a placeholder for Net Address Group you created using the Assistant combination when you import the template as a rule set into an existing ACL.

   b. Enter a name for this variable in the field to the right.

9. If you selected TCP or UDP as the protocol you want to apply this ACL rule to in Step 8, you must also specify the source TCP or UDP port numbers:

   a. Select the source TCP or UDP port option by clicking the radio button to the left of the port option you want to apply in the Source Port field of the Advanced Settings section:

   - Undefined: Allows you to permit or deny traffic for all TCP or UDP port numbers.
o **Specified Port**: Allows you to identify a specific TCP or UDP port number or range of numbers. Click the radio button ☑️ to the left of **Specified Port** and select the operator you want to use from the list located to the right of the **Specified Port** option. Enter the TCP or UDP port number in the **Port** field.

o **Variable Port**: Allows you to create a named variable without requiring you to enter the ports in the template. The named variable then serves as a placeholder for **Service** you creating using the **Assistant** combination when you import the template as a rule set into an existing ACL.

b. Enter a name for this variable in the field to the right.

10. If you selected TCP or UDP as the protocol you want to apply this ACL rule to in **Step 8**, you must also specify the destination TCP or UDP port numbers:

a. Select the destination TCP or UDP port option by clicking the radio button ☑️ to the left of the port option you want to apply in the **Destination Port** field of the **Advanced Settings** section:

o **Undefined**: Allows you to permit or deny traffic for all TCP or UDP port numbers.

o **Specified Port**: Allows you to identify a specific TCP or UDP port number or range of numbers.

b. Click the radio button ☑️ to the left of **Specified Port** and select the operator you want to use from the list located to the right of the **Specified Port** option.

c. Enter the TCP or UDP port number in the **Port** field.

o **Variable Port**: Allows you to create a named variable without requiring you to enter the ports in the template. The named variable then serves as a placeholder for **Service** you creating using the **Assistant** combination when you import the template as a rule set into an existing ACL.

d. Enter a name for this variable in the field to the right.

11. If you selected TCP or UDP as the protocol you want to apply this ACL rule to in **Step 4**, you could be promoted to select these options:

o Click the radio button ☑️ to the left of **Yes** in the **HP ACK** option if you want to apply the rule to match the TCP ACK, otherwise click on the radio button to the left of **No**.

o Click the radio button ☑️ to the left of **Yes** in the **HP FIN** option if you want to apply the rule to match the TCP FIN, otherwise click on the radio button to the left of **No**.

o Click the radio button ☑️ to the left of **Yes** in the **HP RST** option if you want to apply the rule to match the TCP RST, otherwise click on the radio button to the left of **No**.

o Click the radio button ☑️ to the left of **Yes** in the **HP SYN** option if you want to apply the rule to match the TCP SYN, otherwise click on the radio button to the left of **No**.

The **HP ACK**, **HP FIN**, **HP RST**, and **HP SYN** settings are valid only for the HP E series devices.

12. Select the IP priority you want to apply to ACL template from the **IP Priority** list.

13. Select the Type of Service for this ACL template from the **ToS Value** list.

14. Select the DSCP value you want to apply to this ACL template from the **DSCP Value** list.

15. Do one of the following:

o Click the radio button ☑️ to the left of **Yes** in the **Fragment** option if you want to apply the rule to each fragment, or

o Click the radio button ☑️ to the left of **No** in the **Fragment** option if you want to apply the rule to first fragments.

Traditional packet filtering matched only first fragments of IPv4 packets and allowed all subsequent non-first fragments to pass through. This resulted in security risks as hackers can fabricate non-first fragments to attack networks.

16. Click the radio button ☑️ to the left of **Yes** in the **Logging** option if you want to enable logging for this rule.
This feature enables the logging of packet filtering only when a module (for example, a firewall) using the ACL supports logging.

17. Enter the VPN instance you want to apply to this rule by entering the VPN-instance-name in the **VPN Instance** field.

   A valid entry must be 0-31 characters that cannot contain question marks or blank spaces. Note also that this field is case sensitive. If no VPN instance is specified in this field, the rule will apply only to non-VPN packets.

18. Click **OK** to create the rule you have just configured.

19. Click **OK** to add the rule to the ACL template.

**Adding a link rule to a link ACL template**

To add a link rule to a link ACL template:

1. Navigate to **ACL Template**:
   a. Click the **Service** tab from the tabular navigation system on the top.
   b. Click the **ACL Management** icon located under the **Resource and Configuration Management** section of the **Service** tab.
   c. Click the **ACL Template** link located under **ACL Management** on the navigation tree on the left. The Template List displays in the main pane of the page.

2. Click the icon in the **Modify** field associated with the link template you want to modify. The **Modify Template** page appears.

3. Click **Add Rule** to add a rule to the ACL template. The Add Link Rule page appears.

4. Select the action you want to take by clicking the radio button to the left of the option you want to apply to this rule:
   - Select **permit** if, upon matching the specified conditions, the packet should be forwarded, or
   - Select **deny** if, upon matching the specified conditions, the packet should be discarded.

5. Enter a named variable for this ACL template in the **Time Range** field allowing you to create a named variable without requiring you enter the **Time Range** in the template. The named variable then serves as a placeholder for Time Range you created using the Assistant combination when you import the template as a rule set into an existing ACL.

6. Select the source MAC address option you want to use by clicking the radio button to the left of the desired option in the **Source MAC Addr** field of the **Basic Info** section. This option specifies where the pattern matching occurs in this template rule. In this case, the pattern matching is applied to the source MAC address.
   - **All**: Allows you to permit or deny traffic for all MAC addresses.
   - **MAC Address/Mask**: Allows you to enter a specific MAC address and mask for which you want to either permit or deny traffic for.

   A valid MAC address format for IMC consists of three sets of four hexadecimal characters separated by a dash, "-". For example,

```
0014-2ad9-05f7
```

would be a valid entry for a MAC address in IMC.

686
Similarly, the format for a MAC address mask consists of three sets of four hexadecimal characters separated by a dash, ".". For example,

```
ffff-ffff-ffff
```

would be a valid entry for a MAC address mask in IMC.

The MAC address and its mask must be separated by a forward slash, "/".

A valid entry for a MAC Address/Mask would be

```
0014-2ad9-05f7/ffff-ffff-ffff
```

- **Variable Address**: Allows you to create a named variable without requiring you to enter the MAC addresses/masks in the template. The named variable then serves as a placeholder for entering a MAC address/mask combination when you import the template as a rule set into an existing ACL.

  a. Click the radio button to the left of Variable Address in the Source MAC addr portion of the Basic Info section of the page.
  
b. Enter a name for this variable in the field to the right.

7. Select the destination MAC address option you want to use by clicking the radio button to the left of the desired option in the Destination MAC Address field of the Basic Info section.

   This option specifies where the pattern matching occurs in this template rule. In this case, the pattern matching is applied to the source MAC address.

   - **All**: Allows you to permit or deny traffic for all MAC addresses.
   
   - **MAC Address/Mask**: Allows you to identify a specific MAC address and its mask for which you want to either permit or deny traffic.

   A valid MAC address format for IMC consists of three sets of four hexadecimal characters separated by a dash, ".". For example,

```
0014-2ad9-05f7
```

would be a valid entry for a MAC address in IMC.

Similarly, the format for a MAC address mask consists of three sets of four hexadecimal characters separated by a dash, ".". For example,

```
ffff-ffff-ffff
```

would be a valid entry for a MAC address mask in IMC.

The MAC address and its mask must be separated by a forward slash, "/".

A valid entry for a MAC Address/Mask would be

```
0014-2ad9-05f7/ffff-ffff-ffff
```

- **Variable Address**: Allows you to create a named variable without requiring you to enter the MAC addresses/masks in the template. The named variable then serves as a placeholder for entering a MAC address/mask combination when you import the template as a rule set into an existing ACL.

  a. Enter a name for this variable in the field to the right.

8. Select the 802.1 priority you want to apply to this ACL rule from the 802.1 Priority list.

9. Select the Layer 2 encapsulation type you want to apply to this ACL rule from the Encapsulation Type list.

10. Enter the Source VLAN ID by entering it in the Source VLAN ID field.

    This field cannot contain question marks or blank spaces.

11. Select the Layer 2 frame type from the Based Frame Type list.

12. If you selected Ethernet Frame or 802.2 Ethernet Frame in the Base Frame Type list, you must specify a code in the Code field.
A valid entry for this field includes any four character hexadecimal value.

13. If you selected Ethernet Frame or 802.2 Ethernet Frame in the Base Frame Type list, you must also specify a mask in the Mask field.
   A valid entry for this field includes any four character hexadecimal value.

14. Click OK to create the rule you have just configured.

15. Click OK to add the rule to the ACL template.

**Adding a user-defined rule to a user-defined ACL template**

To add a user defined rule to a user-defined ACL template:

1. Navigate to ACL Resource:
   a. Click the Service tab from the tabular navigation system on the top.
   b. Click the ACL Management icon located under the Resource and Configuration Management section of the Service tab.
   c. Click the ACL Template link located under ACL Management on the navigation tree on the left. The Template List displays in the main pane of the page.

2. Click the icon in the Modify field associated with the user-defined template you want to modify. The Modify Template page appears.

3. Click Add Rule to add a rule to the ACL template. The Add User-Defined Rule page appears.

4. Select the action you want to take by clicking the radio button to the left of the option you want to apply to this rule:
   - Select permit if, upon matching the specified conditions, the packet should be forwarded, or
   - Select deny if, upon matching the specified conditions, the packet should be discarded.

5. Enter a named variable for this ACL template in the Time Range field allowing you to create a named variable without requiring you enter the Time Range in the template.
   The named variable then serves as a placeholder for Time Range you created using the Assistant combination when you import the template as a rule set into an existing ACL.

6. Enter up to eight hexadecimal patterns, masks, and offsets for matching the contents of a packet and applying the actions specified in the rule when a hexadecimal pattern is matched.
   The following rules and guidelines apply to constructing a valid hexadecimal string, mask, and offset value:
   - A rule string must be expressed in hexadecimal only
   - A mask must be expressed in hexadecimal only
   - A rule string length must be equal to its mask length
   - Rule string and mask length must be in multiples of 2
   - The minimum length of a rule string and mask is 2
   - The maximum length of a rule string and mask is 160
   - Offsets must be expressed as a decimal integer
   - Offset range varies by the mask length
   - The minimum value for an offset is 0
The maximum value for an offset is 79
The offset must increase progressively
a. Enter a hexadecimal pattern to be matched in the Rule String field.
b. Enter a mask in the Mask field.
c. Enter the offset in the Excursion field.
d. Enter up to eight Rule String/Mask/Excursion combinations.

7. Click OK to create the rule you have just configured.
8. Click OK to add the rule to the ACL template.

Modifying the rules in an ACL template

You can also modify the individual rules of a template.

To modify the basic rule of a basic ACL template:

1. Navigate to ACL Template.
   a. Click the Service tab from the tabular navigation system on the top.
   b. Click the ACL Management icon located under the Resource and Configuration Management section of the Service tab.
   c. Click the ACL Template link located under ACL Management on the navigation tree on the left. The Template List displays in the main pane of the page.

2. Click the icon in the Modify field associated with the basic template you want to modify.
   The Modify Template page displays, with the Modify Template page in the main pane.

3. Click the icon in the Modify field associated with the basic rule you want to modify.

4. Select the action you want to take by clicking the radio button to the left of the option you want to apply to this rule:
   o Select permit if, upon matching the specified conditions, the packet should be forwarded, or
   o Select deny if, upon matching the specified conditions, the packet should be discarded.

5. Enter a named variable for this ACL template in the Time Range field allowing you to create a named variable without requiring you enter the time range in the template.
   The named variable then serves as a placeholder for Time Range you created using the Assistant combination when you import the template as a rule set into an existing ACL.

6. Select the source IP address option you want to use by clicking the radio button to the left of the desired option in the Source Address field in Basic Info section.
   This option specifies where the pattern matching occurs in this template rule. In this case, the pattern matching is applied to the source IP address.
   o All: Allows you to permit or deny traffic for all IP addresses.
   o IP Address/Mask: Allows you to enter a specific IP address and its subnet mask for which you want to either permit or deny traffic for.

Enter an IP address/subnet mask combination in the IP Address/Mask field. The subnet mask must be entered in dotted decimal notation. A valid IP address/subnet mask using dotted decimal notation would be

192.168.1.0/255.255.255.0
Note too that a forward slash "/" must be used to separate the IP address from the subnet mask.

- **Variable Address**: Enter a name for this variable in the field to the right. This option allows you to create a named variable without requiring you to enter the IP addresses/masks in the template. The named variable then serves as a placeholder for **Net Address Group** you created using the **Assistant** combination when you import the template as a rule set into an existing ACL.

7. Do one of the following:
   - Click the radio button ○ to the left of **Yes** in the **Fragment** option if you want to apply the rule to each fragment, or
   - Click the radio button ○ to the left of **No** in the **Fragment** option if you want to apply the rule to first fragments.

Traditional packet filtering matched only first fragments of IPv4 packets and allowed all subsequent non-first fragments to pass through. This resulted in security risks as hackers can fabricate non-first fragments to attack networks.

8. Click the radio button ○ to the left of **Yes** in the **Logging** option if you want to enable logging for this rule.

   This feature enables the logging of packet filtering only when a module (for example, a firewall) using the ACL supports logging.

9. Enter the VPN instance you want to apply to this rule by entering the VPN-instance-name in the **VPN Instance** field.

   A valid entry must be 0 – 31 characters that cannot contain question marks or blank spaces. This field is case sensitive. If no VPN instance is specified in this field, the rule applies only to non-VPN packets.

10. Click **OK** to accept the modifications to the rule.

11. Click **OK** to accept the modifications to the template.

### Modifying advanced rules in advanced ACL templates

To modify the advanced rule of an advanced ACL template:

1. Navigate to **ACL Template**:
   - a. Click the **Service** tab from the tabular navigation system on the top.
   - b. Click the **ACL Management** icon located under the **Resource and Configuration Management** section of the **Service** tab.
   - c. Click the **ACL Template** link located under **ACL Management** on the navigation tree on the left.

   The **Template List** displays in the main pane of the page.

2. Click the icon [Modify] in the **Modify** field associated with the advanced template you want to modify.

   The **Modify Template** page displays with the **Rule List** for the selected ACL template in the main pane of the **Modify Template** page.

3. Click the icon [Modify] in the **Modify** field associated with the rule you want to modify.

4. Select the protocol for which you want to permit or deny traffic from the **Protocol** list by clicking the radio button ○ to the left of the option you want to apply to this rule:
   - Select **permit** if, upon matching the specified conditions, the packet should be forwarded, or
   - Select **deny** if, upon matching the specified conditions, the packet should be discarded.

5. Enter a named variable for this ACL template in the **Time Range** field allowing you to create a named variable without requiring you enter the time range in the template. The named variable then serves as
a placeholder for **Time Range** you created using the **Assistant** combination when you import the template as a rule set into an existing ACL.

6. Select the source IP address option you want to use by clicking the radio button ☐ to the left of the desired option in the **Source Address** field in **Basic Info** section.

This option specifies where the pattern matching occurs in this template rule. In this case, the pattern matching is applied to the source IP address. Options include:

- **All**: Allows you to permit or deny traffic for all IP addresses.
- **IP Address/Mask**: Allows you to enter a specific IP address and its subnet mask for which you want to either permit or deny traffic for.

Enter an IP address/subnet mask combination in the **IP Address/Mask** field. The subnet mask must be entered in dotted decimal notation. A valid IP address/subnet mask using dotted decimal notation would be `192.168.1.0/255.255.255.0`

A forward slash `/` must be used to separate the IP address from the subnet mask.

- **Variable Address**: Allows you to create a named variable without requiring you to enter the IP addresses/masks in the template. The named variable then serves as a placeholder for **Net Address Group** you created using the **Assistant** combination when you import the template as a rule set into an existing ACL.
  
a. Enter a name for this variable in the field to the right.

7. Select the destination IP address option you want to use by clicking the radio button ☐ to the left of the desired option in the **Destination Address** field in **Basic Info** section.

This option specifies where the pattern matching occurs in this template rule. In this case, the pattern matching is applied to the destination IP address. Options include:

- **All**: Allows you to permit or deny traffic for all IP addresses.
- **IP Address/Mask**: Allows you to enter a specific IP address and its subnet mask for which you want to either permit or deny traffic.

8. Enter an IP address/subnet mask combination in the **IP Address/Mask** field.

The subnet mask must be entered in dotted decimal notation. A valid IP address/subnet mask using dotted decimal notation would be `192.168.1.0/255.255.255.0`

A forward slash `/` must be used to separate the IP address from the subnet mask.

- **Variable Address**: Allows you to create a named variable without requiring you to enter the IP addresses/masks in the template. The named variable then serves as a placeholder for **Net Address Group** you created using the **Assistant** combination when you import the template as a rule set into an existing ACL.
  
a. Enter a name for this variable in the field to the right.

9. If you selected TCP or UDP as the protocol you want to apply this ACL rule to in **Step 4**, you must also specify the source TCP or UDP port numbers:

a. Select the source TCP or UDP port option by clicking the radio button ☐ to the left of the port option you want to apply in the **Source Port** field of the **Advanced Settings** section.

- **Undefined**: Allows you to permit or deny traffic for all TCP or UDP port numbers.
- **Specified Port**: Allows you to identify a specific TCP or UDP port number or range of numbers.

b. Click the radio button ☐ to the left of **Specified Port** and select the operator you want to use from the list located to the right of the **Specified Port** option.
c. Enter the TCP or UDP port number in the Port field.
   o Variable Port: Allows you to create a named variable without requiring you to enter the ports in the template. The named variable then serves as a placeholder for Service you creating using the Assistant combination when you import the template as a rule set into an existing ACL.

d. Enter a name for this variable in the field to the right.

10. If you selected TCP or UDP as the protocol you want to apply this ACL rule to in Step 4, you must also specify the destination TCP or UDP port numbers:
   a. Select the destination TCP or UDP port option by clicking the radio button \( \square \) to the left of the port option you want to apply in the Destination Port field of the Advanced Settings section:
      o Undefined: Allows you to permit or deny traffic for all TCP or UDP port numbers.
      o Specified Port: Allows you to identify a specific TCP or UDP port number or range of numbers.
   b. Click the radio button \( \square \) to the left of Specified Port and select the operator you want to use from the list located to the right of the Specified Port option.
   c. Enter the TCP or UDP port number in the Port field.
      o Variable Port: Allows you to create a named variable without requiring you to enter the ports in the template. The named variable then serves as a placeholder for Service you creating using the Assistant combination when you import the template as a rule set into an existing ACL.
   d. Enter a name for this variable in the field to the right.

11. If you selected TCP or UDP as the protocol you want to apply this ACL rule to in Step 4, you could be promoted to select these options:
   o Click the radio button \( \square \) to the left of Yes in the HP ACK option if you want to apply the rule to match the TCP ACK, otherwise click on the radio button to the left of No.
   o Click the radio button \( \square \) to the left of Yes in the HP FIN option if you want to apply the rule to match the TCP FIN, otherwise click on the radio button to the left of No.
   o Click the radio button \( \square \) to the left of Yes in the HP RST option if you want to apply the rule to match the TCP RST, otherwise click on the radio button to the left of No.
   o Click the radio button \( \square \) to the left of Yes in the HP SYN option if you want to apply the rule to match the TCP SYN, otherwise click on the radio button to the left of No.

   The HP ACK, HP FIN, HP RST, and HP SYN settings are valid only for the HP E series devices.

12. Select the IP priority you want to apply to ACL template from the IP Priority list.

13. Select the Type of Service for this ACL template from the TOS Value list.

14. Select the DSCP value you want to apply to this ACL template from the DSCP Value list.

15. Do one of the following:
   o Click the radio button \( \square \) to the left of Yes in the Fragment option if you want to apply the rule to each fragment, or
   o Click the radio button \( \square \) to the left of No in the Fragment option if you want to apply the rule to first fragments.

   Traditional packet filtering matched only first fragments of IPv4 packets and allowed all subsequent non-first fragments to pass through. This resulted in security risks as hackers can fabricate non-first fragments to attack networks.

16. Click the radio button \( \square \) to the left of Yes in the Logging option if you want to enable logging for this rule.
This feature enables the logging of packet filtering only when a module (for example, a firewall) is using the ACL supports logging.

17. Enter the VPN instance you want to apply to this rule by entering the VPN-instance-name in the VPN Instance field.

A valid entry must be 0 – 31 characters that cannot contain question marks or blank spaces. This field is case sensitive. If no VPN instance is specified in this field, the rule applies only to non-VPN packets.

18. Click OK to accept the modifications to the rule.
19. Click OK to accept the modifications to the template.

Modifying the link rule of a link ACL template

To modify the link rule of a link ACL template:

1. Navigate to ACL Template:
   a. Click the Service tab from the tabular navigation system on the top.
   b. Click the ACL Management icon located under the Resource and Configuration Management section of the Service tab.
   c. Click the ACL Template link located under ACL Management on the navigation tree on the left. The Template List displays in the main pane of the page.

2. Click the icon in the Modify field associated with the link template you want to modify. The Modify Template displays with the Rule List for the selected ACL template in the main pane.

3. Click the icon in the Modify field associated with the rule you want to modify.
4. Select the action you want to take by clicking the radio button to the left of the option you want to apply to this rule:
   o Select permit if, upon matching the specified conditions, the packet should be forwarded, or
   o Select deny if, upon matching the specified conditions, the packet should be discarded.

5. Enter a named variable for this ACL template in the Time Range field allowing you to create a named variable without requiring you enter the Time Range in the template. The named variable then serves as a placeholder for Time Range you created using the Assistant combination when you import the template as a rule set into an existing ACL.

6. Select the source MAC address option you want to use by clicking the radio button to the left of the desired option in the Source MAC Addr field of the Basic Info section.

   This option specifies where the pattern matching occurs in this template rule. In this case, the pattern matching is applied to the source MAC address.
   o All: Allows you to permit or deny traffic for all MAC addresses.
   o MAC Address/Mask: Allows you to enter a specific MAC address and mask for which you want to either permit or deny traffic for.

A valid MAC address format for IMC consists of three sets of four hexadecimal characters separated by a dash, ":". For example,

0014-2ad9-05f7

would be a valid entry for a MAC address in IMC.
Similarly, the format for a MAC address mask consists of three sets of four hexadecimal characters separated by a dash, "-". For example,

```
ffff-ffff-ffff
```

would be a valid entry for a MAC address mask in IMC.

The MAC address and its mask must be separated by a forward slash, "/".

A valid entry for a MAC Address/Mask would be

```
0014-2ad9-05f7/ffff-ffff-ffff
```

- **Variable Address**: Allows you to create a named variable without requiring you to enter the MAC addresses/masks in the template. The named variable then serves as a placeholder for entering a MAC address/mask combination when you import the template as a rule set into an existing ACL.
  - a. Enter a name for this variable in the field to the right.

7. Select the destination MAC address option you want to use by clicking the radio button to the left of the desired option in the **Destination MAC Address** section of the **Add Link Rule** page.

This option specifies where the pattern matching occurs in this template rule. In this case, the pattern matching is applied to the source MAC address.

- **All**: Allows you to permit or deny traffic for all MAC addresses.

- **MAC Address/Mask**: Allows you to identify a specific MAC address and its mask for which you want to either permit or deny traffic.

8. Select the destination MAC address option you want to use by clicking the radio button to the left of the desired option in the **Source MAC Address** field of the **Basic Info** section.

This option specifies where the pattern matching occurs in this template rule. In this case, the pattern matching is applied to the source MAC address.

- **All**: Allows you to permit or deny traffic to all MAC addresses.

- **MAC Address/Mask**: Allows you to enter a specific MAC address and mask to which you want to either permit or deny traffic.

A valid MAC address format for IMC consists of three sets of four hexadecimal characters separated by a dash, "-". For example,

```
0014-2ad9-05f7
```

would be a valid entry for a MAC address in IMC.

Similarly, the format for a MAC address mask consists of three sets of four hexadecimal characters separated by a dash, "-". For example,

```
ffff-ffff-ffff
```

would be a valid entry for a MAC address mask in IMC.

The MAC address and its mask must be separated by a forward slash, "/".

A valid entry for a MAC Address/Mask would be

```
0014-2ad9-05f7/ffff-ffff-ffff
```

- **Variable Address**: Allows you to create a named variable without requiring you to enter the MAC addresses/masks in the template. The named variable then serves as a placeholder for entering a MAC address/mask combination when you import the template as a rule set into an existing ACL.
  - a. Enter a name for this variable in the field to the right.

9. Select the 802.1 priority you want to apply to this ACL rule from the **802.1 Priority** list.

10. Select the Layer 2 encapsulation type you want to apply to this ACL rule from the **Encapsulation Type** list.
11. Enter the Source VLAN ID by entering it in the Source VLAN ID field. This field cannot contain question marks or blank spaces.

12. Select the Layer 2 frame type from the Based Frame Type list.

13. If you selected Ethernet Frame or 802.2 Ethernet Frame in the Base Frame Type list, you must specify a code in the Code field. A valid entry for this field includes any four character hexadecimal value.

14. Click OK to accept the modifications to the rule.

15. Click OK to accept the modifications to the template.

Modifying a user-defined rules in a user-defined ACL template

To modify the user-defined rule of a user-defined ACL template:

1. Navigate to ACL Template:
   a. Click the Service tab from the tabular navigation system on the top.
   b. Click the ACL Management icon located under the Resource and Configuration Management section of the Service tab.
   c. Click the ACL Template link located under ACL Management on the navigation tree on the left. The Template List displays in the main pane of the page.

2. Click the icon in the Modify field associated with the user-defined template you want to modify. The Modify Template page displays with the Rule List for the selected ACL template in the main pane.

3. Click the icon in the Modify field associated with the rule you want to modify.

4. Select the action you want to take by clicking the radio button to the left of the option you want to apply to this rule:
   o Select permit if, upon matching the specified conditions, the packet should be forwarded, or
   o Select deny if, upon matching the specified conditions, the packet should be discarded.

5. Enter a named variable for this ACL template in the Time Range field allowing you to create a named variable without requiring you enter the Time Range in the template. The named variable then serves as a placeholder for Time Range you created using the Assistant combination when you import the template as a rule set into an existing ACL.

6. You can modify or enter up to eight hexadecimal patterns, masks, and offsets for matching the contents of a packet and applying the actions specified in the rule when a hexadecimal pattern is matched. The following rules and guidelines apply to constructing a valid hexadecimal string, mask, and offset value:
   o A rule string must be expressed in hexadecimal only
   o A mask must be expressed in hexadecimal only
   o A rule string length must be equal to its mask length
   o Rule string and mask length must be in multiples of 2
   o The minimum length of a rule string and mask is 2
   o The maximum length of a rule string and mask is 160
   o Offsets must be expressed as a decimal integer
- Offset range varies by the mask length
- The minimum value for an offset is 0
- The maximum value for an offset is 79
- The offset must increase progressively
  a. Enter a hexadecimal pattern to be matched in the Rule String field.
  b. Enter a mask in the Mask field.
  c. Enter the offset in the Excursion field.
  d. Enter up to eight Rule String/Mask/Excursion combinations.
7. Click OK to accept the modifications to the Rule String/Mask/Excursion combinations.
8. Click OK to accept the modifications to the template.

Copying a rule in a template

You can copy an existing rule in a template to a new rule in the same template and make modifications to the new copy.

To copy an existing rule in a template and make modifications to it:
1. Navigate to ACL Template:
   a. Click the Service tab from the tabular navigation system on the top.
   b. Click the ACL Management icon located under the Resource and Configuration Management section of the Service tab.
   c. Click the ACL Template link located under ACL Management on the navigation tree on the left. The Template List displays in the main pane of the page.
2. Click the icon in the Modify field associated with the template you want to modify.
   The Modify Template page displays with the list of rules for the associated template in the Rule Maintenance section of the page.
3. Click the icon in the Copy field associated with the rule you want to copy.
   You can make any modifications to the copy of a rule that you can to the rule itself, including creating new rules.
   The steps for creating and modifying rules in a template vary by the template type to which the rule belongs. For more information modifying rules in a template, see "Adding or modifying a basic rule in a basic ACL rule set" (page 744) and specifically to the section that how to modify the type of rule you want to copy.
4. Click OK when you have finished modifying the copy to create the new copy.

Deleting rules from a template

To delete one or more rules from a template:
1. Navigate to ACL Template:
   a. Click the Service tab from the tabular navigation system on the top.
   b. Click the ACL Management icon located under the Resource and Configuration Management section of the Service tab.
c. Click the **ACL Template** link located under **ACL Management** on the navigation tree on the left. The **Template List** displays in the main pane of the page.

2. Click the icon ![Modify](modify_icon.png) in the **Modify** field associated with the template you want to delete rules from. The **Modify Template** page displays with the list of rules for the associated template in the **Rule Maintenance** section of the page.

3. Click the checkboxes 🅱️ to the left of the sequence numbers for the rules you want to delete.

4. Click **Delete**.

5. Click **OK** to confirm the deletion of the selected rules.

6. Click **OK** to complete the modifications to the template.

**Managing ACL resources in IMC**

Resources are comprised of the configured ACLs and their rules sets that are deployed to devices in the network. ACL Management offers you a rich feature set for simplifying the task of resource management. Through the Resource List, you have a single portal for viewing and managing all of the ACLs that can be deployed to network devices. From the **ACL Resource** list, you can view all four types of ACLs, add new ACLs, rename existing ACLs and delete ACLs that are no longer needed. You can also drill down into the **Rule Set List** to view all rules for each ACL, take actions on all rules in the list and import the contents of a template into a new rule set.

The **Rule Set List** also contains a wizard you can use to modify existing rules of a set, including modifying, copying, or deleting existing rules. You can also redefine the order of appearance of rules in a set which can be critical to the effectiveness of a rule set when the match order is based on the order of the rule appearance.

**Managing ACLs**

ACL Management provides you with a single portal for viewing and accessing all ACLs.

**Viewing the ACL resource list**

To view the list of ACL resources in IMC:

1. Navigate to **ACL Resource**:
   a. Click the **Service** tab from the tabular navigation system on the top.

   b. Click the ![ACL Management](management_icon.png) icon located under the **Resource and Configuration Management** section of the **Service** tab.

   c. Click the ![ACL Resource](resource_icon.png) link located under **ACL Management** on the navigation tree on the left. The **ACL Resource** list displays in the main pane of the **ACL Resource** page.

**ACL resource list**

- **ACL Identifier**: Contains the identifier for the ACL. The ACL Identifier serves as a link for navigating to the **Rule Set List** page for the associated ACL. For more information on the Rule Set List, see "Viewing the rule set list for an ACL" (page XX).

- **ACL Resource Name**: Contains a descriptive name for the associated ACL.
- **ACL Type**: Identifies the ACL type. An ACL can be a **Basic**, **Advanced**, **Link**, or **User-Defined** ACL in IMC.

- **Rename**: Contains a link for modifying the **ACL Resource Name** with the associated ACL.

If the **ACL Resource** list contains multiple entries, the following navigational aids may appear:

- Click **»** to page forward in the **ACL Resource** list.
- Click **»** to page forward to the end of the **ACL Resource** list.
- Click **«** to page backward in the **ACL Resource** list.
- Click **«** to page backward to the front of the **ACL Resource** list.

2. Click 8, 15, 50, 100, or 200 from the right side of the main pane to configure how many items per page you want to view.

You can sort the **ACL Resource** list by the **ACL Identifier**, **ACL Resource Name**, and **ACL Type** fields. Click the column label to sort the list by the selected field. The column label is a toggle switch that allows you to toggle between the various sort options specific to each field.

### Adding an ACL

To add an access control list:

1. Navigate to **ACL Resource**:
   - a. Click the **Service** tab from the tabular navigation system on the top.
   - b. Click the **ACL Management** icon located under the **Resource and Configuration Management** section of the **Service** tab.
   - c. Click the **ACL Resource** link located under **ACL Management** on the navigation tree on the left. The **ACL Resource** list displays in the main pane of the **ACL Resource** page.

2. Click **Add**.
   - The **Add ACL Resource** page appears.

3. Select the type of ACL you want to create by clicking the radio button **»** to the left of the desired **ACL Identity Type**. Option for identifying the ACL is by **Number** or by **Name**.

4. Select the type of ACL you want to create by selecting it from the **ACL Type** list. Operators have four ACL types to choose from:
   - o **Basic**: Enables you to create rules based on source IP addresses.
   - o **Advanced**: Enables you to define rules based on Layer 3 and Layer 4 information including IP source and destination addresses, TCP and UDP port information, as well as protocol specific features.
   - o **Link**: Enables you to define rules based on Layer 2 information including source MAC and destination MAC addresses, VLAN priority information as well as data link layer protocol type.
   - o **User-Defined**: Enables you to define a hexadecimal pattern and mask and the offset in the packet header to begin the pattern matching. When a pattern is matched, the conditions of the rule in the ACL template will be applied.

5. Enter a valid ACL identifier for the ACL type you have selected in the **ACL Identifier** field. Valid entries for each ACL type is provided below:
   - o **Basic**: Any number in the range of 1-99, 1300-1399, or 2000-2999.
Advanced: Any number in the range of 100-199, 2000-2699, or 3000-3999.

Link: Any number in the range of 4000-4999.

User Defined: Any number in the range of 5000-5999.

6. Enter a valid name for the ACL in the **ACL Resource Name** field.
   A valid length for an ACL name is 1 – 32 characters. An ACL name cannot begin with a space [ ].

7. Click **OK** to create the ACL.

**Renaming an ACL**

To rename an access control list:

1. Navigate to **ACL Resource**:
   a. Click the **Service** tab from the tabular navigation system on the top.
   b. Click the **ACL Management** icon located under the **Resource and Configuration Management** section of the **Service** tab.
   c. Click the **ACL Resource** link located under **ACL Management** on the navigation tree on the left.
      The **ACL Resource** list displays in the main pane of the **ACL Resource** page.

2. Click the icon in the **Rename** field associated with the ACL you want to rename.
   The **Rename ACL Resource** dialog box appears.

3. Delete the current value in the **ACL Resource Name** field and enter the new name for the ACL.

4. Click **OK** to apply the new name to the ACL resource.

**Deleting ACLs**

To delete one or more ACLs from the ACL Management:

1. Navigate to **ACL Resource**:
   a. Click the **Service** tab from the tabular navigation system on the top.
   b. Click the **ACL Management** icon located under the **Resource and Configuration Management** section of the **Service** tab.
   c. Click the **ACL Resource** link located under **ACL Management** on the navigation tree on the left.
      The **ACL Resource** list displays in the main pane of the **ACL Resource** page.

2. Click the checkbox to the left of the **ACL Identifiers** you want to delete.

3. Click **Delete**.

4. Click **OK** to confirm the deletion of the selected ACLs.

**Managing rule sets**

ACL Management provides you with a rich feature set for managing ACLs and the rule sets that constitute them. From the **ACL Resource** list, you can drill down into the **Rule Set List** to view every rule set for a given ACL. From the **Rule Set List** page, you can view rule set information including basic rule set information, time ranges applied to rules in the list. In addition, you can view information for every rule in the list.
From the **Rule Set List**, you can also take action rules all of the rules in the list including adding new rule sets, modifying, copying, deploying, and deleting existing rule sets, as well as importing the contents of a template into a new rule set of an existing ACL.

You can also navigate to the **Modify Rule Set** wizard for modifying the existing rules of a rule set. Using this wizard, you can modify, copy, or delete an existing rule, or redefine the order of appearance of rules in a set. In addition, you can initiate the evaluation of any rule set for optimizing its effect on network performance and have ACL Management make and implement recommendations for the improvement of rule sets.

**Viewing rule set information**

Rule sets are the core of an ACL, providing you with a single view of rule sets via the **Rule Set List**. From this list, you can view detailed information for every rule set in an ACL. Operators can also view detailed information for every rule in a rule set, including rule and time range information.

**To view the Rule Set List for an ACL resource in IMC:**

1. **Navigate to ACL Resource:**
   a. Click the **Service** tab from the tabular navigation system on the top.
   b. Click the **ACL Management** icon located under the **Resource and Configuration Management** section of the **Service** tab.
   c. Click the **ACL Resource** link located under **ACL Management** on the navigation tree on the left.

   The **ACL Resource** list displays in the main pane of the **ACL Resource** page.

2. **Click the ACL Identifier for the ACL for which you want to view the Rules Set List.**

   The **Rule Set List** displays in the main pane of the **ACL Resource→<ACL Resource Name (ACL Identifier)>** page.

**Rule set list field names and explanations:**

- **Rule Set Name**: Contains the name of the Rule Set. The **Rule Set Name** serves as a link for navigating to the **Rule Set Info** page for the associated Rule Set. This page displays Rule Set configuration information for the associated Rule Set. For more information viewing rule set information, see "Viewing rule set information" (page 700).
- **Description**: Contains a description for the associated Rule Set.
- **Deploy**: Contains a link for deploying the associated Rule Set.
- **Copy**: Contains a link for copying the associated Rule Set.
- **Modify**: Contains a link for modifying the associated Rule Set.

If the **Rule Set List** contains multiple entries, the following navigational aids may appear:

- Click to page forward in the **Rule Set List**.
- Click to page forward to the end of the **Rule Set List**.
- Click to page backward in the **Rule Set List**.
- Click to page backward to the front of the **Rule Set List**.

3. **Click 8, 15, 50, 100, or 200 from the right side of the main pane to configure how many items per page you want to view.**
You can sort the Rule Set List by the Rule Set Name and the Description fields. Click the column label to sort the list by the selected field. The column label is a toggle switch that allows you to toggle between the various sort options specific to each field.

To view the information for a Rule Set for an ACL:

1. Navigate to ACL Resource:
   a. Click the Service tab from the tabular navigation system on the top.
   b. Click the ACL Management icon located under the Resource and Configuration Management section of the Service tab.
   c. Click the ACL Resource link located under ACL Management on the navigation tree on the left. The ACL Resource list displays in the main pane of the ACL Resource page.

2. Click the ACL Identifier for the ACL for which you want to view the Rules Set List. The Rule Set List displays in the main pane of the ACL Resource page.

3. Click the name in the Rule Set Name field for the Rule Set for which you want to view configuration information. The Rule Set Info page displays in the main pane of the ACL Resource page. This page includes three fields, Basic Info, Rule Info, and Time Range Info. The field for the Rule Info field varies based on ACL type.

   Basic info
   - ACL Identifier: Contains the identifier for the ACL.
   - ACL Resource Name: Contains a descriptive name for the associated ACL.
   - ACL Type: Identifies the ACL type. An ACL can be a Basic, Advanced, Link, or User-Defined ACL in IMC.
   - ACL Description: Contains a description for the associated ACL.
   - Rule Set Name: Contains the name of the Rule Set.
   - Match Order: Contains the match order type for the associated rule. The Match Order can either be Config or Auto. Rule Set Description: Contains a description for the associated Rule Set.

   Rule info for basic ACL
   - No.: Contains the sequence or rule number for the associated rule in the Rule Set. The value in the sequence filed serves as a link for navigating to the Rule Info page for the associated rule. This page displays rule configuration information for the associated rule. For more information viewing rule information, refer to the section of this manual on "Viewing rule set information" (page 700).
   - Action: Contains the access control action specified in the associated rule. Actions include permit and deny.
   - Source Address: Contains the source address specified in the associated rule. Actions include permit and deny.

   Rule info for Advanced ACL
   - No.: Contains the sequence or rule number for the associated rule in the Rule Set. The value in the sequence field serves as a link for navigating to the Rule Info page for the associated rule. This page displays rule configuration information for the associated rule. For more information viewing rule information, see "Viewing ACL templates" (page 659).
- **Action**: Contains the access control action specified in the associated rule. Actions include permit and deny.
- **Protocol**: Contains the protocol specified in the associated rule for which the action will be taken.
- **Source Address**: Contains the source address specified in the associated rule for which the action is taken. For example, if the action is to permit IP traffic, this field identifies the source IP address from which IP traffic is permitted.
- **Destination Address**: Contains the destination address specified in the associated rule for which the action is taken. For example, if the action is to permit IP traffic, this field identifies the destination IP address to which IP traffic is permitted.

**Rule info for link ACL:**
- **No.**: Contains the sequence or rule number for the associated rule in the Rule Set. The value in the sequence field serves as a link for navigating to the **Rule Info** page for the associated rule. This page displays rule configuration information for the associated rule. For more information viewing rule information, see "Viewing ACL templates" (page 659).
- **Action**: Contains the access control action specified in the associated rule. Actions include permit and deny.
- **Source MAC Addr**: Contains the source MAC address specified in the associated rule for which the action will be taken.
- **Destination MAC Addr**: Contains the destination MAC address specified in the associated rule for which the action will be taken.

**Rule info for user-defined ACL:**
- **No.**: This field contains the sequence or rule number for the associated rule in the Rule Set. The value in the **No.** field serves as a link for navigating to the **Rule Info** page for the associated rule. This page displays rule configuration information for the associated rule. For more information viewing rule information, see "Viewing ACL templates" (page 659).
- **Action**: Contains the access control action specified in the associated rule. Actions include permit and deny.
- **Matching String**: Contains the hexadecimal string to be matched in a packet, the mask, and the offset values for a user-defined pattern-matching rule.

**Time range info:**
- **No.**: Contains the sequence or rule number for the time range specified for the associated the Rule Set.
- **Name**: Contains the name assigned to the Time Range specified for the associated rule set. The value in the **Name** field serves as a link for navigating to the **View Time Range** page for the associated rule. This page displays time range configuration information for the associated rule.

**To view the rule information for a rule for an ACL resource:**
1. Navigate to **ACL Resource**:
   a. Click the **Service** tab from the tabular navigation system on the top.
   b. Click the **ACL Management** icon located under the **Resource and Configuration Management** section of the **Service** tab.
   c. Click the **ACL Resource** link located under **ACL Management** on the navigation tree on the left. The **ACL Resource** list displays in the main pane of the **ACL Resource** page.
2. Click the **ACL Identifier** for the ACL for which you want to view the **Rule Set List**.
   The **Rule Set List** displays in the main pane of the **ACL Resource→<ACL Resource Name (ACL Identifier)>** page.

3. Click the name in the **Rule Set Name** field for the Rule Set for which you want to view configuration information.
   The **Rule Set Info** displays in the main pane of the **ACL Resource→<ACL Resource Name (ACL Identifier)>→<Rule Set Name>** page.

4. Click the rule **No.** in the **Rule Info** section of the **Rule Set Info** page for which you want to view rule information.
   The ACL Rule Information page varies based on ACL type.

**Rule Info page for Basic ACL**

The **Rule Info** page displays in the main pane of the **ACL Resource→<ACL Resource Name (ACL Identifier)>→<Rule Set Name>→View Basic Rule** page.

The Basic Info field names and explanations include:

- **Action**: Contains the access control action specified in the associated rule. Actions include **permit** and **deny**.
- **Time Range**: Contains the time range specified for this rule.
- **Source Address**: Contains the source address specified in the associated rule for which the action is taken. For example, if the action is to permit IP traffic, this field identifies the source IP address from which IP traffic is permitted.

The Other Settings field names and explanations include:

- **Fragment**: Identifies whether or not the rule is configured to apply to all fragments (**Yes**) or to apply to first fragments (**No**).
- **Logging**: Identifies whether or not logging is enabled.
- **VPN Instance**: Identifies the VPN instance name for the VPN instance to which this rule is applied. The VPN-instance-name argument takes a case sensitive string of 0-31 characters. If no VPN is specified, the rule applies only to non-VPN packets.

**Rule Info page for advanced ACL**

The **Rule Info** page displays in the main pane of the **ACL Resource→<ACL Resource Name (ACL Identifier)>→<Rule Set Name>→View Advanced Rule** page.

The Basic Info field names and explanations include:

- **Protocol**: Contains the protocol specified in the associated rule for which the action to be taken. If the Protocol is TCP or UDP, the Advanced Settings field displays below the Basic Info field.
- **Action**: Contains the access control action specified in the associated rule. Actions include **permit** and **deny**.
- **Time Range**: Contains the time range specified for this rule.
- **Source Address**: Contains the source address specified in the associated rule for which the action to be taken. For example, if the action is to permit IP traffic, this field identifies the source IP address from which IP traffic is permitted.
- **Destination Address**: Contains the destination address specified in the associated rule for which the action to be taken. For example, if the action is to permit IP traffic, this field identifies the destination IP address to which IP traffic is permitted.
The Advanced Settings field names and explanations include:

- **Source Port**: Contains the source port specified in the associated rule for which the action to be taken.
- **Destination Port**: Contains the destination port specified in the associated rule for which the action to be taken.

The Other Settings field names and explanations include:

- **IP Priority**: Contains the IP priority setting for this rule.
- **ToS Value**: Contains the type of service setting for this rule.
- **DSCP Value**: Contains the differentiated control services protocol value for this rule.
- **Fragment**: Identifies whether or not the rule is configured to apply to all fragments (Yes) or to apply to first fragments (No).
- **Logging**: Identifies whether or not logging is enabled.
- **VPN Instance**: Identifies the VPN instance name for the VPN instance to which this rule is applied. The VPN-instance-name argument takes a case sensitive string of 0-31 characters. If no VPN is specified, the rule applies only to non-VPN packets.

**Rule info page for link ACL:**

The Rule Info page displays in the main pane of the ACL Resource→<ACL Resource Name (ACL Identifier)>→<Rule Set Name>→View Link Rule page.

The Basic Info field names and explanations include:

- **Protocol**: Contains the protocol specified in the associated rule for which the action is taken. If the Protocol is TCP or UDP, the Advanced Settings field appears below the Basic Info field.
- **Action**: Contains the access control action specified in the associated rule. Actions include permit and deny.
- **Time Range**: Contains the time range specified for this rule.
- **Source MAC Addr**: Contains the source MAC address specified in the associated rule for which the action is taken.
- **Destination MAC Addr**: This field contains the destination MAC address specified in the associated rule for which the action is taken.

The Other Settings field names and explanations include:

- **802.1 Priority**: Contains the priority you want to apply to this ACL rule.
- **Encapsulation Type**: Contains the Layer 2 encapsulation type you want to apply to this ACL rule.
- **Source VLAN ID**: Contains the source VLAN ID.
- **Base Frame Type**: Contains the Layer 2 frame type.
- **Code**: If you selected Ethernet Frame or 802.2 Ethernet Frame in the Base Frame Type field, you must specify a code in the Code field.
  A valid entry for this field includes any four character hexadecimal value.
- **Mask**: If you selected Ethernet Frame or 802.2 Ethernet Frame in the Base Frame Type field, you must also specify a mask in the Mask field.
  A valid entry for this field includes any four character hexadecimal value.

**Rule Info page for user-defined ACL:**
The Rule Info page displays in the main pane of the 

ACL Resource→<ACL Resource Name (ACL Identifier)>→<Rule Set Name>→View User-Defined Rule page.

The Basic Info field names and explanations include:

- **Action**: Contains the access control action specified in the associated rule. Actions include permit and deny.
- **Time Range**: Contains the time range specified for this rule.
- **Rule String**: Contains up to eight hexadecimal patterns, masks, and offsets for matching the contents of a packet and applying the actions specified in the rule when a hexadecimal pattern is matched.

To view the time range information for a rule for an ACL resource:

1. Navigate to ACL Resource:
   a. Click the Service tab from the tabular navigation system on the top.
   b. Click the ACL Management icon located under the Resource and Configuration Management section of the Service tab.
   c. Click the ACL Resource link located under ACL Management on the navigation tree on the left.
      The ACL Resource list displays in the main pane of the ACL Resource page.

2. Click the ACL Identifier for the ACL for which you want to view the Rules Set List.
   The Rules Set List displays in the main pane of the ACL Resource→<ACL Resource Name (ACL Identifier)> page.

3. Click the name in the Rule Set Name field for the Rule Set for which you want to view configuration information.
   The Rule Set Info displays in the main pane of the ACL Resource→<ACL Resource Name (ACL Identifier)>→<Rule Set Name> page.

4. Click the rule Name field in the Time Range Info section of the Rule Set Info page for the rule for which you want to view time range information.
   The View Time Range page displays in the main pane of the ACL Resource→<ACL Resource Name (ACL Identifier)>→<Rule Set Name>→View Time Range page.

**Time range list**

- **Start Time**: Contains the start of the time range in hours and minutes that the associated rule is or will be in effect.
- **End Time**: Contains the end of the time range in hours and minutes that the associated rule is or will be in effect.
- **Type**: Identifies what type of time range is or will be in effect.
- **Execution Period**: Identifies the days of the week that the associated time range is or will be in effect.

**Adding rule sets**

Rule sets are the core of an ACL because they contain the conditions that define how traffic is handled by network devices. An ACL can contain one or more rule sets and each rule set can contain one or more rules that determine whether or not traffic is to be forwarded.
An ACL is defined by its type and an ACL can contain rule sets of the same type only. There are four types of ACLs: Basic, Advanced, Link, and User-Defined.

Adding a basic rule set

Basic ACLs enable you to create one or more rules based on source IP addresses or address ranges and their subnet masks. A valid numeric range for assigning ACL Identifiers to basic ACLs is 1-99, 1300-1999, or 2000-2999. When adding a rule set to an ACL, the ACL type automatically defines the rule set you can create.

To add a basic rule set to an ACL resource:
1. Navigate to ACL Resource:
   a. Click the Service tab from the tabular navigation system on the top.
   b. Click the ACL Management icon located under the Resource and Configuration Management section of the Service tab.
   c. Click the ACL Resource link located under ACL Management on the navigation tree on the left. The ACL Resource list displays in the main pane of the ACL Resource page.
2. Click the ACL Identifier for the basic ACL for which you want to create a new rule set. Refer to the ACL Type field in the ACL Resource list for identifying ACLs for which the type is Basic. The Rule Set List for the selected ACL displays in the main pane of the ACL Resource→<ACL Resource Name (ACL Identifier)> page.
3. Click Add.
   The Basic Info step of the Add Rule Set page appears.
   Several fields are already configured and cannot be changed. These include the ACL Identifier, the ACL Type, and the ACL Resource Name. These parameters cannot be changed because they are inherited by the ACL to which this rule set belongs.
   You can create rule sets of the same type as the type of ACL to which the rule set belongs.
4. Enter a name for the rule set in the Rule Set Name field.
   A valid length for a rule set name is 1 – 32 characters.
5. Select the match order you want to apply to this rule set by clicking the radio button to the left of the Match Order option you want to use.
   Options include Config and Auto. If you select Config, IMC matches rules in the order in which they were configured, but only works for devices that support it. If you select Auto, IMC matches rules based on the principle of depth priority.
6. Enter a brief description for this ACL in the ACL Description field.
   A valid length for this field is 0 – 127 characters.
7. Enter a brief description for this rule set in the Rule Set Description field.
   A valid length for this field is 0 – 127 characters.
8. If you want to apply a time range to the rule set, click the checkbox to the left of Configure ACL Rules with Time Range.
9. Click Next.
10. Do one of the following:
If you checked the box to Configure ACL Rules with Time Range, click Add under Configure Time Range to add a time range to this rule set, or

If you do not want to add a time range, skip to Step 14.

11. Enter a name for the time range in the Name field of the Add Time Range page. Time Range names must begin with a letter [A-Z] and consist of 1-32 characters. Blank spaces [ ] and question marks [?] are not permitted. Uppercase letters may be converted to lowercase letters by some devices after deployment.

12. Click Add to enter a time range.

The Add Time Range dialog box appears.

13. Select the type of time range you want to create by clicking the radio button ○ to the left of the desired time range type:

- Fixed if you want to identify a specific and finite start and end date and time, or
- Cyclic if you want the time range to recur for selected days of the week.

See "Configuring fixed time ranges" (page 655) to configure fixed time ranges and "Configuring cyclic time ranges" (page 656) to configure cyclic time ranges.

14. Click Add on the Configure Rule page to configure a new rule.

The Add Rule page appears.

15. Select the action you want to take by clicking the radio button ○ to the left of the option you want to apply to this rule:

- Select permit if, upon matching the specified conditions, the packet should be forwarded, or
- Select deny if, upon matching the specified conditions, the packet should be discarded.

16. Select the time range you want to apply to this rule from the Time Range list you created in the Step 10.

17. Select the source IP address option you want to use by clicking the radio button ○ to the left of the desired option in the Source Address field of the Add Rule page.

This option specifies where the pattern matching occurs in this rule. In this case, the pattern matching applies to the source IP address.

- All: Allows you to permit or deny traffic for all IP addresses.
- IP Address/Mask: Allows you to enter a specific IP address and its subnet mask for which you want to either permit or deny traffic for.

Enter an IP address/subnet mask combination in the IP Address/Mask field. Note that the subnet mask must be entered in dotted decimal notation. A valid IP address/subnet mask using dotted decimal notation would be

192.168.1.0/255.255.255.0

A forward slash "/" must be used to separate the IP address from the subnet mask.

18. Do one of the following:

- Click the radio button ○ to the left of Yes in the Fragment option if you want to apply the rule to each fragment, or
- Click the radio button ○ to the left of No in the Fragment option if you want to apply the rule to first fragments.

Traditional packet filtering matched only first fragments of IPv4 packets and allowed all subsequent non-first fragments to pass through. This resulted in security risks as hackers can fabricate non-first fragments to attack networks.
19. Click the radio button ☐ to the left of Yes in the **Logging** option if you want to enable logging for this rule.
   This feature enables the logging of packet filtering only when a module (for example, a firewall) is using the ACL supports logging.

20. Enter the VPN instance you want to apply to this rule by entering the VPN-instance-name in the **VPN Instance** field.
   A valid entry must be 0 – 31 characters that cannot contain question marks or blank spaces. This field is case sensitive. If no VPN instance is specified in this field, the rule applies only to non-VPN packets.

21. Enter the VPN

22. Click **OK** to create the rule you have just configured.

23. To add more rules, modify, copy, sort, optimize or delete existing rules, select one of the following:
   - To add more rules to the ACL, repeat **Steps 14-21**, or
   - To modify rules you have already created, click the **Modify** icon associated with the rule sequence you want to modify. For more information modifying a rule set, see "Adding or modifying a basic rule in a basic ACL rule set" (page 744), or
   - To copy rules you have already created, click the **Copy** icon associated with the rule sequence you want to copy. For more information copying a rule set, see "Copying a rule in an ACL rule set" (page 750), or
   - Rules that belong to a rule set that is configured with a **Match Order** of ‘Config’ are executed in the order in which they appear in the rule set. The order in which rules appear in a rule set is initially defined by the order in which they are created. You can, however, reorder the rules in a rule set using the **Sort** feature. For more information using Sort to redefine the order of appearance of rules in a rule set, see "Using sort to reorder the rules in an ACL rules set" (page 752), or
   - ACLs can have a profound effect on the performance of networks. **ACL Management** automatically evaluates the effectiveness of rules and their effect on overall network performance as you add rules to a rule set. However, you can also manually perform an analysis of a rule set and optimize its effect on network performance using the **Optimize** feature. For more information using this feature, see "Optimizing the rules in a rule set" (page 752), or
   - To delete one or more rules from a rule set, see "Deleting rules from an ACL rule set" (page 751).

24. Click **Finish** when you have finished creating rules for this rule set.
   Once you have created an ACL you are ready to deploy the ACL to devices using the ACL Management’s ACL Deployment wizard. For more information deploying ACLs, see "Deploying ACLs using IMC’s ACL deployment wizard" (page 782).

**Adding an advanced rule set**

Advanced ACLs enable you to define rules based on Layer three and Layer four information including IP source and destination addresses, TCP and UDP port information, as well as protocol specific features. A valid numeric range for assigning ACL Identifiers to advanced ACLs is 100-199, 2000-2699, or 3000-3999.

To add an advanced rule set to an existing ACL resource:

1. Navigate to **ACL Resource**:
   a. Click the **Service** tab from the tabular navigation system on the top.
b. Click the **ACL Management** icon located under the **Resource and Configuration Management** section of the **Service** tab.

c. Click the **ACL Resource** link located under **ACL Management** on the navigation tree on the left. The **ACL Resource** list displays in the main pane of the **ACL Resource** page.

2. Click the **ACL Identifier** for the advanced ACL for which you want to create a new rule set. Refer to the **ACL Type** field in the **ACL Resource** list for identifying ACLs for which the type is **Advanced**. The **Rule Set List** for the selected ACL displays in the main pane of the **ACL Resource** page.

3. Click **Add**.

   The **Basic Info** step of the **Add Rule Set** page appears.

   Several fields are already configured and cannot be changed. These include the **ACL Identifier**, the **ACL Type**, and the **ACL Resource Name**. These cannot be changed because they are inherited by the ACL to which this rule set belongs.

   You can create rule sets of the same type as the type of ACL to which the rule set belongs.

4. Enter a name for the rule set in the **Rule Set Name** field.
   A valid length for a rule set name is 1 – 32 characters.

5. Select the match order you want to apply to this rule set by clicking the radio button ○ to the left of the **Match Order** option you want to use. Options include **Config** and **Auto**:
   - **Config**: IMC matches rules in the order in which they were configured. Note that this feature works only for devices that support it.
   - **Auto**: IMC matches rules based on the principle of depth priority.

6. Enter a brief description for this ACL in the **ACL Description** field.
   A valid length for this field is 0 – 127 characters.

7. Enter a brief description for this rule set in the **Rule Set Description** field.
   A valid length for this field is 0 – 127 characters.

8. Do one of the following:
   - If you checked the box to **Configure ACL Rules with Time Range**, click **Add** under **Configure Time Range** to add a time range to this rule set, or
   - If you do not want to add a time range, skip to **Step 14**.

9. Enter a name for the time range in the **Name** field of the **Add Time Range** page.
   Time Range names must begin with a letter [A-Z] and consist of 1-32 characters. Blank spaces [ ] and question marks [?] are not permitted. Uppercase letters may be converted to lowercase letters by some devices after deployment.

10. Click **Add** to enter a time range.

    The **Add Time Range** dialog box appears.

11. Select the type of time range you want to create by clicking the radio button ○ to the left of the desired time range type:
    - **Fixed** if you want to identify a specific and finite start and end date and time, or
    - **Cyclic** if you want the time range to recur for selected days of the week.

12. Click **Add** on the **Configure Rule** page to configure a new rule.
13. See "Configuring fixed time ranges" (page 655) to configure fixed time ranges and "Configuring cyclic time ranges" (page 656) to configure cyclic time ranges.

14. Select the protocol for which you want to permit or deny traffic from the Protocol list.

15. Select the action you want to take by clicking the radio button ☐ to the left of the option you want to apply to this rule:
   o Select permit if, upon matching the specified conditions, the packet should be forwarded, or
   o Select deny if, upon matching the specified conditions, the packet should be discarded.

16. Select the time range you want to apply to this rule from the Time Range list you created in the Step 10.

17. Select the source IP address option you want to use by clicking the radio button ☐ to the left of the desired option in the Source Address section of the Configure Rule - Add Rule page.
   This option specifies where the pattern matching occurs in this rule. In this case, the pattern matching is applied to the source IP address.
   o All: Allows you to permit or deny traffic for all IP addresses.
   o IP Address/Mask: Allows you to enter a specific IP address and its subnet mask for which you want to either permit or deny traffic for.
   Enter an IP address/subnet mask combination in the IP Address/Mask field. The subnet mask must be entered in dotted decimal notation. A valid IP address/subnet mask using dotted decimal notation would be
   192.168.1.0/255.255.255.0
   A forward slash "/" must be used to separate the IP address from the subnet mask.

18. Select the destination IP address option you want to use by clicking the radio button ☐ to the left of the desired option in the Destination Address portion of the Configure Rule - Add Rule page.
   This option specifies where the pattern matching occurs in this rule. In this case, the pattern matching is applied to the destination IP address.
   o All: Allows you to permit or deny traffic for all IP addresses.
   o IP Address/Mask: Allows you to enter a specific IP address and its subnet mask for which you want to either permit or deny traffic.
   Enter an IP address/subnet mask combination in the IP Address/Mask field. Note that the subnet mask must be entered in dotted decimal notation. A valid IP address/subnet mask using dotted decimal notation would be:
   192.168.1.0/255.255.255.0
   A forward slash "/" must be used to separate the IP address from the subnet mask.

19. If you selected TCP or UDP as the protocol you want to apply this ACL rule to in Step 12, you must also specify the source TCP or UDP port numbers:
   a. Select the source TCP or UDP port by clicking the radio button ☐ to the left of the port option you want to apply in the Source Port portion of the Configure Rule - Add Rule page:
      o Undefined: Allows you to permit or deny traffic for all TCP or UDP port numbers.
      o Specified Port: Allows you to identify a specific TCP or UDP port number or range of numbers.
   b. Click the radio button ☐ to the left of Specified Port and select the operator you want to use from the list located to the right of the Specified Port option.
   c. Enter the TCP or UDP port number in the Port field.

20. If you selected TCP or UDP as the protocol you want to apply this ACL rule to, you must also specify the destination TCP or UDP port numbers:
a. Select the destination TCP or UDP port by clicking the radio button \( \bigcirc \) to the left of the port option you want to apply in the *Destination Port* section of the *Configure Rule – Add Rule* page:

- **Undefined**: Allows you to permit or deny traffic for all TCP or UDP port numbers.
- **Specified Port**: Allows you to identify a specific TCP or UDP port number or range of numbers.

b. Click the radio button \( \bigcirc \) to the left of *Specified Port* and select the operator you want to use from the list located to the right of the *Specified Port* option.

c. Enter the TCP or UDP port number in the *Port* field.

21. If you selected TCP or UDP as the protocol you want to apply this ACL rule to in **Step 12**, you could be prompted to select these options:

- Click the radio button \( \bigcirc \) to the left of *Yes* in the *HP ACK* option if you want to apply the rule to match the TCP ACK, otherwise click on the radio button to the left of *No*.
- Click the radio button \( \bigcirc \) to the left of *Yes* in the *HP FIN* option if you want to apply the rule to match the TCP FIN, otherwise click on the radio button to the left of *No*.
- Click the radio button \( \bigcirc \) to the left of *Yes* in the *HP RST* option if you want to apply the rule to match the TCP RST, otherwise click on the radio button to the left of *No*.
- Click the radio button \( \bigcirc \) to the left of *Yes* in the *HP SYN* option if you want to apply the rule to match the TCP SYN, otherwise click on the radio button to the left of *No*.

The *HP ACK*, *HP FIN*, *HP RST*, or *HP SYN* settings are valid only for the HP E series devices.

22. Select the IP priority you want to apply to ACL from the *IP Priority* list.

23. Select the Type of Service for this ACL from the *TOS Value* list.

24. Select the DSCP value you want to apply to this ACL from the *DSCP Value* list.

25. Do one of the following:

- Click the radio button \( \bigcirc \) to the left of *Yes* in the *Fragment* option if you want to apply the rule to each fragment, or
- Click the radio button \( \bigcirc \) to the left of *No* in the *Fragment* option if you want to apply the rule to first fragments.

Traditional packet filtering matched only first fragments of IPv4 packets and allowed all subsequent non-first fragments to pass through. This resulted in security risks as hackers can fabricate non-first fragments to attack networks.

26. Click the radio button \( \bigcirc \) to the left of *Yes* in the *Logging* option if you want to enable logging for this rule.

This feature enables the logging of packet filtering only when a module (for example, a firewall) using the ACL supports logging.

27. Enter the VPN instance you want to apply to this rule by entering the VPN-instance-name in the *VPN Instance* field.

A valid entry must be 0 – 31 characters that cannot contain question marks or blank spaces. This field is case sensitive. If no VPN instance is specified in this field, the rule applies to non-VPN packets only.

28. Click **OK** to create the rule you have just configured.

29. To add more rules, modify, copy, sort, optimize or delete existing rules, select one of the following:

- To add more rules to the ACL, repeat **Steps 14-27**, or
- To modify rules you have already created, click the **Modify** icon associated with the rule sequence you want to modify. For more information modifying a rule set, see "Adding or modifying an advanced rule in an advanced rule set" (page 745), or
To copy rules you have already created, click the **Copy** icon associated with the rule sequence you want to copy. For more information copying a rule set, see "Copying a rule in an ACL rule set" (page 750), or

Rules that belong to a rule set that is configured with a **Match Order** of **Config** are executed in the order in which they appear in the rule set. The order in which rules appear in a rule set is initially defined by the order in which they are created. You can, however, reorder the rules in a rule set using the **Sort** feature. For more information using Sort to redefine the order of appearance of rules in a rule set, see "Using sort to reorder the rules in an ACL rules set" (page 752), or

ACLs can have a profound effect on the performance of networks. ACL Management automatically evaluates the effectiveness of rules and their effect on overall network performance as you add rules to a rule set. However, you can also manually perform an analysis of a rule set and optimize its effect on network performance using the **Optimize** feature. For more information using this feature, see "Optimizing the rules in a rule set" (page 752), or

To delete one or more rules from a rule set, see "Deleting rules from an ACL rule set" (page 751).

**30.** Click **Finish** when you have finished creating rules for this rule set.

Once you have created an ACL you are ready to deploy the ACL to devices using the ACL Management’s ACL Deployment wizard. For more information deploying ACLs, see "Deploying ACLs using IMC’s ACL deployment wizard" (page 782).

### Adding a link rule set

Link ACLs enable you to define rules based on Layer 2 information including MAC source and destination addresses, VLAN priority information as well as link layer protocol type.

When you add a rule set to an existing ACL, the ACL type automatically defines the rule set you create.

To add a link rule set to an existing ACL resource:

1. **Navigate to ACL Resource:**
   a. Click the **Service** tab from the tabular navigation system on the top.
   b. Click the **ACL Management** icon located under the **Resource and Configuration Management** section of the **Service** tab.
   c. Click the **ACL Resource** link located under **ACL Management** on the navigation tree on the left. The **ACL Resource** list displays in the main pane of the **ACL Resource** page.

2. Click the **ACL Identifier** for the link ACL for which you want to create a new rule set. Refer to the **ACL Type** field in the **ACL Resource** list for identifying ACLs for which the type is **Link**.
   The **Rule Set List** displays in the main pane of the **ACL Resource**→<ACL Resource Name (ACL Identifier)> page.

3. Click **Add**.
   The **Basic Info** step of the **Add Rule Set** page appears.
   Several fields are already configured and cannot be changed. These include the **ACL Identifier**, the **ACL Type**, and the **ACL Resource Name**. These cannot be changed because they are inherited by the ACL to which this rule set belongs.
   You can create rule sets of the same type as the type of ACL to which the rule set belongs.

4. Enter a name for the rule set in the **Rule Set Name** field.
A valid length for a rule set name is 1 – 32 characters.

5. Select the match order you want to apply to this rule set by clicking the radio button to the left of the Match Order option you want to use.
   Options include Config and Auto:
   o If you select Config, IMC matches rules in the order in which they were configured. However, this feature works only for devices that support it.
   o If you select Auto, IMC matches rules based on the principle of depth priority.

6. Enter a brief description for this ACL in the ACL Description field.
   A valid length for this field is 0 – 127 characters.

7. Enter a brief description for this rule set in the Rule Set Description field.
   A valid length for this field is 0 – 127 characters.

8. If you want to apply a time range to the rule set, click the checkbox to the left of Configure ACL Rules with Time Range.

9. Click Next.

10. If you checked the box to Configure ACL Rules with Time Range, click Add under Configure Time Range to add a time range to this rule set. If you do not want to add a time range, skip to Step 11.

11. Enter a name for the time range in the Name field of the Add Time Range page.
    Time Range names must begin with a letter [A-Z] and consist of 1-32 characters. Blank spaces [ ] and question marks [?] are not permitted. Uppercase letters may be converted to lowercase letters by some devices after deployment.

12. Click Add to enter a time range.
    The Add Time Range dialog box appears.

13. Select the type of time range you want to create by clicking the radio button to the left of the desired time range type:
    o Fixed if you want to identify a specific and finite start and end date and time, or
    o Cyclic if you want the time range to recur for selected days of the week.

14. Click Add on the Configure Rule page to configure a new rule.
    See "Configuring fixed time ranges" (page 655) to configure fixed time ranges and "Configuring cyclic time ranges" (page 656) to configure cyclic time ranges.
    The Configure Rule – Add Rule page appears.

15. Select the action you want to take by clicking the radio button to the left of the option you want to apply to this rule:
    o Select permit if, upon matching the specified conditions, the packet should be forwarded, or
    o Select deny if, upon matching the specified conditions, the packet should be discarded.

16. Select the time range you want to apply to this rule from the Time Range list you created in the Step 10.

17. Select the source MAC address option you want to use by clicking the radio button to the left of the desired option in the Source MAC Addr section of the Configure Rule – Add Rule page.
    This option specifies where the pattern matching occurs in this rule. In this case, the pattern matching is applied to the source MAC address.
    o All: Allows you to permit or deny traffic for all MAC addresses.
    o MAC Address/Mask: Allows you to enter a specific MAC address and mask for which you want to either permit or deny traffic for.
A valid MAC address format for IMC consists of three sets of four hexadecimal characters separated by a dash, ".". For example,

0014-2ad9-05f7

would be a valid entry for a MAC address in IMC.

Similarly, the format for a MAC address mask consists of three sets of four hexadecimal characters separated by a dash, ".". For example,

ffff-ffff-ffff

would be a valid entry for a MAC address mask in IMC.

The MAC address and its mask must be separated by a forward slash, "/".

A valid entry for a MAC Address/Mask would be

0014-2ad9-05f7/ffff-ffff-ffff

18. Select the destination MAC address option you want to use by clicking the radio button to the left of the desired option in the Destination MAC Address section of the Configure Rule – Add Rule page.

This option specifies where the pattern matching will occur in this rule. In this case, the pattern matching will be applied to the destination MAC address. Options include:

- **All**: Allows you to permit or deny traffic for all MAC addresses.
- **MAC Address/Mask**: Allows you to identify a specific MAC address and its mask for which you want to either permit or deny traffic.

A valid MAC address format for IMC consists of three sets of four hexadecimal characters separated by a dash, ".". For example,

0014-2ad9-05f7

would be a valid entry for a MAC address in IMC.

Similarly, the format for a MAC address mask consists of three sets of four hexadecimal characters separated by a dash, ".". For example,

ffff-ffff-ffff

would be a valid entry for a MAC address mask in IMC.

The MAC address and its mask must be separated by a forward slash, "/".

A valid entry for a MAC Address/Mask would be

0014-2ad9-05f7/ffff-ffff-ffff

19. Select the 802.1 priority you want to apply to this ACL rule from the 802.1 Priority list.

20. Select the Layer 2 encapsulation type you want to apply to this ACL rule from the Encapsulation Type list.

Options include **Undefined**, **Ethernet II**, **SNAP**, **IEEE 802.2/802.3**, and **IEEE 802.3**.

21. Enter the source VLAN ID by entering it in the Source VLAN ID field.

This field cannot contain question marks or blank spaces.

22. Select the Layer 2 frame type from the Based Frame Type list.

Options include **Undefined**, **Ethernet Frame**, and **802.2 Ethernet Frame**.

23. If you selected **Ethernet Frame** or **802.2 Ethernet Frame** in the Base Frame Type list, you must specify a code in the Code field.

A valid entry for this field includes any four character hexadecimal value.

24. If you selected **Ethernet Frame** or **802.2 Ethernet Frame** in the Base Frame Type list, you must also specify a mask in the Mask field.

A valid entry for this field includes any four character hexadecimal value.
25. Click OK to create the rule you have just configured.

26. To add more rules, modify, copy, sort, optimize or delete existing rules, select one of the following:
   - To add more rules to the ACL, repeat Steps 11-25, or
   - To modify rules you have already created, click the Modify icon associated with the rule sequence you want to modify. For more information modifying a rule set, see "Adding or modifying a link rule in a link rule set" (page 747), or
   - To copy rules you have already created, click the Copy icon associated with the rule sequence you want to copy. For more information copying a rule set, see "Copying a rule in an ACL rule set" (page 750), or
   - Rules that belong to a rule set that is configured with a Match Order of ‘Config’ are executed in the order in which they appear in the rule set. The order in which rules appear in a rule set is initially defined by the order in which they are created. You can, however, reorder the rules in a rule set using the Sort feature. For more information using Sort to redefine the order of appearance of rules in a rule set, see “Using sort to reorder the rules in an ACL rules set” (page 752), or
   - ACLs can have a profound effect on the performance of networks. ACL Management automatically evaluates the effectiveness of rules and their effect on overall network performance as you add rules to a rule set. However, you can also manually perform an analysis of a rule set and optimize its effect on network performance using the Optimize feature. For more information using this feature, see “Optimizing the rules in a rule set” (page 752), or
   - To delete one or more rules from a rule set, see "Deleting rules from an ACL rule set" (page 751).

27. Click Finish when you have finished creating rules for this rule set.

   Once you have created an ACL you are ready to deploy the ACL to devices using the ACL Management’s ACL Deployment wizard. For more information deploying ACLs, see “Deploying ACLs using IMC’s ACL deployment wizard” (page 782).

Adding a user-defined rule set

User-Defined ACLs enable you to define a hexadecimal pattern and mask and the offset in the packet header that identifies where to begin the pattern matching. When a pattern is matched, the conditions of the rule in the ACL will be applied. A valid numeric range for assigning ACL Identifiers to user-defined ACLs is 5000-5999.

To add a user-defined rule set to an existing ACL resource:

1. Navigate to ACL Resource:
   a. Click the Service tab from the tabular navigation system on the top.
   b. Click the ACL Management icon located under the Resource and Configuration Management section of the Service tab.
   c. Click the ACL Resource link located under ACL Management on the navigation tree on the left. The ACL Resource list displays in the main pane of the ACL Resource page.

2. Click the ACL Identifier for the user-defined ACL for which you want to create a new rule set. Refer to the ACL Type field in the ACL Resource list for identifying ACLs for which the type is ‘User-Defined’. The Rule Set List displays in the main pane of the ACL Resource→<ACL Resource Name (ACL Identifier)> page.
3. Click **Add**.
   The **Basic Info** step of the **Add Rule Set** page appears.

   Several fields are already configured and cannot be changed. These include the **ACL Identifier**, the **ACL Type**, and the **ACL Resource Name**. These cannot be changed because they are inherited by the ACL to which this rule set belongs.

   You can create rule sets of the same type as the type of ACL to which the rule set belongs.

4. Enter a name for the rule set in the **Rule Set Name** field.
   A valid length for a rule set name is 1 – 32 characters.

5. Select the match order you want to apply to this rule set by clicking the radio button ○ to the left of the **Match Order** option you want to use.
   Options include **Config** and **Auto**:
   
   o If you select **Config**, IMC matches rules in the order in which they were configured and only works for devices that support it, or
   
   o If you select **Auto**, IMC matches rules based on the principle of depth priority.

6. Enter a brief description for this ACL in the **ACL Description** field.
   A valid length for this field is 0 – 127 characters.

7. Enter a brief description for this rule set in the **Rule Set Description** field.
   A valid length for this field is 0 – 127 characters.

8. If you want to apply a time range to the rule set, click on the checkbox ○ to the left of **Configure ACL Rules with Time Range**.

9. Click **Next**.

10. If you checked the box to **Configure ACL Rules with Time Range**, click **Add** under **Configure Time Range** to add a time range to this rule set. If you do not want to add a time range, skip to **Step 11**.

11. Enter a name for the time range in the **Name** field of the **Add Time Range** page.

    Time Range names must begin with a letter [A-Z] and consist of 1-32 characters. Blank spaces [ ] and question marks [?] are not permitted. Uppercase letters may be converted to lowercase letters by some devices after deployment.

12. Click **Add** to enter a time range.

    The **Add Time Range** dialog box appears.

13. Select the type of time range you want to create by clicking the radio button ○ to the left of the desired time range type:

    o **Fixed** if you want to identify a specific and finite start and end date and time, or
    
    o **Cyclic** if you want the time range to recur for selected days of the week.

14. Click **Add** on the **Configure Rule** page to configure a new rule.

    The **Configure Rule – Add Rule** page appears.

    See "Configuring fixed time ranges" (page 655) to configure fixed time ranges and "Configuring cyclic time ranges" (page 656) to configure cyclic time ranges.

15. Select the action you want to take by clicking the radio button ○ to the left of the option you want to apply to this rule.

    o **Select permit** if, upon matching the specified conditions, the packet should be forwarded, or
    
    o **Select deny** if, upon matching the specified conditions, the packet should be discarded.

16. Select the time range you want to apply to this rule from the **Time Range** list you created in the **Step 10**.
17. Enter up to eight hexadecimal patterns, masks, and offsets for matching the contents of a packet and applying the actions specified in the rule when a hexadecimal pattern is matched.

The following rules and guidelines apply to constructing a valid hexadecimal string, mask, and offset value.

- A rule string must be expressed in hexadecimal only
- A mask must be expressed in hexadecimal only
- A rule string length must be equal to its mask length
- Rule string and mask length must be in multiples of 2
- The minimum length of a rule string and mask is 2
- The maximum length of a rule string and mask is 160
- Offsets must be expressed as a decimal integer
- Offset range varies by the mask length
- The minimum value for an offset is 0
- The maximum value for an offset is 79
- The offset must increase progressively

a. Enter a hexadecimal pattern to be matched in the Rule String field.

b. Enter a mask in the Mask field.

c. Enter the offset in the Excursion field.

d. Enter up to eight Rule String/Mask/Excursion combinations.

18. Click OK to create the rule you have just configured.

19. To add more rules, modify, copy, sort, optimize or delete existing rules, select one of the following:

- To add more rules to the ACL, repeat Steps 11-18, or

- To modify rules you have already created, click the Modify icon associated with the rule sequence you want to modify. For more information modifying a rule set, see "Adding or modifying a user-defined rule in a user-defined rule set" (page 749), or

- To copy rules you have already created, click the Copy icon associated with the rule sequence you want to copy. For more information copying a rule set, see "Copying a rule in an ACL rule set" (page 750), or

- Rules that belong to a rule set that is configured with a Match Order of 'Config' are executed in the order in which they appear in the rule set. The order in which rules appear in a rule set is initially defined by the order in which they are created. You can, however, reorder the rules in a rule set using the Sort feature. For more information using Sort to redefine the order of appearance of rules in a rule set, see "Using sort to reorder the rules in an ACL rules set" (page 752), or

- ACLs can have a profound effect on the performance of networks. ACL Management automatically evaluates the effectiveness of rules and their effect on overall network performance as you add rules to a rule set. However, you can also manually perform an analysis of a rule set and optimize its effect on network performance using the Optimize feature. For more information using this feature, see "Optimizing the rules in a rule set" (page 752), or

- To delete one or more rules from a rule set, see "Deleting rules from an ACL rule set" (page 751).

20. Click Finish when you have finished creating rules for this rule set.
Once you have created an ACL you are ready to deploy the ACL to devices using the ACL Management’s ACL Deployment wizard. For more information deploying ACLs, see “Deploying ACLs using IMC’s ACL deployment wizard” (page 782).

Modifying ACL rule sets

Many of the parameters used to create a rule set can be changed using the modify option for all of the ACL rule types.

Modifying a basic rule set

To modify the basic rule set of an existing ACL resource:

1. Navigate to ACL Resource:
   a. Click the Service tab from the tabular navigation system on the top.
   b. Click the ACL Management icon located under the Resource and Configuration Management section of the Service tab.
   c. Click the ACL Resource link located under ACL Management on the navigation tree on the left.
      
      The ACL Resource list displays in the main pane of the ACL Resource page.

2. Click the ACL Identifier for the basic ACL for which you want to modify a rule. Refer to the ACL Type field in the ACL Resource list for identifying ACLs for which the type is Basic.
   
   The Rule Set List for the selected ACL displays in the main pane of the ACL Resource →<ACL Resource Name (ACL Identifier)> page.

3. Click the icon in the Modify field associated with the rule set you want to modify.
   
   The Basic Info step of the Modify Rule Set page appears.
   
   Several fields cannot be changed. These include the ACL Identifier, the ACL Type, the ACL Resource Name, the Rule Set Name, and the Match Order.

4. Modify the description for this ACL as needed in the ACL Description field.
   
   A valid length for this field is 0 – 127 characters.

5. Modify the description for this rule set as needed in the Rule Set Description field.
   
   A valid length for this field is 0 – 127 characters.


7. If you do not want to modify or add a time range, click Next and skip to Step 8.
   
   o To modify an existing time range, click the icon in the Modify field of the time range table, the Modify Time Range page will be displayed. Modification options include adding new time ranges or deleting existing time ranges, or

   o To modify the time range name, enter a new name for the time range in the Name field of the Modify Time Range page. Time Range names must begin with a letter [A-Z] and consist of 1-32 characters. Blank spaces [ ] and question marks [?] are not permitted. Uppercase letters may be converted to lowercase letters by some devices after deployment, or

   o To configure a new time range item, click Add under the Time Range Items section and follow the instructions below.

   The Add Time Range dialog box appears.
8. Select the type of time range you want to create by clicking the radio button ⊗ to the left of the desired time range type:
   o **Fixed** to identify a specific and finite start and end date and time, or
   o **Cyclic** for the time range to recur for selected days of the week.

9. Do one of the following:
   o To add a new rule click **Add** on the **Configure Rule** page to configure a new rule, or
     The **Add Rule** page appears.
   o To modify an existing rule, click on the icon ⊗ in the **Modify** field associated with the rule you want to modify.

10. Select the action you want to take by clicking the radio button ⊗ to the left of the option you want to apply to this rule:
    o **Select** **permit** if, upon matching the specified conditions, the packet should be forwarded, or
    o **Select** **deny** if, upon matching the specified conditions, the packet should be discarded.

11. Select the time range you want to apply to this rule from the **Time Range** list you created in the **Step 7**.

12. Select the source IP address option you want to use by clicking the radio button ⊗ to the left of the desired option in the **Source Address** field of the **Add Rule** page.

    This option specifies where the pattern matching occurs in this rule. In this case, the pattern matching is applied to the source IP address.
    o **All**: Allows you to permit or deny traffic for all IP addresses.
    o **IP Address/Mask**: Allows you to enter a specific IP address and its subnet mask for which you want to either permit or deny traffic for.

    a. Enter an IP address/subnet mask combination in the **IP Address/Mask** field.

    The subnet mask must be entered in dotted decimal notation. A valid IP address/subnet mask using dotted decimal notation would be 192.168.1.0/255.255.255.0

    A forward slash “/” must be used to separate the IP address from the subnet mask.

13. Do one of the following:
    o Click the radio button ⊗ to the left of **Yes** in the **Fragment** option if you want to apply the rule to each fragment, or
    o Click the radio button ⊗ to the left of **No** in the **Fragment** option if you want to apply the rule to first fragments.

    Traditional packet filtering matched only first fragments of IPv4 packets and allowed all subsequent non-first fragments to pass through. This resulted in security risks as hackers can fabricate non-first fragments to attack networks.

14. Click the radio button ⊗ to the left of **Yes** in the **Logging** option if you want to enable logging for this rule.

    This feature enables the logging of packet filtering only when a module (for example, a firewall) using the ACL supports logging.

15. Enter the VPN instance you want to apply to this rule by entering the VPN-instance-name in the **VPN Instance** field.  

    A valid entry must be 0 – 31 characters that cannot contain question marks or blank spaces. This field is case sensitive. If no VPN instance is specified in this field, the rule applies only to non-VPN packets.

16. Click **OK** to create the rule you have just configured or to accept the modifications to the existing rule.
17. To add more rules, modify, copy, sort, optimize or delete existing rules, select one of the following:
   o To add more rules to the ACL, repeat Steps 8-16, or
   o To copy rules you have already created, click the Copy icon associated with the rule sequence you want to copy. For more information copying a rule set, see "Copying a rule in an ACL rule set" (page 750), or
   o Rules that belong to a rule set that is configured with a Match Order of ‘Config’ are executed in the order in which they appear in the rule set. The order in which rules appear in a rule set is initially defined by the order in which they are created. You can, however, reorder the rules in a rule set using the Sort feature. For more information using Sort to redefine the order of appearance of rules in a rule set, see “Using sort to reorder the rules in an ACL rules set” (page 752), or
   o ACLs can have a profound effect on the performance of networks. ACL Management automatically evaluates the effectiveness of rules and their effect on overall network performance as you add rules to a rule set. However, you can also manually perform an analysis of a rule set and optimize its effect on network performance using the Optimize feature. For more information using this feature, see “Optimizing the rules in a rule set” (page 752), or
   o To delete one or more rules from a rule set, see “Deleting rules from an ACL rule set” (page 751).

18. Click Finish when you have finished modifying this rule set.

Modifying an advanced rule set

To modify the advanced rule set of an existing ACL:

1. Navigate to ACL Resource:
   a. Click the Service tab from the tabular navigation system on the top.
   b. Click the ACL Management icon located under the Resource and Configuration Management section of the Service tab.
   c. Click the ACL Resource link located under ACL Management on the navigation tree on the left.
      The ACL Resource list displays in the main pane of the ACL Resource page.

2. Click the ACL Identifier for the advanced ACL for which you want to modify a rule. Refer to the ACL Type field in the ACL Resource list for identifying ACLs for which the type is Advanced.
   The Rule Set List for the selected ACL displays in the main pane of the ACL Resource page.

3. Click the icon in the Modify field associated with the rule set you want to modify.
   The Basic Info step of the Modify Rule Set page appears.
   Several fields cannot be changed. These include the ACL Identifier, the ACL Type, the ACL Resource Name, the Rule Set Name, and the Match Order.

4. Modify the description for this ACL as needed in the ACL Description field.
   A valid length for this field is 0 – 127 characters.

5. Modify the description for this rule set as needed in the Rule Set Description field.
   A valid length for this field is 0 – 127 characters.

6. Click Next.
   The Configure Time Range step of the Modify Rule Set page appears.

7. Do one of the following:
If you do not want to modify or add a time range, click **Next** and skip to **Step 9**, or

If you want to modify an existing time range, click on the icon ** 修改 ** in the **Modify** field of the time range table, the **Modify Time Range** page appears.

Modification options include adding new time ranges or deleting existing time ranges.

- To modify the time range name, enter a new name for the time range in the **Name** field of the **Modify Time Range** page and skip to **Step 9**.
- Time Range names must begin with a letter [A-Z] and consist of 1-32 characters. Blank spaces [] and question marks [?] are not permitted. Uppercase letters may be converted to lowercase letters by some devices after deployment.

**b.** To configure a new time range item, click **Add** under the **Time Range Items** section and:

The **Add Time Range** dialog box appears.

**c.** Select the type of time range you want to create by clicking the radio button ** Fixed ** to the left of the desired time range type:

- Select **Fixed** if you want to identify a specific and finite start and end date and time, or
- Select **Cyclic** if you want the time range to recur for selected days of the week.

8. To add a new rule, click **Add** on the **Configure Rule** page to configure a new rule. The **Add Rule** page appears.

9. To modify an existing rule, click the icon ** 修改 ** in the **Modify** field associated with the rule you want to modify.

10. Select the action you want to take by clicking the radio button ** permit ** to the left of the option you want to apply to this rule:

- Select **permit** if, upon matching the specified conditions, the packet should be forwarded, or
- Select **deny** if, upon matching the specified conditions, the packet should be discarded.

11. Select the time range you want to apply to this rule from the **Time Range** list you created in the **Step 7**.

12. Select the protocol for which you want to permit or deny traffic from the **Protocol** list.

13. Select the source IP address option you want to use by clicking the radio button ** All ** to the left of the desired option in the **Source Address** section of the **Configure Rule – Modify Rule** page.

   This option specifies where the pattern matching occurs in this rule. In this case, the pattern matching is applied to the source IP address.

   - **All**: Allows you to permit or deny traffic for all IP addresses.
   - **IP Address/Mask**: Allows you to enter a specific IP address and its subnet mask for which you want to either permit or deny traffic for. If you are modifying an existing rule, you need to delete the existing value before entering a new IP address and subnet mask.

14. Enter an IP address/subnet mask combination in the **IP Address/Mask** field.

   The subnet mask must be entered in dotted decimal notation. A valid IP address/subnet mask using dotted decimal notation would be 192.168.1.0/255.255.255.0

   Note too that a forward slash “/” must be used to separate the IP address from the subnet mask.

15. Select the destination IP address option you want to use by clicking the radio button ** All ** to the left of the desired option in the **Destination Address** section of the **Configure Rule – Modify Rule** page.

This option specifies where the pattern matching occurs in this rule. In this case, the pattern matching is applied to the destination IP address. Options include:

- **All**: Allows you to permit or deny traffic for all IP addresses.
IP Address/Mask: Allows you to enter a specific IP address and its subnet mask for which you want to either permit or deny traffic. If you are modifying an existing rule, you will need to delete the existing value before entering a new IP address and subnet mask.

a. Enter an IP address/subnet mask combination in the IP Address/Mask field. The subnet mask must be entered in dotted decimal notation. A valid IP address/subnet mask using dotted decimal notation would be 192.168.1.0/255.255.255.0. A forward slash “/” must be used to separate the IP address from the subnet mask.

16. If you selected TCP or UDP as the protocol you want to apply this ACL rule to in Step 11, you must also specify the source TCP or UDP port numbers:

a. Select the source TCP or UDP port by clicking the radio button to the left of the port option you want to apply in the Source Port section of the Configure Rule – Modify Rule page:
   - Undefined: Allows you to permit or deny traffic for all TCP or UDP port numbers, or
   - Specified Port: Allows you to identify a specific TCP or UDP port number or range of numbers.

b. Click the radio button to the left of Specified Port and select the operator you want to use from the list located to the right of the Specified Port option.

c. Enter the TCP or UDP port number in the Port field.

17. If you selected TCP or UDP as the protocol you want to apply this ACL rule to, you must also specify the destination TCP or UDP port numbers, select the destination TCP or UDP port by clicking the radio button to the left of the port option you want to apply in the Destination Port section of the Configure Rule – Modify Rule page:

   - Undefined: Allows you to permit or deny traffic for all TCP or UDP port numbers.
   - Specified Port: Allows you to identify a specific TCP or UDP port number or range of numbers. Click the radio button to the left of Specified Port and select the operator you want to use from the list located to the right of the Specified Port option. Enter the TCP or UDP port number in the Port field.

18. If you selected TCP or UDP as the protocol you want to apply this ACL rule to in Step 11, you could be promoted to select these options:

   - Click the radio button to the left of Yes in the HP ACK option if you want to apply the rule to match the TCP ACK, otherwise click on the radio button to the left of No.
   - Click the radio button to the left of Yes in the HP FIN option if you want to apply the rule to match the TCP FIN, otherwise click on the radio button to the left of No.
   - Click the radio button to the left of Yes in the HP RST option if you want to apply the rule to match the TCP RST, otherwise click on the radio button to the left of No.
   - Click the radio button to the left of Yes in the HP SYN option if you want to apply the rule to match the TCP SYN, otherwise click on the radio button to the left of No.

The HP ACK, HP FIN, HP RST, and HP SYN settings are valid only for the HP E series devices.

19. Select the IP priority you want to apply to ACL from the IP Priority list.

20. Select the Type of Service for this ACL from the TOS Value list.

21. Select the DSCP value you want to apply to this ACL from the DSCP Value list.

22. Do one of the following:

   - Click the radio button to the left of Yes in the Fragment option if you want to apply the rule to each fragment, or
   - Click the radio button to the left of No in the Fragment option if you want to apply the rule to first fragments.
Traditional packet filtering matched only first fragments of IPv4 packets and allowed all subsequent non-first fragments to pass through. This resulted in security risks as hackers can fabricate non-first fragments to attack networks.

23. Click the radio button ☐ to the left of Yes in the Logging option if you want to enable logging for this rule.

This feature enables the logging of packet filtering only when a module (for example, a firewall) using the ACL supports logging.

24. Enter the VPN instance you want to apply to this rule by entering the VPN-instance-name in the VPN Instance field.

A valid entry must be 0-31 characters that cannot contain question marks or blank spaces. This field is case sensitive. If no VPN instance is specified in this field, the rule will apply only to non-VPN packets.

25. Click OK to create the rule you have just configured or to accept the modifications to the existing rule.

26. Select from the following to add more rules, copy, sort, optimize, or delete existing rules:
   - To add more rules to the ACL, repeat Steps 8-21, or
   - To copy rules you have already created, click the Copy icon associated with the rule sequence you want to copy. For more information copying a rule set, see "Copying a rule in an ACL rule set" (page 750), or
   - Rules that belong to a rule set that is configured with a Match Order of ‘Config’ are executed in the order in which they appear in the rule set. The order in which rules appear in a rule set is initially defined by the order in which they are created. You can, however, reorder the rules in a rule set using the Sort feature. For more information using Sort to redefine the order of appearance of rules in a rule set, see “Using sort to reorder the rules in an ACL rules set” (page 752), or
   - ACLs can have a profound effect on the performance of networks. ACL Management automatically evaluates the effectiveness of rules and their effect on overall network performance as you add rules to a rule set. However, you can also manually perform an analysis of a rule set and optimize its effect on network performance using the Optimize feature. For more information using this feature, see “Optimizing the rules in a rule set” (page 752), or
   - To delete one or more rules from a rule set, see "Deleting rules from an ACL rule set" (page 751).

27. Click Finish when you have finished modifying this rule set.

Modifying a link rule set

To modify the link rule set of an existing ACL:

1. Navigate to ACL Resource:
   a. Click the Service tab from the tabular navigation system on the top.
   b. Click the ACL Management icon located under the Resource and Configuration Management section of the Service tab.
   c. Click the ACL Resource link located under ACL Management on the navigation tree on the left.

   The ACL Resource list displays in the main pane of the ACL Resource page.

2. Click the ACL Identifier for the basic ACL for which you want to modify a rule. Refer to the ACL Type field in the ACL Resource List for identifying ACLs for which the type is Link.

   The Rule Set List for the selected ACL displays in the main pane of the ACL Resource page.

3. Click the icon in the Modify field associated with the rule set you want to modify.
The Basic Info step of the Modify Rule Set page appears.

Several fields cannot be changed. These include the ACL Identifier, the ACL Type, the ACL Resource Name, the Rule Set Name, and the Match Order.

4. Modify the description for this ACL as needed in the ACL Description field.
A valid length for this field is 0 – 127 characters.

5. Modify the description for this rule set as needed in the Rule Set Description field.
A valid length for this field is 0 – 127 characters.

6. Click Next.
The Configure Time Range step of the Modify Rule Set page appears.

7. Do one of the following:
   o If you do not want to modify or add a time range, click Next and skip to Step 8, or
   o If you want to modify an existing time range, click on the icon  in the Modify field of the time range table, the Modify Time Range page appears.

Modification options include adding new time ranges or deleting existing time ranges.

8. Enter a new name for the time range in the Name field of the Modify Time Range page to modify the time range name.

   Time Range names must begin with a letter [A-Z] and consist of 1-32 characters. Blank spaces [ ] and question marks [?] are not permitted. Uppercase letters may be converted to lowercase letters by some devices after deployment.

   o To configure a new time range item, click Add under the Time Range Items section and the Add Time Range dialog box appears. Follow the instructions below:

   a. Select the type of time range you want to create by clicking the radio button  to the left of the desired time range type.

   b. Select Fixed if you want to identify a specific and finite start and end date and time, or
   c. Select Cyclic if you want the time range to recur for selected days of the week.

9. To add a new rule click Add on the Configure Rule page to configure a new rule.
The Add Rule page appears.

10. To modify an existing rule, click the icon  in the Modify field associated with the rule you want to modify.

11. Select the action you want to take by clicking the radio button  to the left of the option you want to apply to this rule:

   a. Select permit if, upon matching the specified conditions, the packet should be forwarded, or
   b. Select deny if, upon matching the specified conditions, the packet should be discarded.

12. Select the time range you want to apply to this rule from the Time Range list you created in the Step 7.

13. Select the source MAC address option you want to use by clicking the radio button  to the left of the desired option in the Source MAC Addr field of the Configure Rule – Add Rule page.

   This option specifies where the pattern matching occurs in this rule. In this case, the pattern matching is applied to the source MAC address.

   a. All: Allows you to permit or deny traffic for all MAC addresses.
   b. MAC Address/Mask: Allows you to enter a specific MAC address and mask for which you want to either permit or deny traffic for. If you are modifying an existing rule, you will need to delete the existing value before entering a new MAC address and mask.
A valid MAC address format for IMC consists of three sets of four hexadecimal characters separated by a dash, ".". For example,
0014-2ad9-05f7
would be a valid entry for a MAC address in IMC.
Similarly, the format for a MAC address mask consists of three sets of four hexadecimal characters separated by a dash, ".". For example,
ffff-ffff-ffff
would be a valid entry for a MAC address mask in IMC.
The MAC address and its mask must be separated by a forward slash, "/".
A valid entry for a MAC Address/Mask would be
0014-2ad9-05f7/ffff-ffff-ffff

14. Select the destination MAC address option you want to use by clicking the radio button to the left of the desired option in the Destination MAC Address field of the Configure Rule – Modify Rule page. This option specifies where the pattern matching occurs in this rule. In this case, the pattern matching is applied to the source MAC address.
 o All: Allows you to permit or deny traffic for all MAC addresses.
 o MAC Address/Mask: Allows you to identify a specific MAC address and its mask for which you want to either permit or deny traffic. If you are modifying an existing rule, you will need to delete the existing value before entering a new MAC address and mask.

A valid MAC address format for IMC consists of three sets of four hexadecimal characters separated by a dash, ".". For example,
0014-2ad9-05f7
would be a valid entry for a MAC address in IMC.
Similarly, the format for a MAC address mask consists of three sets of four hexadecimal characters separated by a dash, ".". For example,
ffff-ffff-ffff
would be a valid entry for a MAC address mask in IMC.
The MAC address and its mask must be separated by a forward slash, "/".
A valid entry for a MAC Address/Mask would be
0014-2ad9-05f7/ffff-ffff-ffff

15. Select the 802.1 priority you want to apply to this ACL rule from the 802.1 Priority list.
16. Select the Layer 2 encapsulation type you want to apply to this ACL rule from the Encapsulation Type list.
17. Enter the source VLAN ID by entering it in the Source VLAN ID field.
This field cannot contain question marks or blank spaces.
18. Select the Layer 2 frame type from the Based Frame Type list.
19. If you selected Ethernet Frame or 802.2 Ethernet Frame in the Base Frame Type list, you must specify a code in the Code field.
A valid entry for this field includes any four character hexadecimal value.
20. If you selected Ethernet Frame or 802.2 Ethernet Frame in the Base Frame Type list, you must also specify a mask in the Mask field.
A valid entry for this field includes any four character hexadecimal value.
21. Click OK to create the rule you have just configured or to accept the modifications to the existing rule.
22. Select from the following to add more rules, copy, sort, optimize, or delete existing rules:
   o To add more rules to the ACL, repeat Steps 8-19, or
   o To copy rules you have already created, click the Copy icon associated with the rule sequence you want to copy. For more information copying a rule set, see “Copying a rule in an ACL rule set” (page 750), or
   o Rules that belong to a rule set that is configured with a Match Order of ‘Config’ are executed in the order in which they appear in the rule set. The order in which rules appear in a rule set is initially defined by the order in which they are created. You can, however, reorder the rules in a rule set using the Sort feature. For more information using Sort to redefine the order of appearance of rules in a rule set, see “Using sort to reorder the rules in an ACL rules set” (page 752), or
   o ACLs can have a profound effect on the performance of networks. ACL Management automatically evaluates the effectiveness of rules and their effect on overall network performance as you add rules to a rule set. However, you can also manually perform an analysis of a rule set and optimize its effect on network performance using the Optimize feature. For more information using this feature, see “Optimizing the rules in a rule set” (page 752), or
   o To delete one or more rules from a rule set, see "Deleting rules from an ACL rule set" (page 751).

23. Click Finish when you have finished modifying this rule set.

Modifying a user-defined rule set

To modify the user-defined rule set of an existing ACL:
1. Navigate to ACL Resource:
   a. Click the Service tab from the tabular navigation system on the top.
   b. Click the ACL Management icon located under the Resource and Configuration Management section of the Service tab.
   c. Click the ACL Resource link located under ACL Management on the navigation tree on the left.
      The ACL Resource list displays in the main pane of the ACL Resource page.
2. Click the ACL Identifier for the basic ACL for which you want to modify a rule. Refer to the ACL Type field in the ACL Resource list for identifying ACLs for which the type is User-Defined.
   The Rule Set List for the selected ACL displays in the main pane of the ACL Resource → <ACL Resource Name (ACL Identifier)> page.
3. Click the icon in the Modify field associated with the rule set you want to modify.
   The Basic Info step of the Modify Rule Set page appears.
   Several fields cannot be changed. These include the ACL Identifier, the ACL Type, the ACL Resource Name, the Rule Set Name, and the Match Order.
4. Modify the description for this ACL as needed in the ACL Description field.
   A valid length for this field is 0 – 127 characters.
5. Modify the description for this rule set as needed in the Rule Set Description field.
   A valid length for this field is 0 – 127 characters.
6. Click Next.
   The Configure Time Range step of the Modify Rule Set page appears.
7. Do one of the following:
   o If you do not want to modify or add a time range, click Next and skip to Step 8, or
   o If you want to modify an existing time range, click on the icon in the Modify field of the time range table, the Modify Time Range page appears, or
   Modification options include adding new time ranges or deleting existing time ranges.
   o Enter a new name for the time range in the Name field of the Modify Time Range page to modify the time range name.
   Time Range names must begin with a letter [A-Z] and consist of 1-32 characters. Blank spaces [ ] and question marks [?] are not permitted. Uppercase letters may be converted to lowercase letters by some devices after deployment.

   • To configure a new time range item, click Add under the Time Range Items section and the Add Time Range dialog box appears. Follow the instructions below:
     a. Select the type of time range you want to create by clicking the radio button to the left of the desired time range type.
     o Select Fixed if you want to identify a specific and finite start and end date and time, or
     o Select Cyclic if you want the time range to recur for selected days of the week.

8. To add a new rule click Add on the Configure Rule page to configure a new rule.
   The Add Rule page appears.

9. To modify an existing rule, click the icon in the Modify field associated with the rule you want to modify.

10. Select the action you want to take by clicking the radio button to the left of the option you want to apply to this rule:
    o Select permit if, upon matching the specified conditions, the packet should be forwarded, or
    o Select deny if, upon matching the specified conditions, the packet should be discarded.

11. Select the time range you want to apply to this rule from the Time Range list you created in the Step 7.

12. Modify the existing Rule String/Mask/Excursion combinations or enter new combinations.

   You can enter up to eight hexadecimal patterns, masks, and offsets for matching the contents of a packet and applying the actions specified in the rule when a hexadecimal pattern is matched. The following rules and guidelines apply to constructing a valid hexadecimal string, mask, and offset value:
   o A rule string must be expressed in hexadecimal only
   o A mask must be expressed in hexadecimal only
   o A rule string length must be equal to its mask length
   o Rule string and mask length must be in multiples of 2
   o The minimum length of a rule string and mask is 2
   o The maximum length of a rule string and mask is 160
   o Offsets must be expressed as a decimal integer
   o Offset range varies by the mask length
   o The minimum value for an offset is 0
   o The maximum value for an offset is 79
   o The offset must increase progressively
   a. Modify or enter a hexadecimal pattern to be matched in the Rule String field.
b. Modify or enter a mask in the **Mask** field.

c. Modify or enter the offset in the **Excursion** field.

d. Enter up to eight **Rule String/Mask/Excursion** combinations.

13. Click **OK** to create the rule you have just configured or to accept the modifications to the existing rule.

14. Do one of the following:
   
   o To add more rules to the ACL, repeat **Steps 8-12**, or
   
   o To copy rules you have already created, click the **Copy** icon associated with the rule sequence you want to copy. For more information copying a rule set, see "Copying a rule in an ACL rule set" (page 750), or
   
   o Rules that belong to a rule set that is configured with a **Match Order of Config** are executed in the order in which they appear in the rule set. The order in which rules appear in a rule set is initially defined by the order in which they are created. You can, however, reorder the rules in a rule set using the **Sort** feature. For more information using Sort to redefine the order of appearance of rules in a rule set, see "Using sort to reorder the rules in an ACL rules set" (page 752), or
   
   o ACLs can have a profound effect on the performance of networks. ACL Management automatically evaluates the effectiveness of rules and their effect on overall network performance as you add rules to a rule set. However, you can also manually perform an analysis of a rule set and optimize its effect on network performance using the **Optimize** feature. For more information using this feature, see "Optimizing the rules in a rule set" (page 752), or
   
   o To delete one or more rules from a rule set, see "Deleting rules from an ACL rule set" (page 751).

15. Click **Finish** when you have finished modifying this rule set.

**Copying rule sets**

To simplify the process of creating new rule sets, you can make a copy of an existing rule set and copy it to the same ACL and make modifications to create a new rule set.

To copy a rule set:

1. Navigate to **ACL Resource**:
   
   a. Click the **Service** tab from the tabular navigation system on the top.
   
   b. Click the **ACL Management** icon located under the **Resource and Configuration Management** section of the **Service** tab.
   
   c. Click the **ACL Resource** link located under **ACL Management** on the navigation tree on the left. The **ACL Resource** list displays in the main pane of the **ACL Resource** page.

2. Click the **ACL Identifier** of the ACL for which you want to create a copy of a rule set.

   The **Rule Set List** for the selected ACL displays in the main pane of the **ACL Resource→<ACL Resource Name (ACL Identifier)>** page.

3. Click the icon in the **Copy** field associated with the rule set you want to copy.

   You can make any modifications to the copy of a rule set that you can to the rule set itself, including creating new rules. Note that the steps for creating and modifying rule sets vary by the ACL type to which the rule set belongs. For more information modifying rules, see "Modifying ACL rule sets" (page 718) and specifically to the section that addresses how to modify the type of rule set you want to copy.

4. Click **Finish** when you have completed your modifications to the rule set copy.
Deploying rule sets

The Deploy link in the Rule Set List is a shortcut to the ACL Deployment wizard. For more information deploying an ACL, see “Deploying ACLs using IMC’s ACL deployment wizard” (page 782).

Importing rule sets

You can import the contents of an ACL template to an existing ACL, which accelerates and standardizes the process for creating rule sets. You can only import a template of the same type as the ACL.

Importing a basic ACL template into a basic ACL

To import the contents of a basic template into a basic ACL:

1. Navigate to ACL Resource:
   a. Click the Service tab from the tabular navigation system on the top.
   b. Click the ACL Management icon located under the Resource and Configuration Management section of the Service tab.
   c. Click the ACL Resource link located under ACL Management on the navigation tree on the left. The ACL Resource list displays in the main pane of the ACL Resource page.

2. Click the ACL Identifier for the Basic ACL for which you want to import the contents of a basic template.
   The Rule Set List for the selected ACL displays in the main pane of the ACL Resource page.

3. Click Import.
   The Import ACL Template to ACL Resource page appears.

4. Select the ACL template you want to import from the ACL Template list.
   Only templates of the same type as the ACL you are importing into display in the ACL Template list. The page updates to display the time ranges and network address groups configured in the ACL template, if any, as shown in the title bar examples below.

   September (Type: Time Range)
   NetMgmt_Servers (Type: Network)

5. Select from one of the methods for configuring the time range contents of an ACL:
   o To configure the imported rules without limitations to the dates and times that the rule lists will be in effect, click the checkbox to the left of All, or
   o To configure a time range using a pre-configured time range from the Assistant, click Select, and the Select Time Ranges dialog box appears:
     a. Click or more of the checkboxes to the left of the time ranges you want to add. For more information viewing the details of a time range in the Assistant, see “Viewing the time range list” (page 772).
     b. Click OK to accept your selection.
   o To customize a time range configuration for this import, click Add and the Add Time Range dialog box appears:
     c. Select the type of time range you want to create by clicking the radio button to the left of the desired time range type:
     o Select Fixed if you want to identify a specific and finite start and end date and time, or
o Select **Cyclic** if you want the time range to recur for selected days of the week.

See “Configuring fixed time ranges” (page 655) to configure fixed time ranges and “Configuring cyclic time ranges” (page 656) to configure cyclic time ranges.

6. Select from the following options to import the source IP addresses and subnet mask combination contents of an ACL template:

o To configure the rule sets to apply to all devices, click the checkbox to the left of **All**. This configuration does not apply to any rules for which the source IP address and subnet mask have been configured in the rule.

o Click **Select** to configure an IP address/subnet mask combination using a pre-configured network address group from the Assistant and the **Select Networks** dialog box appears:

a. Click one or more of the checkboxes to the left of the network address groups you want to add. For more information viewing the details of an individual network address group, see “Viewing a network address group” (page 651).

b. Click **OK** to accept your selection.

o To customize a network segment configuration for this import, enter the IP address and subnet mask in the field to the right of **Input Network (IP/Mask)** field.

The subnet mask must be entered in dotted decimal notation. A valid IP address/subnet mask using dotted decimal notation would be 192.168.1.0/255.255.255.0

c. Click **Add**. Repeat this step to add more IP address/subnet mask combinations

7. Click **OK** when you have completed the configuration of time ranges and network addresses as the source IP addresses of a basic ACL.

The **Basic Info** step of the **Add Rule Set** page appears.

Several fields cannot be changed. These include the **ACL Identifier**, the **ACL Type**, and the **ACL Resource Name**.

8. Enter a name for the rule set in the **Rule Set Name** field.

A valid length for a rule set name is 1 – 32 characters.

9. Select the match order you want to apply to this rule set by clicking the radio button to the left of the **Match Order** option you want to use:

o If you select **Config**, IMC matches rules in the order in which they were configured and works only for the devices that support it, or

o If you select **Auto**, IMC matches rules based on the principle of depth priority.

10. Enter a brief description for this ACL in the **ACL Description** field.

A valid length for this field is 0 – 127 characters.

11. Enter a brief description for this rule set in the **Rule Set Description** field.

A valid length for this field is 0 – 127 characters.

12. Do one of the following:

o To add a new time ranges you have already configured to the rule set, leave checkbox to the left of **Configure ACL Rules with Time Range** checked, or

o To proceed with the import using the time ranges already configured in the previous steps, uncheck the box to the left of **Configure ACL Rules with Time Range**.

13. Click **Next**.
14. Do one of the following:
   o If you checked the box to **Configure ACL Rules with Time Range**, click **Add** under **Configure Time Range** to add a time range to this rule set, or
   o If you do not want to add a time range, skip to **Step 15**.

15. Enter a name for the time range in the **Name** field of the **Add Time Range** page.
    Time Range names must begin with a letter [A-Z] and consist of 1-32 characters. Blank spaces [ ] and question marks [?] are not permitted. Uppercase letters may be converted to lowercase letters by some devices after deployment.

16. Click **Add** to enter a time range.
    The **Add Time Range** dialog box appears.

17. Select the type of time range you want to create by clicking the radio button ○ to the left of the desired time range type:
   o **Fixed** if you want to identify a specific and finite start and end date and time, or
   o **Cyclic** if you want the time range to recur for selected days of the week.

18. Select from one of the following to import rules:
   o To add all rules from the template to the new ACL, skip to the next step, or
   o To delete one or more of the template rules:
     a. Click the checkbox ○ to the left of the sequence number for each of the rules you want to delete.
     b. Click **Delete**. When prompted, click **OK** to confirm the deletion of the selected rules.
   c. Skip to the next step
   o To add new rules:
     d. Click **Add** on the **Configure Rule** page and the **Add Rule** page appears.
     e. Select the action you want to take by clicking the radio button ○ to the left of the option you want to apply to this rule:
        o **Select permit** if, upon matching the specified conditions, the packet should be forwarded, or
        o **Select deny** if, upon matching the specified conditions, the packet should be discarded.
     f. Select the time range you want to apply to this rule from the **Time Range** list.
        o Select the source IP address option you want to use by clicking the radio button ○ to the left of the desired option:
           This option specifies where the pattern matching occurs in this rule. In this case, the pattern matching is applied to the source IP address.
           o **All**: Allows you to permit or deny traffic for all IP addresses.
           o **IP Address/Mask**: Allows you to enter a specific IP address and its subnet mask for which you want to either permit or deny traffic for.
     g. Enter an IP address/subnet mask combination in the **IP Address/Mask** field.
        The subnet mask must be entered in dotted decimal notation. A valid IP address/subnet mask using dotted decimal notation would be
        192.168.1.0/255.255.255.0
        A forward slash "/" must be used to separate the IP address from the subnet mask.

19. Do one of the following:
o Click the radio button  to the left of Yes in the Fragment option if you want to apply the rule to each fragment, or
o Click the radio button  to the left of No in the Fragment option if you want to apply the rule to first fragments.

Traditional packet filtering matched only first fragments of IPv4 packets and allowed all subsequent non-first fragments to pass through. This resulted in security risks as hackers can fabricate non-first fragments to attack networks.

o Click the radio button  to the left of Yes in the Logging option if you want to enable logging for this rule.

This feature enables the logging of packet filtering only when a module (for example, a firewall) using the ACL supports logging.

o Enter the VPN instance you want to apply to this rule by entering the VPN-instance-name in the VPN Instance field. Note that a valid entry must be 0-31 characters that cannot contain question marks or blank spaces. Note also that this field is case sensitive. If no VPN instance is specified in this field, the rule will apply only to non-VPN packets.

o Click OK to create the rule you have just configured.

20. Do one of the following:
   o To add more rules to the ACL, repeat this step, or
   o To modify rules you have already created, click the Modify icon associated with the rule sequence you want to modify. For more information modifying a rule set, see "Adding or modifying a basic rule in a basic ACL rule set" (page 744), or
   o To copy rules you have already created, click the Copy icon associated with the rule sequence you want to copy. For more information copying a rule set, see "Copying a rule in an ACL rule set" (page 750), or
   o Rules that belong to a rule set that is configured with a Match Order of ‘Config’ are executed in the order in which they appear in the rule set. The order in which rules appear in a rule set is initially defined by the order in which they are created. You can, however, reorder the rules in a rule set using the Sort feature. For more information using Sort to redefine the order of appearance of rules in a rule set, see "Using sort to reorder the rules in an ACL rules set" (page 752), or
   o ACLs can have a profound effect on the performance of networks. ACL Management automatically evaluates the effectiveness of rules and their effect on overall network performance as you add rules to a rule set. However, you can also manually perform an analysis of a rule set and optimize its effect on network performance using the Optimize feature. For more information using this feature, see "Optimizing the rules in a rule set" (page 752), or
   o To delete one or more rules from a rule set, see "Deleting rules from an ACL rule set" (page 751).

21. Click Finish to accept your configuration for the import process and to create the new rule set.

Importing an advanced ACL template into an advanced ACL

To import the contents of an advanced template into an advanced ACL:

1. Navigate to ACL Resource:
   a. Click the Service tab from the tabular navigation system on the top.
   b. Click the ACL Management icon located under the Resource and Configuration Management section of the Service tab.
   c. Click the ACL Resource link located under ACL Management on the navigation tree on the left.
The **ACL Resource** list displays in the main pane of the **ACL Resource** page.

2. Click the **ACL Identifier** for the Advanced ACL for which you want to import the contents of an **Advanced** template.

The **Rule Set List** for the selected ACL displays in the main pane of the **ACL Resource** page.

3. Click **Import**.

The **Import ACL Template to ACL Resource** page appears.

4. Select the ACL template you want to import from the **ACL Template** list.

Only templates of the same type as the ACL you are importing into displays on the **ACL Template** list.

The page updates to display the time ranges, network access groups, and ports configured in the ACL template, if any, as shown in the title bar examples below.

- `<WorkDays>` (Type: Time Range)
- `<NetMgmt_Servers>` (Type: Network)
- `<NetMgmt_Protocols>` (Type: Port)

5. Select from the three methods to configure the time range contents of an ACL:

   - To configure the imported rules without limitations to the dates and times that the rule lists will be in effect, click the checkbox ☑️ to the left of **All**, or
   - To configure a time range using a pre-configured time range, click **Select**.

   The **Select Time Ranges** dialog box appears.

   a. Click one or more of the checkboxes ☑️ to the left of the time ranges you want to add. For more information viewing the details of a time range in the **Assistant**, see "Viewing the time range list" (page 772).

   b. Click **OK** to accept your selection.

   - To customize a time range configuration for this import, click **Add**.

   The **Add Time Range** dialog box appears.

   c. Select the type of time range you want to create by clicking the radio button ☑️ to the left of the desired time range type.

      - Select **Fixed** if you want to identify a specific and finite start and end date and time, or
      - Select **Cyclic** if you want the time range to recur for selected days of the week.

6. Select from the three options for importing the source IP addresses and subnet masks combination contents of an ACL template:

   - To configure the rule sets to apply to all devices, click on the checkbox ☑️ to the left of **All**.

     This configuration applies to any rules for which the source IP address and subnet mask have been configured in the rule.

   - To use pre-configured network address groups, click **Select** to configure an IP address/subnet mask combination using a pre-configured network address group from the **Assistant**.

     The **Select Networks** dialog box appears.

   a. Click one or more of the checkboxes ☑️ to the left of the network address groups you want to add. For more information viewing the details of an individual network address group, see "Viewing a network address group" (page 651).

   b. Click **OK** to accept your selection.
To customize a time range configuration for this import, enter the IP address and subnet mask in the field to the right of **Input Network (IP/Mask)** field.

The subnet mask must be entered in dotted decimal notation. A valid IP address/subnet mask using dotted decimal notation would be 192.168.1.0/255.255.255.0

A forward slash "/" must be used to separate the IP address from the subnet mask.

c. Click **Add**. Repeat this step to add more IP address/subnet mask combinations.

d. Select from the options for importing the port configuration contents of an ACL template:

   - To configure the rule set to apply to all ports, click on the checkbox to the left of **All**, or
   - To use pre-configured services, click **Select** to configure a port using a pre-configured service.

   The **Select Services** dialog box appears.

   This configuration does not apply to any rules for which the ports have been specified.

e. Click one or more of the checkboxes to the left of the services you want to add. For more information viewing the details of an individual service, see "Viewing a service" (page XX).

f. Click **OK** to accept your selection.

   - To customize a port configuration for this import, enter the port in the field to the right of **Input Port** field.

   A valid port entry must in the range of 1-65535.

g. Click **Add**. Repeat this step to add more port numbers.

7. Click **OK** when you have completed the configuration of time ranges, network addresses, and protocols for advanced ACL.

   The **Basic Info** step of the **Add Rule Set** page appears.

   Several fields cannot be changed. These include the **ACL Identifier**, the **ACL Type**, and the **ACL Resource Name**.

8. Enter a name for the rule set in the **Rule Set Name** field.

   A valid length for a rule set name is 1 – 32 characters.

9. Select one of the following match orders you want to apply to this rule set by clicking the radio button to the left of the **Match Order** option you want to use:

   - If you select **Config**, IMC matches rules in the order in which they were configured, only for devices that support it, or
   - If you select **Auto**, IMC matches rules based on the principle of depth priority.

10. Enter a brief description for this ACL in the **ACL Description** field.

    A valid length for this field is 0 – 127 characters.

11. Enter a brief description for this rule set in the **Rule Set Description** field.

    A valid length for this field is 0 – 127 characters.

12. Do one of the following:

   - If you want add a new time ranges you have already configured to the rule set, leave checkbox to the left of **Configure ACL Rules with Time Range** checked , or
   - If you want to proceed with the import using the time ranges already configured in the previous steps, uncheck the box to the left of **Configure ACL Rules with Time Range**.

13. Click **Next**.
14. Do one of the following:
   o If you checked the box to **Configure ACL Rules with Time Range**, click **Add** under **Configure Time Range** to add a time range to this rule set, or
   o If you do not want to add a time range, skip to **Step 17**.

15. Enter a name for the time range in the **Name** field of the **Add Time Range** page.
   Time Range names must begin with a letter [A-Z] and consist of 1-32 characters. Blank spaces [ ] and question marks [?] are not permitted. Uppercase letters may be converted to lowercase letters by some devices after deployment.
   a. Click **Add** to enter a time range.
      The **Add Time Range** dialog box appears.
   b. Select the type of time range you want to create by clicking the radio button ☐ to the left of the desired time range type
      o **Fixed** if you want to identify a specific and finite start and end date and time, or
      o **Cyclic** if you want the time range to recur for selected days of the week.

16. Select one of the options for importing rules:
   o To add all of the rules from the template the new ACL, skip to the next step, or
   o To delete one or more of the template rules, click the checkbox ☐ to the left of the sequence number for each of the rules you want to delete
   a. Click **Delete**. When prompted, click **OK** to confirm the deletion of the selected rules.
   b. Skip to the next step.
   o To add new rules click **Add** on the **Configure Rule** page.
      The **Add Rule** page appears.
   c. Select the protocol for which you want to permit or deny traffic from the **Protocol** list.
   d. Select the action you want to take by clicking the radio button ☐ to the left of the option you want to apply to this rule.
      o Select permit if, upon matching the specified conditions, the packet should be forwarded, or
      o Select **deny** if, upon matching the specified conditions, the packet should be discarded.

17. Select the time range you want to apply to this rule from the **Time Range** list.

18. Select the source IP address option you want to use by clicking the radio button ☐ to the left of the desired option in the **Source Address** field of the **Add Rule** page.
   This option specifies where the pattern matching occurs in this rule. In this case, the pattern matching is applied to the source IP address.
   o **All**: Allows you to permit or deny traffic for all IP addresses.
   o **IP Address/Mask**: Allows you to enter a specific IP address and its subnet mask for which you want to either permit or deny traffic for.
   a. Enter an IP address/subnet mask combination in the **IP Address/Mask** field.
      The subnet mask must be entered in dotted decimal notation. A valid IP address/subnet mask using dotted decimal notation would be
      192.168.1.0/255.255.255.0
   A forward slash “/” must be used to separate the IP address from the subnet mask.

19. Select the destination IP address option you want to use by clicking the radio button ☐ to the left of the desired option in the **Destination Address** field of the **Add Rule** page.
This option specifies where the pattern matching occurs in this rule. In this case, the pattern matching is applied to the source IP address.

- **All**: Allows you to permit or deny traffic for all IP addresses.
- **IP Address/Mask**: Allows you to enter a specific IP address and its subnet mask for which you want to either permit or deny traffic.

  a. Enter an IP address/subnet mask combination in the **IP Address/Mask** field.

The subnet mask must be entered in dotted decimal notation. A valid IP address/subnet mask using dotted decimal notation would be 192.168.1.0/255.255.255.0

A forward slash "/" must be used to separate the IP address from the subnet mask.

20. If you selected TCP or UDP as the protocol you want to apply this ACL rule to in **Step 17**, you must also specify the source TCP or UDP port numbers.

21. Select the source TCP or UDP port by clicking the radio button ○ to the left of the port option you want to apply in the **Source Port** field of the **Add Rule** page. Options include:

- **Undefined**: Allows you to permit or deny traffic for all TCP or UDP port numbers, or
- **Specified Port**: Allows you to identify a specific TCP or UDP port number or range of numbers.

  a. Click the radio button ○ to the left of **Specified Port** and select the operator you want to use from the list located to the right of the **Specified Port** option.

  b. Enter the TCP or UDP port number in the **Port** field.

22. If you selected TCP or UDP as the protocol you want to apply this ACL rule to, you must also specify the destination TCP or UDP port numbers:

- Select the destination TCP or UDP port by clicking the radio button ○ to the left of the port option you want to apply in the **Destination Port** field of the **Add Rule** page. Options include:

  - **Undefined**: Allows you to permit or deny traffic for all TCP or UDP port numbers, or
  - **Specified Port**: Allows you to identify a specific TCP or UDP port number or range of numbers. Click the radio button ○ to the left of **Specified Port** and select the operator you want to use from the list located to the right of the **Specified Port** option.

  a. Enter the TCP or UDP port number in the **Port** field.

23. If you selected TCP or UDP as the protocol you want to apply this ACL rule to, you could be promoted to select these options:

- Click the radio button ○ to the left of **Yes** in the **HP ACK** option if you want to apply the rule to match the TCP ACK, otherwise click on the radio button to the left of **No**.

- Click the radio button ○ to the left of **Yes** in the **HP FIN** option if you want to apply the rule to match the TCP FIN, otherwise click on the radio button to the left of **No**.

- Click the radio button ○ to the left of **Yes** in the **HP RST** option if you want to apply the rule to match the TCP RST, otherwise click on the radio button to the left of **No**.

- Click the radio button ○ to the left of **Yes** in the **HP SYN** option if you want to apply the rule to match the TCP SYN, otherwise click on the radio button to the left of **No**.

The **HP ACK**, **HP FIN**, **HP RST**, or **HP SYN** settings are valid only for the HP E series devices.

24. Select the IP priority you want to apply to ACL from the **IP Priority** list.

25. Select the Type of Service for this ACL from the **TOS Value** list.

26. Select the DSCP value you want to apply to this ACL from the **DSCP Value** list.

27. Do one of the following:
o Click the radio button ☐ to the left of Yes in the Fragment option if you want to apply the rule to each fragment, or
o Click the radio button ☐ to the left of No in the Fragment option if you want to apply the rule to first fragments.

Traditional packet filtering matched only first fragments of IPv4 packets and allowed all subsequent non-first fragments to pass through. This resulted in security risks as hackers can fabricate non-first fragments to attack networks.

28. Click the radio button ☐ to the left of Yes in the Logging option if you want to enable logging for this rule.

This feature enables the logging of packet filtering only when a module (for example, a firewall) using the ACL supports logging.

29. Enter the VPN instance you want to apply to this rule by entering the VPN-instance-name in the VPN Instance field.

30. A valid entry must be 0-31 characters that cannot contain question marks or blank spaces. Note also that this field is case sensitive. If no VPN instance is specified in this field, the rule will apply only to non-VPN packets.

31. Click OK to create the rule you have just configured.

32. Do one of the following:
   o To add more rules to the ACL, repeat this step, or
   o To modify rules you have already created, click the Modify icon associated with the rule sequence you want to modify. For more information modifying a rule set, see “Adding or modifying an advanced rule in an advanced rule set” (page 745), or
   o To copy rules you have already created, click the Copy icon associated with the rule sequence you want to copy. For more information copying a rule set, see “Copying a rule in an ACL rule set” (page 750), or
   o Rules that belong to a rule set that is configured with a Match Order of ‘Config’ are executed in the order in which they appear in the rule set. The order in which rules appear in a rule set is initially defined by the order in which they are created. You can, however, reorder the rules in a rule set using the Sort feature. For more information using Sort to redefine the order of appearance of rules in a rule set, see “Using sort to reorder the rules in an ACL rules set” (page 752), or
   o ACLs can have a profound effect on the performance of networks. ACL Management automatically evaluates the effectiveness of rules and their effect on overall network performance as you add rules to a rule set. However, you can also manually perform an analysis of a rule set and optimize its effect on network performance using the Optimize feature. For more information using this feature, see “Optimizing the rules in a rule set” (page 752), or
   o To delete one or more rules from a rule set, see “Deleting rules from an ACL rule set” (page 751).

33. Click Finish to accept your configuration for the import process and to create the new rule set.

Importing a link ACL template into a link ACL

To import the contents of a link template into a link ACL:

1. Navigate to ACL Resource:
   a. Click the Service tab from the tabular navigation system on the top.
   b. Click the ACL Management icon located under the Resource and Configuration Management section of the Service tab.
c. Click the **ACL Resource** link located under **ACL Management** on the navigation tree on the left. The **ACL Resource** list displays in the main pane of the **ACL Resource** page.

2. Click the **ACL Identifier** for the Link ACL for which you want to import the contents of a link template. The **Rule Set List** for the selected ACL displays in the main pane of the **ACL Resource** page.

3. Click **Import**. The **Import ACL Template to ACL Resource** page appears.

4. Select the ACL template you want to import from the **ACL Template** list. The page updates to display the **Basic Info** step of the **Add Rule Set** page.

A valid entry must be 0-31 characters that cannot contain question marks or blank spaces. This field is case sensitive. If no VPN instance is specified in this field, the rule applies only to non-VPN packets. Several fields cannot be changed. These include the **ACL Identifier**, the **ACL Type**, and the **ACL Resource Name**.

5. Enter a name for the rule set in the **Rule Set Name** field. A valid length for a rule set name is 1 – 32 characters.

6. Select the match order you want to apply to this rule set by clicking the radio button **Config** to the left of the **Match Order** option you want to use:
   - If you select **Config**, IMC matches rules in the order in which they were configured and only works for devices that support it, or
   - If you select **Auto**, IMC matches rules based on the principle of depth priority.

7. Enter a brief description for this ACL in the **ACL Description** field. A valid length for this field is 0 - 127 characters.

8. Enter a brief description for this rule set in the **Rule Set Description** field. A valid length for this field is 0 - 127 characters.

9. Do one of the following:
   - To add a new time ranges you have already configured to the rule set, leave checkbox to the left of **Configure ACL Rules with Time Range** checked **✓**, or
   - To proceed with the import using the time ranges already configured in the previous steps, uncheck the box to the left of **Configure ACL Rules with Time Range**.

10. Click **Next**.

11. Do one of the following:
   - If you checked the box to **Configure ACL Rules with Time Range**, click **Add** under **Configure Time Range** to add a time range to this rule set, or
   - If you do not want to add a time range, skip to **Step 12**.

12. Enter a name for the time range in the **Name** field of the **Add Time Range** page. Time Range names must begin with a letter [A-Z] and consist of 1-32 characters. Blank spaces [ ] and question marks [?] are not permitted. Uppercase letters may be converted to lowercase letters by some devices after deployment.

13. Click **Add** to enter a time range. The **Add Time Range** dialog box appears.
14. Select the type of time range you want to create by clicking the radio button ☐ to the left of the desired time range type:
   - **Fixed** if you want to identify a specific and finite start and end date and time, or
   - **Cyclic** if you want the time range to recur for selected days of the week.

15. Select from the following options to import rules:
   - To add all of the rules from the template to the new ACL, skip to the next, or
   - To delete one or more of the template rules, click the checkbox ☐ to the left of the sequence number for each of the rules you want to delete, and:
     a. Click Delete.
     b. When prompted, click OK to confirm the deletion of the selected rules.
     c. Skip to the next step.
   - To add new rules, click Add on the Configure Rule page.
     The Add Rule page appears.

16. Select the action you want to take by clicking the radio button ☐ to the left of the option you want to apply to this rule:
   - Select **permit** if, upon matching the specified conditions, the packet should be forwarded, or
   - Select **deny** if, upon matching the specified conditions, the packet should be discarded.

     a. Select the time range you want to apply to this rule from the **Time Range** list.
     b. Select the source MAC address option you want to use by clicking the radio button ☐ to the left of the desired option in the **Source MAC Addr** section of the Configure Rule – Add Rule page.

     This option specifies where the pattern matching occurs in this rule. In this case, the pattern matching is applied to the source MAC address.

     - **All**: Allows you to permit or deny traffic for all MAC addresses.
     - **MAC Address/Mask**: Allows you to enter a specific MAC address and mask for which you want to either permit or deny traffic for.

     A valid MAC address format for IMC consists of three sets of four hexadecimal characters separated by a dash, ".". For example,
     0014-2ad9-05f7
     would be a valid entry for a MAC address in IMC.

     Similarly, the format for a MAC address mask consists of three sets of four hexadecimal characters separated by a dash, ".". For example,
     ffff-ffff-ffff
     would be a valid entry for a MAC address mask in IMC.

     The MAC address and its mask must be separated by a forward slash, "/".

     A valid entry for a **MAC Address/Mask** would be
     0014-2ad9-05f7/ffff-ffff-ffff

17. Select the destination MAC address option you want to use by clicking the radio button ☐ to the left of the desired option in the **Destination MAC Address** section of the Configure Rule – Add Rule page.

     This option specifies where the pattern matching occurs in this rule. In this case, the pattern matching is applied to the source MAC address.

     - **All**: Allows you to permit or deny traffic for all MAC addresses.
- **MAC Address/Mask**: Allows you to identify a specific MAC address and its mask for which you want to either permit or deny traffic.

A valid MAC address format for IMC consists of three sets of four hexadecimal characters separated by a dash, ".". For example,

```
0014-2ad9-05f7
```

would be a valid entry for a MAC address in IMC.

Similarly, the format for a MAC address mask consists of three sets of four hexadecimal characters separated by a dash, ".". For example,

```
ffff-ffff-ffff
```

would be a valid entry for a MAC address mask in IMC.

The MAC address and its mask must be separated by a forward slash, "/".

A valid entry for a **MAC Address/Mask** would be

```
0014-2ad9-05f7/ffff-ffff-ffff
```

18. Select the 802.1 priority you want to apply to this ACL rule from the **802.1 Priority** list.

19. Select the Layer 2 encapsulation type you want to apply to this ACL rule from the **Encapsulation Type** list.

20. Enter the Source VLAN ID by entering it in the **Source VLAN ID** field.

   This field cannot contain question marks or blank spaces.

21. Select the Layer 2 frame type from the **Based Frame Type** list.

22. If you selected Ethernet Frame or 802.2 Ethernet Frame in the **Base Frame Type** list, you must specify a code in the **Code** field.

   A valid entry for this field includes any four character hexadecimal value.

23. If you selected Ethernet Frame or 802.2 Ethernet Frame in the **Base Frame Type** list, you must also specify a mask in the **Mask** field.

   A valid entry for this field includes any four character hexadecimal value.

24. Click **OK** to create the rule you have just configured.

25. Do one of the following:

   - To add more rules to the ACL, repeat this step, or
   - To modify rules you have already created, click the **Modify** icon associated with the rule sequence you want to modify. For more information modifying a rule set, see "Adding or modifying a link rule in a link rule set" (page 747), or
   - To copy rules you have already created, click the **Copy** icon associated with the rule sequence you want to copy. For more information copying a rule set, see "Copying a rule in an ACL rule set" (page 750), or
   - Rules that belong to a rule set that is configured with a **Match Order** of 'Config' are executed in the order in which they appear in the rule set. The order in which rules appear in a rule set is initially defined by the order in which they are created. You can, however, reorder the rules in a rule set using the **Sort** feature. For more information using Sort to redefine the order of appearance of rules in a rule set, see "Using sort to reorder the rules in an ACL rules set" (page 752), or
   - ACLs can have a profound effect on the performance of networks. ACL Management automatically evaluates the effectiveness of rules and their effect on overall network performance as you add rules to a rule set. However, you can also manually perform an analysis of a rule set and optimize its effect on network performance using the **Optimize** feature. For more information using this feature, see "Optimizing the rules in a rule set" (page 752), or
To delete one or more rules from a rule set, see "Deleting rules from an ACL rule set" (page 751).

26. Click Finish to accept your configuration for the import process and to create the new rule set.

Importing a user-defined ACL template into a user-defined ACL

To import the contents of a user-defined template into a user-defined ACL:

1. Navigate to ACL Resource:
   a. Click the Service tab from the tabular navigation system on the top.
   b. Click the ACL Management icon located under the Resource and Configuration Management section of the Service tab.
   c. Click the ACL Resource link located under ACL Management on the navigation tree on the left. The ACL Resource list displays in the main pane of the ACL Resource page.

2. Click the ACL Identifier for the User-Defined ACL for which you want to import the contents of a User-Defined template.
   The Rule Set List for the selected ACL displays in the main pane of the ACL Resource →<ACL Resource Name (ACL Identifier)> page.

3. Click Import.
   The Import ACL Template to ACL Resource page appears.

4. Select the ACL template you want to import from the ACL Template list.
   The page updates to display the Basic Info step of the Add Rule Set page.
   Only templates of the same type as the ACL you are importing into display on the ACL Template list.
   Several fields cannot be changed. These include the ACL Identifier, the ACL Type, and the ACL Resource Name.

5. Enter a name for the rule set in the Rule Set Name field.
   A valid length for a rule set name is 1 – 32 characters.
   You cannot configure or modify the Match Order configuration of a User-Defined Rule.

6. Enter a brief description for this ACL in the ACL Description field.
   A valid length for this field is 0 – 127 characters.

7. Enter a brief description for this rule set in the Rule Set Description field.
   A valid length for this field is 0 – 127 characters.

8. Do one of the following:
   o To add a new time ranges you have already configured to the rule set, leave checkbox to the left of Configure ACL Rules with Time Range checked ✓, or
   o To proceed with the import using the time ranges already configured in the previous steps, uncheck the box to the left of Configure ACL Rules with Time Range □.

9. Click Next.

10. Do one of the following:
    o If you checked the box to Configure ACL Rules with Time Range, click Add under Configure Time Range to add a time range to this rule set, or
    o If you do not want to add a time range, skip to Step 11.
    a. Enter a name for the time range in the Name field of the Add Time Range page.
Time Range names must begin with a letter [A-Z] and consist of 1-32 characters. Blank spaces [ ] and question marks [?] are not permitted. Uppercase letters may be converted to lowercase letters by some devices after deployment.

b. Click Add to enter a time range.

The Add Time Range dialog box appears.

c. Select the type of time range you want to create by clicking the radio button ○ to the left of the desired time range type:

- Fixed if you want to identify a specific and finite start and end date and time, or
- Cyclic if you want the time range to recur for selected days of the week.

11. Select from the following options to import rules:

- To add all of the rules from the template to the new ACL, skip to the next step, or,
- To delete one or more of the template rules, click the checkbox square to the left of the sequence number for each of the rules you want to delete.

a. Click Delete.

b. When prompted, click OK to confirm the deletion of the selected rules.

c. Skip to the next step, or

- To add new rules, click Add on the Configure Rule page to configure a new rule.

The Add Rule page appears.

12. Select the action you want to take by clicking the radio button ○ to the left of the option you want to apply to this rule:

- Select permit if, upon matching the specified conditions, the packet should be forwarded, or
- Select deny if, upon matching the specified conditions, the packet should be discarded.

13. Select the time range you want to apply to this rule from the Time Range list.

You can enter up to eight hexadecimal patterns, masks, and offsets for matching the contents of a packet and applying the actions specified in the rule when a hexadecimal pattern is matched. The following rules and guidelines apply to constructing a valid hexadecimal string, mask, and offset value.

- A rule string must be expressed in hexadecimal only
- A mask must be expressed in hexadecimal only
- A rule string length must be equal to its mask length
- Rule string and mask length must be in multiples of 2
- The minimum length of a rule string and mask is 2
- The maximum length of a rule string and mask is 160
- Offsets must be expressed as a decimal integer
- Offset range varies by the mask length
- The minimum value for an offset is 0
- The maximum value for an offset is 79
- The offset must increase progressively

a. Enter a hexadecimal pattern to be matched in the Rule String field.

b. Enter a mask in the Mask field.

c. Enter the offset in the Excursion field.
d. Enter up to eight Rule String/Mask/Excursion combinations.

14. Click OK to create the rule you have just configured.

15. Select one of the following:
   o To add more rules to the ACL, repeat this step, or
   o To modify rules you have already created, click the Modify icon associated with the rule sequence you want to modify. For more information modifying a rule set, see "Adding or modifying a user-defined rule in a user-defined rule set" (page 749), or
   o To copy rules you have already created, click the Copy icon associated with the rule sequence you want to copy. For more information copying a rule set, see "Copying a rule in an ACL rule set" (page 750), or
   o Rules that belong to a rule set that is configured with a Match Order of 'Config' are executed in the order in which they appear in the rule set. The order in which rules appear in a rule set is initially defined by the order in which they are created. You can, however, reorder the rules in a rule set using the Sort feature. For more information using Sort to redefine the order of appearance of rules in a rule set, see "Using sort to reorder the rules in an ACL rules set" (page 752), or
   o Access control lists can have a profound effect on the performance of networks. ACL Management automatically evaluates the effectiveness of rules and their effect on overall network performance as you add rules to a rule set. However, you can also manually perform an analysis of a rule set and optimize its effect on network performance using the Optimize feature. For more information using this feature, see "Optimizing the rules in a rule set" (page 752), or
   o To delete one or more rules from a rule set, see "Deleting rules from an ACL rule set" (page 751).

16. Click Finish to accept your configuration for the import process and to create the new rule set.

Deleting rule sets

To delete one or more rule sets from an ACL:

1. Navigate to ACL Resource:
   a. Click the Service tab from the tabular navigation system on the top.
   b. Click the ACL Management icon located under the Resource and Configuration Management section of the Service tab.
   c. Click the ACL Resource link located under ACL Management on the navigation tree on the left. The ACL Resource list displays in the main pane of the ACL Resource page.

2. Click the ACL Identifier of the ACL for which you want to create a copy of a rule set.
   The Rule Set List for the selected ACL displays in the main pane of the ACL Resource page.

3. Click the checkboxes to the left of the rule sets you want to delete from the ACL.

4. Click Delete.

5. Click OK to confirm the deletion of the selected rule sets.

Managing the rules in a rule set

ACL Management provides you with the ability to manage the rules within the rule set, including adding, modifying, copying, deleting, sorting, and optimizing rules.
Adding or modifying the rules in a rule set

Once an ACL has been created, you can add rules to it or modify the existing rules. The process for doing both is essentially the same, however the process for modifying rules of different types is different and you can only add rules of the same type as the ACL.

Adding or modifying a basic rule in a basic ACL rule set

To add or modify a basic rule in a basic rule set:

1. Navigate to ACL Resource.
   a. Click the Service tab from the tabular navigation system on the top.
   b. Click the ACL Management icon located under the Resource and Configuration Management section of the Service tab.
   c. Click the ACL Resource link located under ACL Management on the navigation tree on the left. The ACL Resource list displays in the main pane of the ACL Resource page.
2. Click the ACL Identifier of the ACL for which you want to add or modify a rule.
   The Rule Set List for the selected ACL displays in the main pane of the ACL Resource→ACL Resource Name (ACL Identifier) page.
3. Click the icon in the Modify field associated with the rule you want to add a rule to. The Basic Info step of the Modify Rule Set page appears.
4. Click Next to advance to the next step in the Modify Rule Set page.
   The Configure Time Range step of the Modify Rule Set page appears.
5. Click Next to advance to the next step in the Modify Rule Set page.
   The Configure Rule page appears.
6. Click Add on the Configure Rule page to configure a new rule. The Add Rule page appears.
7. To modify a rule, click the Modify icon associated with the rule you want to modify. The Modify Rule page appears.
8. Select the action you want to take by clicking the radio button to the left of the option you want to apply to this rule:
   o Select permit if, upon matching the specified conditions, the packet should be forwarded, or
   o Select deny if, upon matching the specified conditions, the packet should be discarded.
9. Select the time range you want to apply to this rule from the Time Range list.
10. Select the source IP address option you want to use by clicking the radio button to the left of the desired option in the Source Address field.
    This option specifies where the pattern matching occurs in this rule. In this case, the pattern matching is applied to the source IP address.
    o All: Allows you to permit or deny traffic for all IP addresses.
    o IP Address/Mask: Allows you to enter a specific IP address and its subnet mask for which you want to either permit or deny traffic for.
   a. Enter an IP address/subnet mask combination in the IP Address/Mask field.
   The subnet mask must be entered in dotted decimal notation. A valid IP address/subnet mask using dotted decimal notation would be
192.168.1.0/255.255.255.0

A forward slash “/” must be used to separate the IP address from the subnet mask.

11. Do one of the following:
   o Click the radio button ○ to the left of Yes in the Fragment option if you want to apply the rule to each fragment, or
   o Click the radio button ○ to the left of No in the Fragment option if you want to apply the rule to first fragments.

Traditional packet filtering matched only first fragments of IPv4 packets and allowed all subsequent non-first fragments to pass through. This resulted in security risks as hackers can fabricate non-first fragments to attack networks.

12. Click the radio button ○ to the left of Yes in the Logging option if you want to enable logging for this rule.

   This feature enables the logging of packet filtering only when a module (for example, a firewall) using the ACL supports logging.

13. Enter the VPN instance you want to apply to this rule by entering the VPN-instance-name in the VPN Instance field.

   A valid entry must be 0-31 characters that cannot contain question marks or blank spaces. This field is case sensitive. If no VPN instance is specified in this field, the rule applies only to non-VPN packets.

14. Click OK to create or modify the rule you have just configured.

Adding or modifying an advanced rule in an advanced rule set

To add or modify an advanced rule in an advanced rule set:

1. Navigate to ACL Resource:
   a. Click the Service tab from the tabular navigation system on the top.
   b. Click the ACL Management icon located under the Resource and Configuration Management section of the Service tab.
   c. Click the ACL Resource link located under ACL Management on the navigation tree on the left.

   The ACL Resource list displays in the main pane of the ACL Resource page.

2. Click the ACL Identifier of the Advanced ACL for which you want to add or modify an advanced rule.

   The Rule Set List for the selected ACL displays in the main pane of the ACL Resource → <ACL Resource Name (ACL Identifier)> page.

3. Click the icon in the Modify field associated with the rule you want to add a rule to.

   The Basic Info step of the Modify Rule Set page appears.

4. Click Next to advance to the next step in the Modify Rule Set page.

   The Configure Time Range step of the Modify Rule Set page appears.

5. Click Next to advance to the next step in the Modify Rule Set page.

   The Configure Rule page appears.

6. Click Add on the Configure Rule page to configure a new rule.

   The Add Rule page appears.

7. To modify a rule, click the Modify icon associated with the rule you want to modify.

   The Modify Rule page appears.

8. Select the protocol for which you want to permit or deny traffic from the Protocol list.
9. Select the action you want to take by clicking the radio button ☑️ to the left of the option you want to apply to this rule:
   - Select **permit** if, upon matching the specified conditions, the packet should be forwarded, or
   - Select **deny** if, upon matching the specified conditions, the packet should be discarded.

10. Select the time range you want to apply to this rule from the **Time Range** list.

11. Select the source IP address option you want to use by clicking the radio button ☑️ to the left of the desired option in the **Source Address** section.
   This option specifies where the pattern matching occurs in this template rule. In this case, the pattern matching is applied to the source IP address.
   - **All**: Allows you to permit or deny traffic for all IP addresses.
   - **IP Address/Mask**: Allows you to enter a specific IP address and its subnet mask for which you want to either permit or deny traffic for.
     a. Enter an IP address/subnet mask combination in the **IP Address/Mask** field.
        The subnet mask must be entered in dotted decimal notation. A valid IP address/subnet mask using dotted decimal notation would be
        192.168.1.0/255.255.255.0
        A forward slash “/” must be used to separate the IP address from the subnet mask.

12. Select the destination IP address option you want to use by clicking the radio button ☑️ to the left of the desired option in the **Destination Address** field.
   This option specifies where the pattern matching occurs in this template rule. In this case, the pattern matching is applied to the destination IP address.
   - **All**: Allows you to permit or deny traffic for all IP addresses.
   - **IP Address/Mask**: Allows you to enter a specific IP address and its subnet mask for which you want to either permit or deny traffic.
     a. Enter an IP address/subnet mask combination in the **IP Address/Mask** field.
        The subnet mask must be entered in dotted decimal notation. A valid network/subnet mask using dotted decimal notation would be
        192.168.1.0/255.255.255.0
        A forward slash “/” must be used to separate the IP address from the subnet mask.

13. If you selected TCP or UDP as the protocol you want to apply this ACL rule to in **Step 7**, you must also specify the source TCP or UDP port numbers:
   a. To select the source TCP or UDP port, click the radio button ☑️ to the left of the port option you want to apply in the **Source Port** section:
      - **Undefined**: Allows you to permit or deny traffic for all TCP or UDP port numbers, or
      - **Specified Port**: Allows you to identify a specific TCP or UDP port number or range of numbers.
   b. Click the radio button ☑️ to the left of **Specified Port** and select the operator you want to use from the list located to the right of the **Specified Port** option.
   c. Enter the TCP or UDP port number in the **Port** field.

14. If you selected TCP or UDP as the protocol you want to apply this ACL rule to in **Step 7**, you must also specify the destination TCP or UDP port numbers clicking the radio button ☑️ to the left of the port option you want to apply in the **Destination Port** section.
   - **Undefined**: Allows you to permit or deny traffic for all TCP or UDP port numbers, or
   - **Specified Port**: Allows you to identify a specific TCP or UDP port number or range of numbers.
a. Click the radio button ☐ to the left of Specified Port and select the operator you want to use from the list located to the right of the Specified Port option.

b. Enter the TCP or UDP port number in the Port field.

15. If you selected TCP or UDP as the protocol you want to apply this ACL rule to in Step 7, you could be promoted to select these options:
   o Click the radio button ☐ to the left of Yes in the HP ACK option if you want to apply the rule to match the TCP ACK, otherwise click on the radio button ☐ to the left of No.
   o Click the radio button ☐ to the left of Yes in the HP FIN option if you want to apply the rule to match the TCP FIN, otherwise click on the radio button ☐ to the left of No.
   o Click the radio button ☐ to the left of Yes in the HP RST option if you want to apply the rule to match the TCP RST, otherwise click on the radio button ☐ to the left of No.
   o Click the radio button ☐ to the left of Yes in the HP SYN option if you want to apply the rule to match the TCP SYN, otherwise click on the radio button ☐ to the left of No.
   
The HP ACK, HP FIN, HP RST, and HP SYN settings are valid only for the HP E series devices.

16. Select the IP priority you want to apply to ACL template from the IP Priority list.
17. Select the Type of Service for this ACL template from the ToS Value list.
18. Select the DSCP value you want to apply to this ACL template from the DSCP Value list.
19. Do one of the following:
   o Click the radio button ☐ to the left of Yes in the Fragment option if you want to apply the rule to each fragment, or
   o Click the radio button ☐ to the left of No in the Fragment option if you want to apply the rule to first fragments.
   
Traditional packet filtering matched only first fragments of IPv4 packets and allowed all subsequent non-first fragments to pass through. This resulted in security risks as hackers can fabricate non-first fragments to attack networks.

20. Click the radio button ☐ to the left of Yes in the Logging option if you want to enable logging for this rule.
   
   This feature enables the logging of packet filtering only when a module (for example, a firewall) using the ACL supports logging.

21. Enter the VPN instance you want to apply to this rule by entering the VPN-instance-name in the VPN Instance field.
   
   A valid entry must be 0-31 characters that cannot contain question marks or blank spaces. This field is case sensitive. If no VPN instance is specified in this field, the rule applies only to non-VPN packets.

22. Click OK to create or modify the rule you have just configured.

Adding or modifying a link rule in a link rule set

To add or modify a link rule in a link rule set:

1. Navigate to ACL Resource:
   a. Click the Service tab from the tabular navigation system on the top.
   b. Click the ACL Management icon located under the Resource and Configuration Management section of the Service tab.
   c. Click the ACL Resource link located under ACL Management on the navigation tree on the left.
The **ACL Resource** list displays in the main pane of the **ACL Resource** page.

2. Click the **ACL Identifier** of the ACL for which you want to add or modify a rule.

The **Rule Set List** for the selected ACL displays in the main pane of the **ACL Resource** page.

3. Click the icon in the **Modify** field associated with the rule you want to add a rule to.

The **Basic Info** step of the **Modify Rule Set** page appears.

4. Click **Next** to advance to the next step in the **Modify Rule Set** page.

The **Configure Time Range** step of the **Modify Rule Set** page appears.

5. Click **Next** to advance to the next step in the **Modify Rule Set** page.

The **Configure Rule** page appears.

6. Click **Add** on the **Configure Rule** page to configure a new rule.

The **Add Rule** page appears.

7. To modify a rule, click on the **Modify** icon associated with the rule you want to modify.

The **Modify Rule** page appears.

8. Select the action you want to take by clicking the radio button to the left of the option you want to apply to this rule:
   
   - Select **permit** if, upon matching the specified conditions, the packet should be forwarded, or
   
   - Select **deny** if, upon matching the specified conditions, the packet should be discarded.

9. Select the time range you want to apply to this rule from the **Time Range** list.

10. Select the source MAC address option you want to use by clicking the radio button to the left of the desired option in the **Source MAC Addr** field.

    This option specifies where the pattern matching occurs in this template rule. In this case, the pattern matching is applied to the source MAC address.

    - **All**: Allows you to permit or deny traffic for all MAC addresses.
    
    - **MAC Address/Mask**: Allows you to enter a specific MAC address and mask for which you want to either permit or deny traffic for.

    A valid MAC address format for IMC consists of three sets of four hexadecimal characters separated by a dash, ".". For example:

    0014-2ad9-05f7

    would be a valid entry for a MAC address in IMC.

    Similarly, the format for a MAC address mask consists of three sets of four hexadecimal characters separated by a dash, ".". For example:

    ffff-ffff-ffff

    would be a valid entry for a MAC address mask in IMC.

    The MAC address and its mask must be separated by a forward slash, "/".

    A valid entry for a **MAC Address/Mask** would be

    0014-2ad9-05f7/ffff-ffff-ffff

11. Select the destination MAC address option you want to use by clicking the radio button to the left of the desired option in the **Destination Address** section.

    This option specifies where the pattern matching occurs in this template rule. In this case, the pattern matching is applied to the destination MAC address.
- **All**: Allows you to permit or deny traffic for all MAC addresses, or
- **MAC Address/Mask**: Allows you to identify a specific MAC address and its mask for which you want to either permit or deny traffic.

A valid MAC address format for IMC consists of three sets of four hexadecimal characters separated by a dash, ",-". For example:
```
0014-2ad9-05f7
```
would be a valid entry for a MAC address in IMC.

Similarly, the format for a MAC address mask consists of three sets of four hexadecimal characters separated by a dash, ",-". For example:
```
ffff-ffff-ffff
```
would be a valid entry for a MAC address mask in IMC.

The MAC address and its mask must be separated by a forward slash, "/".

A valid entry for a **MAC Address/Mask** would be
```
0014-2ad9-05f7/ffff-ffff-ffff
```

12. Select the 802.1 priority you want to apply to this ACL rule from the **802.1 Priority** list.
13. Select the Layer 2 encapsulation type you want to apply to this ACL rule from the **Encapsulation Type** list.
14. Enter the Source VLAN ID by entering it in the **Source VLAN ID** field. This field cannot contain question marks or blank spaces.
15. Select the Layer 2 frame type from the **Based Frame Type** list.
16. If you selected **Ethernet Frame** or **802.2 Ethernet Frame** in the **Base Frame Type** list, you must specify a code in the **Code** field. A valid entry for this field includes any four character hexadecimal value.
17. If you selected **Ethernet Frame** or **802.2 Ethernet Frame** in the **Base Frame Type** list, you must also specify a mask in the **Mask** field. A valid entry for this field includes any four character hexadecimal value.
18. Click **OK** to create the rule you have just configured.

Adding or modifying a user-defined rule in a user-defined rule set

To add or modify a user-defined rule in a user-defined rule set:

1. Navigate to **ACL Resource**:
   a. Click the **Service** tab from the tabular navigation system on the top.
   b. Click the **ACL Management** icon located under the **Resource and Configuration Management** section of the **Service** tab.
   c. Click the **ACL Resource** link located under **ACL Management** on the navigation tree on the left. The **ACL Resource** list displays in the main pane of the **ACL Resource** page.
2. Click the **ACL Identifier** of the User-Defined ACL for which you want to add or modify a user-defined rule.
   The **Rule Set List** for the selected ACL displays in the main pane of the **ACL Resource→<ACL Resource Name (ACL Identifier)>** page.
3. Click the icon in the **Modify** field associated with the rule you want to add a rule to. The **Basic Info** step of the **Modify Rule Set** page appears.

4. Click **Next** to advance to the next step in the **Modify Rule Set** page. The **Configure Time Range** step of the **Modify Rule Set** page appears.

5. Click **Next** to advance to the next step in the **Modify Rule Set** page. The **Configure Rule** page appears.

6. Click **Add** on the **Configure Rule** page to configure a new rule. The **Add Rule** page appears.

7. To modify a rule, click on the **Modify** icon associated with the rule you want to modify. The **Modify Rule** page appears.

8. Select the action you want to take by clicking the radio button to the left of the option you want to apply to this rule:
   - Select **permit** if, upon matching the specified conditions, the packet should be forwarded, or
   - Select **deny** if, upon matching the specified conditions, the packet should be discarded.

9. Select the time range you want to apply to this rule from the **Time Range** list.

10. Enter up to eight hexadecimal patterns, masks, and offsets for matching the contents of a packet and applying the actions specified in the rule when a hexadecimal pattern is matched. The following rules and guidelines apply to constructing a valid hexadecimal string, mask, and offset value:
    - A rule string must be expressed in hexadecimal only
    - A mask must be expressed in hexadecimal only
    - A rule string length must be equal to its mask length
    - Rule string and mask length must be in multiples of 2
    - The minimum length of a rule string and mask is 2
    - The maximum length of a rule string and mask is 160
    - Offsets must be expressed as a decimal integer
    - Offset range varies by the mask length
    - The minimum value for an offset is 0
    - The maximum value for an offset is 79
    - The offset must increase progressively
    
    a. Enter a hexadecimal pattern to be matched in the **Rule String** field.
    b. Enter a mask in the **Mask** field.
    c. Enter the offset in the **Excursion** field.
    d. Enter up to eight **Rule String/Mask/Excursion** combinations.

11. Click **OK** to create the rule you have just configured.

**Copying a rule in an ACL rule set**

You can copy an existing rule in a rule set to a new rule in the same rule set and make modifications to the new copy.

To copy an existing rule and make modifications to it:

1. Navigate to **ACL Resource**:
a. Click the Service tab from the tabular navigation system on the top.

b. Click the ACL Management icon located under the Resource and Configuration Management section of the Service tab.

c. Click the ACL Resource link located under ACL Management on the navigation tree on the left.

The ACL Resource list displays in the main pane of the ACL Resource page.

2. Click the ACL Identifier of the ACL for which you want to copy a rule.

The Rule Set List for the selected ACL displays in the main pane of the ACL Resource → <ACL Resource Name (ACL Identifier)> page.

3. Click the icon in the Modify field associated with the rule you want to copy.

The Basic Info step of the Modify Rule Set page appears.

4. Click Next to advance to the next step in the Modify Rule Set page.

The Configure Time Range step of the Modify Rule Set page appears.

5. Click Next to advance to the next step in the Modify Rule Set page.

The Configure Rule step of the Modify Rule Set page appears with the rules for the associated rule set displayed.

6. Click the icon in the Copy field associated with the rule you want to copy.

7. You can make any modifications to the copy of a rule that you can to the rule itself, including creating new rules.

The steps for creating and modifying rules in a rule set vary by the ACL type to which the rule set belongs. For more information modifying rules, see "Modifying ACL rule sets" (page 718) and specifically to the section that addresses how to modify the type of rule set you want to copy. For example, if you have copied a rule from an advanced ACL, see "Modifying an advanced rule set" (page 720).

8. Click OK when you have finished modifying the copy to create the new copy.

Deleting rules from an ACL rule set

To delete one or more rules from a rule set:

1. Navigate to ACL Resource:

a. Click the Service tab from the tabular navigation system on the top.

b. Click the ACL Management icon located under the Resource and Configuration Management section of the Service tab.

c. Click the ACL Resource link located under ACL Management on the navigation tree on the left.

The ACL Resource list displays in the main pane of the ACL Resource page.

2. Click the ACL Identifier of the ACL from which you want to delete one or more rules.

The Rule Set List for the selected ACL displayed in the main pane of the ACL Resource → <ACL Resource Name (ACL Identifier)> page.

3. Click the icon in the Modify field associated with the rule you want to copy.

The Basic Info step of the Modify Rule Set page appears.

4. Click Next to advance to the next step in the Modify Rule Set page.

The Configure Time Range step of the Modify Rule Set page appears.

5. Click Next to advance to the next step in the Modify Rule Set page.
The **Configure Rule** step of the **Modify Rule Set** page displays with the associated rule set listed.

6. Click the checkbox □ to the left of the sequence numbers for the rules you want to delete.

7. Click **Delete**.

8. Click **OK** to confirm the deletion of the selected rules.

**Using sort to reorder the rules in an ACL rules set**

The order in which rules appear in a rule set can influence the effectiveness of an ACL rule set and its effect on network performance. This is true for rules that belong to a rule set that is configured with a **Match Order** of **Config** because rules are executed in the order in which they appear in the rule set. The order in which rules appear in a rule set is initially defined by the order in which they are created but you can reorder the rules in a rule set using the **Sort** feature.

To use the sort feature to reorder the rules in a rule set:

1. Navigate to **ACL Resource**:
   a. Click the **Service** tab from the tabular navigation system on the top.
   b. Click the **ACL Management** icon located under the **Resource and Configuration Management** section of the **Service** tab.
   c. Click the **ACL Resource** link located under **ACL Management** on the navigation tree on the left. The **ACL Resource** list displays in the main pane of the **ACL Resource** page.

2. Click the **ACL Identifier** of the ACL for which you want to sort a rule set.

   The **Rule Set List** for the selected ACL displays in the main pane of the **ACL Resource →<ACL Resource Name (ACL Identifier)>** page.

3. Click the icon in the **Modify** field associated with the rule set you want to sort.

   The **Basic Info** step of the **Modify Rule Set** page appears.

4. Click **Next** to advance to the next step in the **Modify Rule Set** page.

   The **Configure Time Range** step of the **Modify Rule Set** page appears.

5. Click **Next** to advance to the next step in the **Modify Rule Set** page.

   The **Configure Rule** step of the **Modify Rule Set** page displays with the associated rule set listed.

6. Click **Sort**.

   The **Rule Sort** dialog box appears.

7. Click the checkbox □ to the left of the rules you want to move.

8. Click one of the four navigation buttons located at the top of the **Rule Sort** dialog box:
   - Click **Top** to move the selected rules to the top of the list, or
   - Click **Up** to move the selected rules up one position in the list, or
   - Click **Down** to move the selected rules down one position in the list, or
   - Click **Bottom** to move the selected rules to the bottom of the list.

9. Click **OK** when you have finished sorting the rule set.

10. Click **Finish** to complete your modifications to the selected rule set.

**Optimizing the rules in a rule set**

ACLs can have a profound effect on the performance of networks. ACL Management automatically evaluates the effectiveness of rules and their effect on overall network performance as you add rules to a rule set, but
you can also initiate an analysis of a rule set and optimize its effect on network performance using the **Optimize** feature.

There are essentially two causes for performance degradation related to ACLs. First, every packet that arrives at an interface is matched against all the ACL rules until a match is found. The more rules there are, the longer it takes to process every packet. Second, all rules are matched in a certain order and more rules lead to more time processing the matching requirements of every rule and therefore leads to more time processing every packet.

ACL Management’s rule optimization algorithms improve both causes for performance degradation for ACLs that use **Config** as the **Match Order** because the sorting rules remove unnecessary rules and determine the applicable rules to reduce the effect of ACLs and to improve the overall performance of the device. In addition, ACL Management provides suggestions for efficient ACL implementation and simplified configurations based on the configured rules and the relations between them.

ACL Management optimizes the rules in the following ways:

- **Removing coverable rules**: If the coverage of a rule includes the coverage of another rule, the former overwrites the latter. The default rule is **Permit All**.
- **Removing duplicate rules**: If several rules perform the same function, the rule set is reduced to one rule that performs the same function.
- **Merging rules with mask-identified address segments**: If several rules have the same parameter values (including the address mask) with the exception of the IP or MAC address range, these rules are merged using appropriate mask settings.
- **Merging rules with duplicate port assignments**: If several rules have the same parameter values with the exception of the port, the rules are merged using appropriate port range settings.
- **Removing redundant rules**: If the coverage of a rule is included in the coverage of a preceding rule, the former rule is removed.
- **Reordering the rule set**: ACL Management reorders rule sets by placing the most commonly matched rules first.

In addition optimizing rule sets, ACL Management also notifies you of rules that may jeopardize device to IMC connections. To optimize a rule set:

1. **Navigate to **ACL Resource**:
   a. Click the **Service** tab from the tabular navigation system on the top.
   b. Click the **ACL Management** icon located under the **Resource and Configuration Management** section of the **Service** tab.
   c. Click the **ACL Resource** link located under **ACL Management** on the navigation tree on the left.
      The **ACL Resource** list displays in the main pane of the **ACL Resource** page.

2. **Click the **ACL Identifier** of the ACL for which you want to optimize a rule set.

ACL Management can optimize rule sets for ACLs that use **Config** as the **Match order**. Rule sets that use the **Match order Auto** cannot be optimized.

In addition, rule sets that use Services to define the port assignments for a rule cannot be optimized.

The **Rule Set List** for the selected ACL displays in the main pane of the **ACL Resource →<ACL Resource Name (ACL Identifier)>** page.

3. **Click the icon** in the **Modify** field associated with the rule set you want to optimize.
   The **Basic Info** step of the **Modify Rule Set** page appears.

4. **Click **Next** to advance to the next step in the **Modify Rule Set** page.
The **Configure Time Range** step of the **Modify Rule Set** page appears.

5. Click **Next** to advance to the next step in the **Modify Rule Set** page.

The **Configure Rule** step of the **Modify Rule Set** page displays with the rules for the associated rule set listed.

6. Click the **Optimize** button located at the top of the **Configure Rule** page.

The **Optimize** dialog box appears.

7. Select the device for which you want to optimize this rule set from the list located in upper left corner of the **Optimize** dialog box.

ACL Management displays a summary of all of the rules in a rule set in the **Before Optimize** column of the **Optimize** dialog box. The contents of this column changes based upon the device command line format selected in the **Select a device** list located in the upper left corner of the **Optimize** dialog box. The recommended changes to the rule set display in the **After Optimize** column of the **Optimize** dialog box, and the optimize advices display in the **Optimize Advice** box.

8. Select the device command line format you intend to apply this ACL rule set to from the **Select a device** list in the upper right corner. The columns update to reflect any changes required by the device command line format change.

9. Review the recommendations in the **After Optimize** column.

10. Click **OK** if you want to apply the changes recommended in the **After Optimize** column.

    If you select this option, the dialog box closes and the rule list in the **Configure Rule** step of the **Modify Rule Set** page updates to reflect the rule changes that resulted from the Optimize process.

11. Click **Cancel** if you do not want to apply the changes recommended in the **After Optimize** column. The rules in the rule set remain unchanged.

12. Click **Finish** to complete your modifications to the selected rule set.

### Managing device ACL configurations

ACL Management simplifies and streamlines the process of managing ACLs on devices by providing you with a single portal for viewing and managing the configurations for all devices that support ACLs. From the ACL Device List, you can view all devices that support ACLs and navigate quickly to the device configuration page to view detailed information the configuration for a single device.

From the configuration page you can synchronize and refresh the ACL configuration data for the device as well as configure the ACL configuration polling interval.

The tabs located in the lower half of the page provide the following:

- **ACL Definitions** tab: Add ACL definitions to the device or delete ACL definitions, export ACL to a text file, view details page for a single ACL or a single rule, save the selected device as an ACL resource or template, apply the ACL as a packet filter to one or more interfaces on the device, and view applied ACL uses that already exist on the device.
- **ACL Uses** tab: View the ACL uses currently deployed on the device as well as add and remove ACL uses.
- **Time Ranges** tab: View and delete time ranges that have been applied to ACLs.
- **Config History** tab: View the ACL configuration history for the selected device as well as view the configuration details for every entry in the configuration history. In addition, you can modify a configuration history entry and baseline an entry.
- **Flow Template Definitions** tab: View, add, modify, and remove flow templates for devices.
- **Flow Template Applications** tab: View, add, and remove flow templates that have been applied.
ACL device list management

ACL Management provides you with a single portal for viewing and managing the ACL configurations for all devices that support ACLs.

Viewing the ACL device list

To view the ACL devices list:

1. Navigate to **ACL Devices**:
   a. Click the **Service** tab from the tabular navigation system on the top.
   b. Click the **ACL Management** icon located under the **Resource and Configuration Management** section of the **Service** tab.
   c. Click the **ACL Devices** link located under **ACL Management** on the navigation tree on the left.

   The **ACL Devices** page appears with the deployment **ACL Devices** list displayed in this page.

   **ACL Devices** list
   o **Status**: Contains the most current status of the device. Status is determined by the highest severity or alarm level for the device, when the device has one or more current alarms that has not been cleared or recovered.
   o **Device Name**: Contains the IMC name for the device, which, by default, is the name assigned to it by IMC in its device configuration. The contents of the device label field serve as an active link for navigating to the **Device Details** page for the associated device.
   o **IP Address**: Contains the IP address of the associated device.
   o **Device Model**: Contains the model information for the associated device.
   o **Poll Interval**: Contains the ACL configuration polling interval for the selected device.
   o **Last Synchronize Time**: Contains the date and time stamp for the last time the IMC database was polled for the latest device configuration, including ACL definitions, ACL uses, and time ranges.
   o **Last Poll Result**: Contains information whether or not the last poll of the device was successful or not. Note that this field contains information for the cause of poll failures.
   o **ACL Config**: Contains an icon for navigating to the **ACL Device** configuration page for the associated device. This page provides detailed information the ACL configuration for associated device as well as features for managing the ACL configuration of the device.

   You can sort the **ACL Devices** list by every field with the exception of the **ACL Config** field. Click the column label to sort the list by the selected field. The column label is a toggle switch that allows you to toggle between the various sort options specific to each field.

   If the **ACL Devices** list contains multiple entries, the following navigational aids may appear:
   o Click to page forward in the **ACL Devices** list.
   o Click to page forward to the end of the **ACL Devices** list.
   o Click to page backward in the **ACL Devices** list.
   o Click to page backward to the front of the **ACL Devices** list.

2. Click 8, 15, 50, 100, or 200 from the right side of the main pane to configure how many items per page you want to view.

   You can configure the **ACL Devices** list to display all devices managed in IMC or only those devices that can support ACLs. To view only the devices in IMC that support ACLs, click the checkbox to
Only Show the devices that support ACL option located in the upper right corner of the ACL Devices list. IMC determines which devices support ACLs by the methods of communication that IMC uses to configure ACLs on devices. Therefore, if the device you want to manage ACLs for does not appear on this list, check the SNMP, Telnet, and SSH settings to ensure that IMC can communicate with the device.

**Querying ACL devices list**

To search the ACL devices list for a specific device:

1. Navigate to ACL Devices:
   a. Click the Service tab from the tabular navigation system on the top.
   b. Click the ACL Management icon located under the Resource and Configuration Management section of the Service tab.
   c. Click the ACL Devices link located under ACL Management on the navigation tree on the left. The search conditions display in the Query Condition section of the ACL Devices page.

2. Enter one or more of the following search criteria in the Query Condition section of the page:
   - Device Name: Enter a partial or complete device name in the Device Name field, or
   - Device IP: Enter a partial or complete device IP in the Device IP field.

3. Click Query to submit your filter criteria. The results of your filter or search query display in the ACL Devices list.

4. Click Reset when you want to restore the full ACL Devices list.

**Synchronizing ACL devices**

ACL Management provides you with a facility for polling the IMC database for the most current information device configuration, including ACL definitions, ACL uses, and time ranges for devices in the ACL Devices list.

To synchronize the ACL Devices list with the most current status and ACL configuration information in the IMC database:

1. Navigate to ACL Devices:
   a. Click the Service tab from the tabular navigation system on the top.
   b. Click the ACL Management icon located under the Resource and Configuration Management section of the Service tab.
   c. Click the ACL Devices link located under ACL Management on the navigation tree on the left. The ACL Devices page appears and the deployment ACL Devices list displays in this page.

2. Click the checkboxes to the left of the devices you want to synchronize data for.

3. Click the Synchronize button located at the top of the ACL Devices list. The page display a message indicating that device configuration is being synchronized.

4. Click Refresh to refresh the page with current data.

**Customizing ACL configuration polling for devices**

ACL Management provides you with the ability to customize the polling interval for ACL configuration information for every device.

To configure the ACL configuration polling interval for one or more devices:
1. Navigate to **ACL Devices**:
   a. Click the **Service** tab from the tabular navigation system on the top.

   b. Click the **ACL Management** icon located under the **Resource and Configuration Management** section of the **Service** tab.

   c. Click the **ACL Devices** link located under **ACL Management** on the navigation tree on the left. The **ACL Devices** page appears and the deployment **ACL Devices** list displays in this page.

2. Click the checkboxes ☑️ to the left of the **Status** and **Device Name** fields for the devices for which you want to customize ACL configuration polling.

3. Click the **Poll Setting** button located at the top of the ACL Devices list. The **Poll Setting** dialog box appears.

4. Click the radio button ☑️ to the left of the poll option you want to implement for the selected devices:
   o Select **Poll Interval** if you want to poll the selected devices and you want to customize the polling interval.
     a. Enter the poll interval value in the **Poll Interval** field.
        A valid polling interval range is 2 – 168 hours.
     o Select **Disable Polling** if you do not want to poll the selected devices for their ACL configuration information.

5. Click **OK** to accept your ACL configuration polling configuration changes.
   The results of your configuration change displays in the **ACL Devices** list banner.

**ACL device configurations**

The **ACL Device** configuration page provides you with many features for managing ACL configurations for the selected device. At the top of this page, IMC provides you with access to summary details for the selected device.

In the lower half of this page, there are many options for managing ACL device configurations using the tabs provided:

- **ACL Definitions** tab: Add ACL definitions to the device or delete ACL definitions from it. In addition, you can export ACLs to a text file. By navigating to the **View ACL details** page for a single ACL, you can view ACL rule details for a single rule as well as save the selected ACL as an ACL resource or template in ACL Management, apply the ACL as a packet filter or VLAN packet filter to one or more interfaces on the device, and view applied ACL uses that already exist on the device.

- **ACL Uses** tab: View the ACL uses for packet filtering and VLAN packet filtering currently deployed on the device as well as add and remove these ACL uses.

- **Time Ranges** tab: View and delete time ranges that have been applied to ACLs.

- **Config History** tab: View the ACL configuration history for the selected device as well as view the configuration details for every entry in the configuration history. In addition, you can modify the description of a configuration history entry and baseline an entry.

- **Flow Template Definitions** tab: View, add, modify, and remove flow templates for devices.

- **Flow Template Applications** tab: View, add, and remove flow templates that have been applied.

You can view and manage the details for a single device’s ACL configuration from a single portal. From the **ACL Device** configuration page, you can view basic device information, synchronize and refresh ACL data.
This page also provides you with access to the tabs for managing ACLs and ACL uses, ACL time ranges and ACL configuration histories, flow template definitions, and flow template applications. From these tabs, you can add, delete, or export device ACLs, add and delete ACL packet filtering, delete time ranges, view and manage ACL configuration history for a single device, view, add, modify, and remove device flow templates, and view, add, and remove flow template applications.

**Viewing the ACL device configuration page**

To view the ACL Device Configuration page for managing the ACL configuration for a single device:

1. Navigate to **ACL Devices**:
   a. Click the **Service** tab from the tabular navigation system on the top.
   b. Click the **ACL Management** icon located under the **Resource and Configuration Management** section of the **Service** tab.
   c. Click the **ACL Devices** link located under **ACL Management** on the navigation tree on the left. The **ACL Devices** page appears and the deployment **ACL Devices** list displays in this page.

2. Click the icon in the **ACL Config** field for the device for which you want to view and manage the ACL configuration.
   The **ACL Device** configuration page appears.

The upper portion of this page provides basic device information including:

- **Name**: Contains the device label for the selected device.
- **Status**: Contains the most current status of the device. Status is determined by the highest severity or alarm level for the device, when the device has one or more current alarms that has not been cleared or recovered.
- **IP Address**: Contains the IP address for the selected device.
- **Mask**: Contains the IP address subnet mask for the selected device.
- **Poll Interval**: Contains the ACL configuration polling interval for the selected device as well as a **Modify** link for changing the ACL configuration polling interval.

3. To modify the polling interval for the selected device, click the **Modify** link.
   The **Poll Settings** dialog box appears.

4. Click the radio button to the left of the poll option you want to implement for the selected devices:
   - Select **Poll Interval** if you want to poll the selected devices and you want to customize the polling interval and enter the poll interval value in the **Poll Interval** field, or
     Valid polling interval range is 2-168 hours.
   - Select **Disable Polling** if you do not want to poll the selected devices for their ACL configuration information.

5. Click **OK** to accept modifications to the polling interval.
   **Last Poll Time**: Contains the date and time stamp for the last ACL configuration poll.

The lower portion of the ACL Device configuration page contains several tabs that provide you with a feature set for managing various aspects of a device’s ACL configuration. These tabs include:

- **ACL Definitions**: Add ACL definitions to the device or delete ACL definitions from it. For additional information, see "Managing device ACL definitions" (page 759).
- **ACL Uses**: View the ACL uses currently deployed on the device as well as add and remove ACL uses.
Managing device ACL definitions

From the ACL Definitions tab of the ACL Device configuration page, you can add ACL definitions to the device or delete ACL definitions from it and export an ACL to a text file. By navigating to the View ACL details page for a single ACL on the device, you can view ACL rule details for a single rule, save the selected ACL as an ACL resource or template in ACL Management, apply the ACL as a packet filter or VLAN packet filter to one or more interfaces on the device, and view applied ACL uses that already exist on the device.

Viewing the ACL definition list

To view the list of ACLs that do not currently exist on the selected device:

1. Navigate to ACL Devices:
   a. Click the Service tab from the tabular navigation system on the top.
   b. Click the ACL Management icon located under the Resource and Configuration Management section of the Service tab.
   c. Click the ACL Devices link located under ACL Management on the navigation tree on the left.
      The ACL Devices page appears and the deployment ACL Devices list displays in this page.

2. Click the icon in the ACL Config field for the device for which you want to view and manage the ACL configuration.
   The ACL Device configuration page appears.

3. Click the ACL Definitions tab.
   ACL information for ACLs on the selected device displays in a list below the ACL Definition tab. The contents of this list are described below.

ACL definitions list

- **ACL Identifier**: Contains the identifier for the ACL.
  The contents of this field serve as a link for navigating to the View ACL page for the associated ACL.
- **ACL Type**: Contains the ACL type for the associated ACL. There are five types of ACL in IMC: Interface, Basic, Advanced, Link, or User-Defined.
- **Match Order**: Contains the match order type for the associated ACL. The Match Order can either be Config or Auto.
- **ACL Description**: Contains a description for the associated ACL.
- **Operation**: Contains two icons that serve as links: the Add Use icon for adding packet filtering and VLAN packet filtering for one or more interfaces on the selected device; and an Applied ACLs icon for navigating to a view of all applied ACL uses for the associated ACL.

You can sort the ACL Definitions list by the ACL Identifier, ACL Type, Match Order, and ACL Description fields by clicking the column label to sort the list by the selected field. The column label is a toggle switch that allows you to toggle between the various sort options specific to each field.
You can filter the **ACL Definitions** list by **ACL Type** by selecting the ACL type you want to filter for from the **ACL Type** list located in the upper right corner of the ACL list. Options include **All**, **Interface**, **Basic**, **Advanced**, **Link**, and **User-Defined**. The default is **All**.

**To add an ACL to the selected device**
1. Navigate to **ACL Devices**.
   a. Click the **Service** tab from the tabular navigation system on the top.
   b. Click the **ACL Management** icon located under the **Resource and Configuration Management** section of the **Service** tab.
   c. Click the **ACL Devices** link located under **ACL Management** on the navigation tree on the left.
      The **ACL Devices** page appears and the deployment **ACL Devices** list displays in this page.
2. Click the icon in the **ACL Config** field for the device for which you want to view and manage the ACL configuration.
   The **ACL Device** configuration page appears.
3. Click the **ACL Definitions** tab.
   ACL information for ACLs on the selected device displays in a list below the **ACL Definition** tab.
4. Click **Add**.
5. The **Add** button navigates you to the **Deploy ACLs** wizard of ACL Management’s **ACL Deployment** feature for managing the deployment of ACLs to devices. For more information this feature, see "Deploying ACLs to devices" (page 787).

**Deleting ACLs**

**To delete one or more ACLs from the selected device:**
1. Navigate to **ACL Devices**:
   a. Click the **Service** tab from the tabular navigation system on the top.
   b. Click the **ACL Management** icon located under the **Resource and Configuration Management** section of the **Service** tab.
   c. Click the **ACL Devices** link located under **ACL Management** on the navigation tree on the left.
      The **ACL Devices** page appears and the deployment **ACL Devices** list displays in this page.
2. Click the icon in the **ACL Config** field for the device for which you want to view and manage the ACL configuration.
   The **ACL Device** configuration page appears.
3. Click the **ACL Definitions** tab.
   The **ACL Definitions** tab contents display along with a list of ACLs that currently exist on the device.
4. Click the checkbox to the left of the **ACL Identifier** for the ACLs you want to delete.
5. Click **Delete**.
6. When prompted, click **OK** to confirm the deletion of the selected ACLs.
   The **Add Task** page displays with the default task name displayed in the **Task Name** field.
7. To enter a task name for this deployment task, delete the contents of this field and enter a new task name.
   A valid length for a task name is 1-32 characters. Note that the task name cannot begin with a number [0-9].

8. Enter a brief description for this deployment task in the Description field.

9. Select how you want IMC to execute the task to every device from the Deployment Order section of the Add Task page by clicking the radio button to the left of each option:
   o Select Concurrent if you want ACL Management to execute the task to multiple devices simultaneously, or
   o Select Sequential if you want ACL Management to execute the task to one device at a time.

10. Select the strategy you want ACL Management to use should a problem arise in the execution of the task from the Error Handling list:
   o Select Abort the task if you want to stop the deployment to pending devices, but not affect devices to which deployments are in progress or to which deployments have successfully completed once an error in deployment arises, or
   o Select Abort the task and clear data deployed on the error device if you want to stop the deployment and clear all deployments on the device experiencing a problem once an error in deployment arises, or
   o Select Skip the error device and continue if you want to stop all deployments on the device experiencing a problem once an error in deployment arises, or
   o Select Clear data deployed on the error device and continue if you want to clear all deployments on the device experiencing a problem once an error in deployment arises.

11. Do one of the following regarding the device’s running configuration:
   o To save the device’s running configuration as the startup configuration prior to execution click the radio button to the left of Yes in the Save to Startup File field, or
   o Click the radio button to the left of No if you do not want to save the current configuration.

12. You can select when you want ACL Management to execute the task to the selected device from one of the following:
   o To execute the task immediately, click on the radio button to the left of Immediately, or
   o To schedule a time for ACL Management to execute the task, click on the radio button to the left of At Scheduled Time.

   a. Click on the calendar function to the right of the At Scheduled Time field to populate the date and time for the execution of this task.
      A popup calendar appears.
   b. Select the date from the calendar.

   Alternatively, you can enter the date and time manually. Valid date and time format for this entry is YYYY-MM-DD hh:mm where YYYY denotes the four digit year, MM denotes the two digit month, DD denotes the two digit day and hh denotes the two digit hour, mm denotes the two digit minute.

13. To preview the commands of the task, click on the icon in the Preview Commands field of the Deploy Details list.
    The Preview Commands dialog box displays and the commands of the task to be executed are listed.
    a. Review the contents to verify that these are the commands you want to execute.
    b. Click OK when you have finished previewing the commands.
14. Click **OK** to accept the deployment and task configuration and to submit this request to the deployment task queue.

   If the task is scheduled to run immediately, the **Task Result** dialog box appears, providing a real time status of the deployment task.

   o Click **Close** on the **Task Result** dialog box when the task has finished executing.

   o Review the results of the task in the **Result** field of the **Task List**.

   a. Click the **Refresh** button located at the top of the **Task List** to reload the page with the most current information for all tasks in the list.

   b. Review the results of your deployment task in the **Result** field of the deployment **Task List**.

      The contents of this field serve as a link to the **Task Result** page that contains more detailed information the result and causes for a failed deployment. From this page, you can also review the commands executed by the deployment task.

**Exporting an ACL**

To export the contents of an ACL on the selected device to a text file on your local computer:

1. Navigate to **ACL Devices**:

   a. Click the **Service** tab from the tabular navigation system on the top.

   b. Click the [ACL Management](#) icon located under the **Resource and Configuration Management** section of the **Service** tab.

   c. Click the [ACL Devices](#) link located under **ACL Management** on the navigation tree on the left.

   The **ACL Devices** page appears and the deployment **ACL Devices** list displayed in this page.

2. Click the icon in the **ACL Config** field for the device for which you want to view and manage the ACL configuration.

   The **ACL Device** configuration page appears.

3. Click the **ACL Definitions** tab.

   ACL information for ACLs on the selected device displays in a list below the **ACL Definition** tab.

4. Click the checkbox to the left of the **ACL Identifier** for the ACLs you want to export.

5. Click **Export**.

6. Follow your web browser’s instruction for opening or saving the contents of the ACL to a file on your local computer.

**Add use**

The **Add Use** option provides you with a shortcut for deploying packet filtering or VLAN packet filtering to one or more interfaces on the selected device.

1. Navigate to **ACL Devices**:

   a. Click the **Service** tab from the tabular navigation system on the top.

   b. Click the [ACL Management](#) icon located under the **Resource and Configuration Management** section of the **Service** tab.

   c. Click the [ACL Devices](#) link located under **ACL Management** on the navigation tree on the left.

   The **ACL Devices** page appears and the deployment **ACL Devices** list displays in this page.
2. Click the icon in the **ACL Config** field for the device for which you want to view and manage the ACL configuration.
   The **ACL Device** configuration page appears.

3. Click the **ACL Definitions** tab.
   ACL information for ACLs on the selected device displays in a list below the **ACL Definition** tab.

4. Click the **Add Use** icon in the **Operation** field to navigate to the **Add Use** feature found under the **ACL Uses** tab.
   For more information using this feature to add packet filtering or VLAN packet filtering to one or more interfaces for the selected device, see "Adding an ACL use" (page 767).

**Viewing applied ACLs**

To view a list of packet filtering and VLAN packet filtering uses for the selected device:

1. Navigate to **ACL Devices**:
   a. Click the **Service** tab from the tabular navigation system on the top.

   b. Click the **ACL Management** icon located under the **Resource and Configuration Management** section of the **Service** tab.

   c. Click the **ACL Devices** link located under **ACL Management** on the navigation tree on the left.
   The **ACL Devices** page appears and the deployment **ACL Devices** list display in this page.

2. Click the icon in the **ACL Config** field for the device for which you want to view and manage the ACL configuration.
   The **ACL Device** configuration page appears.

3. Click the **ACL Definitions** tab.
   ACL information for ACLs on the selected device displays in a list below the **ACL Definition** tab.

4. Click the **Applied ACLs** icon in the **Operation** field associated with the ACL you want to use to packet filtering or VLAN packet filtering for.
   The **Apply ACLs** page appears.

5. Click **Back** when you have finished viewing the application of ACL uses to the selected device.

**The view ACL page**

The **View ACL** page provides you with visibility into more detailed information for the selected ACL on the selected device. In addition, you can save the selected ACL as an ACL resource or ACL template in ACL Management, apply the selected ACL or configure ACL uses for packet filtering and VLAN packet filtering to selected interfaces on the selected device.

To view the **View ACL** page:

1. Navigate to **ACL Devices**:
   a. Click the **Service** tab from the tabular navigation system on the top.

   b. Click the **ACL Management** icon located under the **Resource and Configuration Management** section of the **Service** tab.

   c. Click the **ACL Devices** link located under **ACL Management** on the navigation tree on the left.
The ACL Devices page appears and the deployment ACL Devices list displays in this page.

2. Click the icon in the ACL Config field for the device for which you want to view and manage the ACL configuration.

The ACL Device configuration page appears.

3. Click the ACL Definitions tab.

ACL information for ACLs on the selected device displays in a list below the ACL Definition tab.

4. Click the link in the ACL Identifier field for the ACL you want to view.

The View ACL page appears.

   o The upper portion of this page provides basic ACL information including the ACL Identifier, Description, ACL Type, and Match Order configuration for the selected ACL.
   
   o The lower portion of the ACL View page contains a rule Information list that provides detailed information about the rules in the ACL based on the ACL type.

The sequence number in this list serves as a link for navigating to a dialog box for viewing rule information specific to the rule type.

ACL Management provides rule match count statistics in the Match Count field for the associated rule.

**Saving a device ACL as an ACL rule set**

Operators can save a device’s ACL as a rule set in an existing ACL. Once the ACL on the device has been saved as a rule set, it becomes available for deployment to other network devices. To save an ACL on a device as an ACL rule set in ACL Management:

1. Navigate to ACL Devices:
   
   a. Click the Service tab from the tabular navigation system on the top.
   
   b. Click the ACL Management icon located under the Resource and Configuration Management section of the Service tab.
   
   c. Click the ACL Devices link located under ACL Management on the navigation tree on the left. The ACL Devices page appears and the deployment ACL Devices list displays in this page.

2. Click the icon in the ACL Config field for the device for which you want to view and manage the ACL configuration.

The ACL Device configuration page appears.

3. Click the ACL Definitions tab.

ACL information for ACLs on the selected device displays in a list below the ACL Definition tab.

4. Click the link in the ACL Identifier field for the ACL you want to save as an ACL resource in ACL Management.

   The View ACL page appears.

5. Click Save as Resource.

   The Basic Info step of the Add Rule Set wizard appears.

6. Select the ACL in the ACL Management to which you want to add the device’s ACL as a rule set from the Add to ACL Resource list.

   When you save an ACL on a device as an ACL resource in ACL Management, you are saving it as a rule set in an existing ACL. Therefore, you must first create the ACL in ACL Management before you
can save a device’s ACL to it as a rule set. For more information creating an ACL in ACL Management, see "Adding an ACL use" (page 767).

7. Enter a name for the rule set in the **Rule Set Name** field.
A valid length for a rule set name is 1 – 32 characters.

8. Select the match order you want to apply to this ACL template by clicking the radio button to the left of the **Match Order** option you want to use:
   - If you select **Config**, IMC matches rules in the order in which they were configured but only for devices that support it, or
   - If you select **Auto**, IMC matches rules based on the principle of depth priority.

9. Enter a brief description for this ACL in the **ACL Description** field.
A valid length for this field is 0 - 127 characters.

10. Enter a brief description for this rule set in the **Rule Set Description** field.
A valid length for this field is 0 - 127 characters.

11. If you want to apply a time range to the rule set, click the checkbox to the left of **Configure ACL Rules with Time Range**.

12. Click **Next**.
The **Configure Time Range** step of the **Add Rule Set** wizard appears.

13. Do one of the following:
   - If you checked the box to **Configure ACL Rules with Time Range**, click **Add** under **Configure Time Range** to add a time range to this rule set, or
   - Skip to Step 14.

14. Click **Finish** to save the ACL rules from the selected device to the new rule set.

15. Choose from one of the following to modify, copy, sort, optimize, or delete existing rules:
   - To modify rules, click the **Modify** icon associated with the rule sequence you want to modify. For more information modifying a rule set, see "Modifying ACL rule sets" (page 718), or
   - To copy rules you have already created, click the **Copy** icon associated with the rule sequence you want to copy. For more information copying a rule in an ACL rule set, see "Copying a rule in an ACL rule set" (page 750), or
- Rules that belong to a rule set that is configured with a `Match Order` of `Config` are executed in the order in which they appear in the rule set. The order in which rules appear in a rule set is initially defined by the order in which they are created. You can, however, redefine the order in which the rules in a rule set are executed by using the `Sort` feature. For more information using Sort to redefine the order of appearance of rules in a rule set, see "Using sort to reorder the rules in an ACL rules set" (page 752), or

- ACLs can have a profound effect on the performance of networks. ACL Management automatically evaluates the effectiveness of rules and their effect on overall network performance as you add rules to a rule set. However, you can also manually perform an analysis of a rule set and optimize its effect on network performance using the `Optimize` feature. For more information using this feature, see "Optimizing the rules in a rule set" (page 752), or

- To delete one or more rules from a rule set, see "Deleting rules from an ACL rule set" (page 751).

**Saving a device ACL as a template**

Operators can save a device’s ACL as a template, making it available for importing an ACL resource for deployment to other network devices.

1. Navigate to **ACL Devices**:
   a. Click the **Service** tab from the tabular navigation system on the top.
   b. Click the **ACL Management** icon located under the **Resource and Configuration Management** section of the **Service** tab.
   c. Click the **ACL Devices** link located under **ACL Management** on the navigation tree on the left.

   The **ACL Devices** page appears and the deployment **ACL Devices** list displays in the lower half of this page.

2. Click the icon in the **ACL Config** field for the device for which you want to view and manage the ACL configuration.

   The **ACL Device** configuration page appears.

3. Click the **ACL Definitions** tab.

   ACL information for ACLs on the selected device displays in a list below the **ACL Definition** tab.

4. Click the link in the **ACL Identifier** field for the ACL you want to save as an ACL resource in ACL Management.

   The **View ACL** page appears.

5. Click **Save as Template**.

   The **Save as new template** dialog box appears.

6. Enter the name for the template in the **Save as new template** field.

   A valid length for a template name is 1 – 32 characters. Template names cannot begin with a number or a space.

7. Click **OK** to create the new template using the name provided.

8. Once you have created the template you can view information for it, modify it, copy it, delete it, or export it. For more information managing templates in ACL Management, see "Managing ACL templates in IMC" (page 658).
Apply an ACL

From the View ACL page, you can add packet filtering or VLAN packet filtering to one or more interfaces on the selected device using the rules defined in the ACL for which you are viewing information. To add these ACL uses, the target device must support them. For more information applying the ACL uses of packet filtering and VLAN packet filtering to the selected device, see "Adding an ACL use" (page 767).

Viewing applied ACLs

From the View ACL page, you can view the configured packet filtering or VLAN packet filtering for the selected device and ACL for which you are viewing information. For more information applying the ACL uses of packet filtering and VLAN packet filtering to the selected device, see "Viewing applied ACLs" (page 763).

Managing device ACL uses for packet filtering and VLAN packet filtering

From the ACL Uses tab of the ACL Device configuration page, you can view the ACL uses for packet filtering and VLAN packet filtering currently deployed on the device or add and remove these ACL uses.

Viewing the ACL use list

To view the list of ACL Uses for packet filtering and VLAN packet filtering for the selected ACL on the selected device:

1. Navigate to ACL Devices:
   a. Click the Service tab from the tabular navigation system on the top.
   b. Click the ACL Management icon located under the Resource and Configuration Management section of the Service tab.
   c. Click the ACL Devices link located under ACL Management on the navigation tree on the left. The ACL Devices page appears and the deployment ACL Devices list displays in this page.

2. Click the icon in the ACL Config field for the device for which you want to view and manage the ACL configuration.
   The ACL Device configuration page appears.

3. Click the ACL Uses tab.
   ACL use information for packet filtering and VLAN packet filtering displays in a list below the ACL Uses tab. The contents of this list are described below.

ACL uses list

- **Use Type**: Identifies what type of ACL Use is being used, Packet Filtering or VLAN Packet Filtering.
- **View**: Identifies the view of the ACL that was used.
- **ACL Name**: Identifies the ACL that contains the filtering command in use.
- **Command**: Displays the command used to apply the filtering.

You can filter the ACL Uses list by **Use Type** by selecting the use type you want to filter for from the **Use Type** list located in the upper right corner of the ACL Uses list. Options include All, Packet Filter and VLAN Packet Filter. The default is All.

Adding an ACL use

To add an ACL use for packet filtering and VLAN packet filtering to one or more interfaces on the selected device:

1. Navigate to ACL Devices:
a. Click the **Service** tab from the tabular navigation system on the top.

b. Click the **ACL Management** icon located under the **Resource and Configuration Management** section of the **Service** tab.

c. Click the **ACL Devices** link located under **ACL Management** on the navigation tree on the left. The **ACL Devices** page appears and the deployment **ACL Devices** list displays in this page.

2. Click the icon in the **ACL Config** field for the device for which you want to view and manage the ACL configuration.

The **ACL Device** configuration page appears.

3. Click the **ACL Uses** tab.

4. Click **Add**.

The **Select Use Type** step of the **Add Use** deployment wizard appears.

5. Select the use type you want to deploy from the list provided.

The options displayed are defined by the supported options on the selected device.

6. Click **Next**.

The **Select Object** step of the **Add Use** deployment wizard appears.

7. Select the direction that you want the filter to be applied from the **Filter Direction** list.

8. Select the interfaces or VLAN interfaces you want to apply the filtering to.

9. Select the interfaces that you want to apply the filter to from the **Interface List** column on the left:

   - To select an interface, click the interface to highlight it and then click the right arrow key to select it, or
   - To select all interfaces, click the double right arrow key, or
   - To deselect an interface, click on the interface in the **Selected Interfaces** column to select it and then click the left arrow key to deselect it, or
   - To deselect all interfaces, click on the double left arrow key.

10. Select the VLAN that you want to apply the filter to from the **VLAN List** column on the left:

    - To select a VLAN, click the VLAN to highlight it and click the right arrow key to select it, or
    - To select all interfaces, click the double right arrow key, or
    - To deselect a VLAN, click on the VLAN in the **Selected VLANs** column to highlight it and click the left arrow key to deselect it, or
    - To deselect all VLANs, click on the double left arrow key.

11. Repeat this step for every device you have selected for ACL use deployment.

12. Click **Next** when you have finalized your selection of interfaces for all devices to which you applied filtering.

    The **Select ACL** step of the **Add Use** deployment wizard appears.

13. Select the **ACL** you want to deploy for this use from the list provided.
The **Summary** step of the **Add Use** wizard appears.

14. Review the information provided in the **Summary** page to ensure that you have configured the wizard according to your needs.

15. Click **Finish** when you have finished reviewing the configuration details and are ready to submit the task to the ACL deployment task queue.

The **Add Task** page appears.

16. To enter a task name for this deployment task, delete the contents of this field and enter a new task name.

   A valid length for a task name is 1 – 32 characters. The task name cannot begin with a number [0-9].

17. Enter a brief description for this deployment task in the **Description** field.

18. Select how you want IMC to execute the task to every device from the **Deployment Order** section of the **Add Task** page by clicking the radio button  to the left of each option.

   o Select **Concurrent** if you want ACL Management to execute the task to multiple devices simultaneously, or

   o Select **Sequential** if you want ACL Management to execute the task to one device at a time.

19. Select the strategy you want ACL Management to use should a problem arise in the execution of the task from the **Error Handling** list:

   o Select **Abort the task** if you want to stop the deployment to pending devices, but not affect devices to which deployments are in progress or to which deployments have successfully completed once an error in deployment arises, or

   o Select **Abort the task and clear data deployed on the error device** if you want to stop the deployment and clear all deployments on the device experiencing a problem once an error in deployment arises, or

   o Select **Skip the error device and continue** if you want to stop all deployments on the device experiencing a problem once an error in deployment arises, or

   o **Clear data deployed on the error device and continue** if you want to clear all deployments on the device experiencing a problem once an error in deployment arises.

20. To choose to save or not save the device’s running configuration as the startup configuration prior to execution:

   o Click the radio button  to the left of **Yes** in the **Save to Startup File** field, or

   o Click the radio button  to the left of **No** if you do not want to save the current configuration.

21. You can select when you want ACL Management to execute the task to the selected device by selecting one of the following:

   o To execute the task immediately, click the radio button  to the left of **Immediately**, or

   o To schedule a time for ACL Management to execute the task, click the radio button  to the left of **At Scheduled Time**.

      If you selected **At Scheduled Time**:

      a. Click the calendar function  to the right of the **At Scheduled Time** field to populate the date and time for the execution of this task.

      A popup calendar appears.

      b. Select the date from the calendar.
Alternatively, you can enter the date and time manually. Valid date and time format for this entry is YYYY-MM-DD hh:mm where YYYY denotes the four digit year, MM denotes the two digit month, DD denotes the two digit day and hh denotes the two digit hour, and mm denotes the two digit minute.

22. To preview the commands of the task, click the icon in the Preview Commands field of the Deploy Details list.

The Preview Commands dialog box displays and the commands of the task to be executed appears.

23. Review the contents to verify that these are the commands you want to execute.

24. Click OK when you have finished previewing the commands.

25. Click OK to accept the deployment and task configuration and to submit this request to the deployment task queue.

If the task is scheduled to run immediately, the Task Result dialog box appears, providing you with a real time status of the deployment task.

26. Click Close on the Task Result dialog box when the task has finished executing.

27. Click the Refresh button located at the top of the Task List to reload the page with the most current information for all tasks in the list and review the results of the task in the Result field.

28. Review the results of your deployment task in the Result field of the deployment Task List.

The contents of this field serve as a link to the Task Result page that contains more detailed information the result and causes for a failed deployment. From this page, you can also review the commands executed by the deployment task.

Deleting an ACL use

To delete an ACL packet filtering or VLAN packet filtering use from one or more interfaces on the selected device:

1. Navigate to ACL Devices:
   a. Click the Service tab from the tabular navigation system on the top.
   b. Click the ACL Management icon located under the Resource and Configuration Management section of the Service tab.
   c. Click the ACL Devices link located under ACL Management on the navigation tree on the left. The ACL Devices page appears and the deployment ACL Devices list displays in this page.

2. Click the icon in the ACL Config field for the device for which you want to view and manage the ACL configuration.

The ACL Device configuration page appears.

3. Click the ACL Uses tab.

4. Click the checkbox to the left of the Use Types for the ACL uses you want to delete.

5. Click Delete.

6. When prompted, click OK to confirm the deletion of the selected ACL uses.

The Add Task page appears.

7. To enter a task name for this deployment task, delete the contents of this field and enter a new task name.

A valid length for a task name is 1 – 32 characters. The task name cannot begin with a number [0-9].

8. Enter a brief description for this deployment task in the Description field.
9. Select how you want IMC to execute the task to every device from the Deployment Order section of the Add Task page by clicking the radio button ○ to the left of each option:
   o Select Concurrent if you want ACL Management to execute the task to multiple devices simultaneously, or
   o Select Sequential if you want ACL Management to execute the task to one device at a time.

10. Select the strategy you want ACL Management to use should a problem arise in the execution of the task from the Error Handling list:
   o Select Abort the task if you want to stop the deployment to pending devices, but not affect devices to which deployments are in progress or to which deployments have successfully completed once an error in deployment arises, or
   o Select Abort the task and clear data deployed on the error device if you want to stop the deployment and clear all deployments on the device experiencing a problem once an error in deployment arises, or
   o Select Skip the error device and continue if you want to stop all deployments on the device experiencing a problem once an error in deployment arises, or
   o Select Clear data deployed on the error device and continue if you want to clear all deployments on the device experiencing a problem once an error in deployment arises.

11. To choose to save or not save the device’s running configuration as the startup configuration prior to execution:
   o Click the radio button ○ to the left of Yes in the Save to Startup File field, or
   o Click the radio button ○ to the left of No if you do not want to save the current configuration.

12. You can select when you want ACL Management to execute the task to the selected device:
   o To execute the task immediately, click the radio button ○ to the left of Immediately, or
   o To schedule a time for ACL Management to execute the task, click the radio button ○ to the left of At Scheduled Time.
      If you selected At Scheduled Time:
      a. Click the calendar function  to the right of the At Scheduled Time field to populate the date and time for the execution of this task.
         A popup calendar appears.
      b. Select the date from the calendar.
      Alternatively, you can enter the date and time manually. Valid date and time format for this entry is YYYY-MM-DD hh:mm where YYYY denotes the four digit year, MM denotes the two digit month, DD denotes the two digit day and hh denotes the two digit hour, and mm denotes the two digit minute.

13. To preview the commands of the task, click the icon ⌍ in the Preview Commands field of the Deploy Details list.
      The Preview Commands dialog box appears and the commands of the task to be executed are shown.

14. Review the contents to verify that these are the commands you want to execute.

15. Click OK when you have finished previewing the commands.

16. Click OK to accept the deployment and task configuration and to submit this request to the deployment task queue.
    If the task is scheduled to run immediately, the Task Result dialog box appears. This dialog box provides you with a real time status of the deployment task.
17. Click **Close** on the **Task Result** dialog box when the task has finished executing.

18. Click the **Refresh** button located at the top of the **Task List** to reload the page with the most current information for all tasks in the list and the results of the task in the **Result** field.

19. Review the results of your deployment task in the **Result** field of the deployment **Task List**.

The contents of this field serve as a link to the **Task Result** page that contains more detailed information the result and causes for a failed deployment. From this page, you can also review the commands executed by the deployment task.

**Managing device ACL time ranges**

You can view and delete time ranges that have been applied to ACLs on the selected device from the **Time Ranges** tab of the **ACL Device** configuration page.

**Viewing the time range list**

To view the list of time ranges in use by the selected device:

1. Navigate to **ACL Devices**:
   a. Click the **Service** tab from the tabular navigation system on the top.
   b. Click the **ACL Management** icon located under the **Resource and Configuration Management** section of the **Service** tab.
   c. Click the **ACL Devices** link located under **ACL Management** on the navigation tree on the left.

The **ACL Devices** page appears and the deployment **ACL Devices** list is displayed in this page.

2. Click the icon in the **ACL Config** field for the device for which you want to view and manage the ACL configuration.

The **ACL Device** configuration page appears.

3. Click the **Time Ranges** tab.

ACL time ranges display in a list below the **Time Ranges** tab.

**Time range list**

- **Name**: This field identifies the name of each time range in use by the selected device. The contents of this field serve as a link for navigating to the **View Time Range** page. The **View Time Range** page provides you with more detailed information for the selected time range including the start and end dates and times for the time range if the time range type is **Fixed**. If the time range is **Cyclical**, the **Execution Period** field contains the days of the week that the time range applies to.

4. Click **8, 15, 50, 100, or 200** from the right side of the Time Range list to configure how many items per page you want to view.

**Deleting time ranges**

To delete one or more time ranges from the selected device:

1. Navigate to **ACL Devices**:
   a. Click the **Service** tab from the tabular navigation system on the top.
   b. Click the **ACL Management** icon located under the **Resource and Configuration Management** section of the **Service** tab.
   c. Click the **ACL Devices** link located under **ACL Management** on the navigation tree on the left.
The ACL Devices page appears and the deployment ACL Devices list display in the lower half of this page.

2. Click the icon in the ACL Config field for the device for which you want to view and manage the ACL configuration.
   The ACL Device configuration page appears.
3. Click the Time Ranges tab.
   ACL time ranges displays in a list below the Time Ranges tab.
4. Click the checkbox to the left of the time range Names for every time range you want to delete.
5. Click Delete.
6. When prompted, click OK to confirm the deletion of the selected time ranges.
   The Add Task page displays with the default task name in the Task Name field.
7. To enter a task name for this deployment task, delete the contents of this field and enter a new task name.
   A valid length for a task name is 1-32 characters. Note that the task name cannot begin with a number [0-9].
8. Enter a brief description for this deployment task in the Description field.
9. Select how you want IMC to execute the task to every device from the Deployment Order section of the Add Task page by clicking the radio button to the left of each option:
   o Select Concurrent if you want ACL Management to execute the task to multiple devices simultaneously, or
   o Select Sequential if you want ACL Management to execute the task to one device at a time.
10. Select the strategy you want ACL Management to use should a problem arise in the execution of the task from the Error Handling list. Options include:
    o Select Abort the task if you want to stop the deployment to pending devices, but not affect devices to which deployments are in progress or to which deployments have successfully completed once an error in deployment arises, or
    o Select Abort the task and clear data deployed on the error device if you want to stop the deployment and clear all deployments on the device experiencing a problem once an error in deployment arises, or
    o Select Skip the error device and continue if you want to stop all deployments on the device experiencing a problem once an error in deployment arises, or
    o Select Clear data deployed on the error device and continue if you want to clear all deployments on the device experiencing a problem once an error in deployment arises.
11. To save the device’s running configuration as the startup configuration prior to execution:
    o Click the radio button to the left of Yes in the Save to Startup File field, or
    o Click the radio button to the left of No if you do not want to save the current configuration.
12. Select when you want ACL Management to execute the task to the selected device:
    o To execute the task immediately, click the radio button to the left of Immediately, or
    o To schedule a time for ACL Management to execute the task, click the radio button to the left of At Scheduled Time.
      If you selected At Scheduled Time:
a. Click on the calendar function  to the right of the At Scheduled Time field to populate the date and time for the execution of this task. A popup calendar appears.

b. Select the date from the calendar.

c. Alternatively, you can enter the date and time manually.

Valid date and time format for this entry is YYYY-MM-DD hh:mm where YYYY denotes the four digit year, MM denotes the two digit month, DD denotes the two digit day and hh denotes the two digit hour, and mm denotes the two digit minute.

13. To preview the commands of the task, click the icon  in the Preview Commands field of the Deploy Details list. The Preview Commands dialog box displays and the commands of the task to be executed appear.

14. Review the contents to verify that these are the commands you want to execute.

15. Click OK when you have finished previewing the commands.

16. Click OK to accept the deployment and task configuration and to submit this request to the deployment task queue.

If the task is scheduled to run immediately, the Task Result dialog box appears, providing you with a real time status of the deployment task.

17. Click Close on the Task Result dialog box when the task has finished executing.

18. Click the Refresh button located at the top of the Task List to reload the page with the most current information for all tasks in the list to review the results of the task in the Result field.

19. Review the results of your deployment task in the Result field of the deployment Task List.

The contents of this field serve as a link to the Task Result page that contains more detailed information the result and causes for a failed deployment. From this page, you can also review the commands executed by the deployment task.

Managing device configuration history

From the Config History tab of the ACL Device configuration page, you can view the ACL configuration history for the selected device and the configuration details for every entry in the ACL configuration history. You can also modify a configuration history entry and baseline an entry.

Viewing the ACL configuration history

To view the ACL configuration history for the selected device:

1. Navigate to ACL Devices:
   a. Click the Service tab from the tabular navigation system on the top.
   b. Click the ACL Management icon located under the Resource and Configuration Management section of the Service tab.
   c. Click the ACL Devices link located under ACL Management on the navigation tree on the left.

   The ACL Devices page appears and the deployment ACL Devices list display in this page.

2. Click the icon  in the ACL Config field for the device for which you want to view and manage the ACL configuration.

   The ACL Device configuration page appears.

3. Click the Config History tab.
The ACL configuration history displays in a list below the Config History tab.

**ACL configuration history list**

- **Version**: Contains the type of ACL configuration history list entry, a common ACL configuration history entry or a baseline entry.
- **Update Date**: Contains the date and time when this entry was executed. The contents of this field serve as a link for navigating to the View Config History page for viewing details for the individual entry. For more information this feature, see “Viewing an ACL configuration history entry” (page 775).
- **Description**: Contains a description for the ACL configuration entry.
- **Baseline**: Contains an icon for setting the associated ACL configuration history event as a baseline configuration.
- **Modify**: Contains an icon for modifying the description of the associated ACL configuration history entry.

If the list contains multiple entries, the following navigational aids may appear:

- Click ☞ to page forward in the ACL Configuration History list.
- Click ☞ to page forward to the end of the ACL Configuration History list.
- Click ☞ to page backward in the ACL Configuration History list.
- Click ☞ to page backward to the front of the ACL Configuration History list.

4. Click 8, 15, 50, 100, or 200 from the right side of the main pane to configure how many items per page you want to view.

You can sort the ACL Configuration History list by the Version, Update Date, and Description fields by clicking the column label to sort the list by the selected field. The column label is a toggle switch that allows you to toggle between the various sort options specific to each field.

**Viewing an ACL configuration history entry**

To view the details for an entry in the ACL configuration history list for the selected device:

1. Navigate to **ACL Devices**:
   a. Click the Service tab from the tabular navigation system on the top.
   b. Click the ACL Management icon located under the Resource and Configuration Management section of the Service tab.
   c. Click the ACL Devices link located under ACL Management on the navigation tree on the left.
      The ACL Devices page display and the deployment ACL Devices list is shown in this page.
   
2. Click the icon ☞ in the ACL Config field for the device for which you want to view and manage the ACL configuration.
   The ACL Device configuration page appears.

3. Click the Config History tab.
   The ACL configuration history displays in a list below the Config History tab.

4. Click the link in the Update Date field of the Config History list associated with the entry you want to view.
The View Config History page appears. The upper portion of the page contains basic information on the configuration history entry and details on the ACL configuration file that was changed on the associated device.

Modifying a configuration history entry
To modify an entry in the ACL configuration history list for the selected device:
1. Navigate to ACL Devices:
   a. Click the Service tab from the tabular navigation system on the top.
   b. Click the ACL Management icon located under the Resource and Configuration Management section of the Service tab.
   c. Click the ACL Devices link located under ACL Management on the navigation tree on the left. The ACL Devices page appears and the deployment ACL Devices list displays in this page.
2. Click the icon in the ACL Config field for the device for which you want to view and manage the ACL configuration.
   The ACL Device configuration page appears.
3. Click the Config History tab.
   The ACL configuration history displays in a list below the Config History tab.
4. Click the icon in the Modify field associated with the ACL configuration history event you want to modify.
   The Modify Config History dialog box appears.
5. Enter a new description for the entry in the Description field provided.
6. Click OK to accept your modifications to the ACL configuration history entry.

Deleting configuration history entries
To delete one or more entries from the ACL configuration history list for the selected device:
1. Navigate to ACL Devices:
   a. Click the Service tab from the tabular navigation system on the top.
   b. Click the ACL Management icon located under the Resource and Configuration Management section of the Service tab.
   c. Click the ACL Devices link located under ACL Management on the navigation tree on the left. The ACL Devices page appears and the deployment ACL Devices list displays in this page.
2. Click the icon in the ACL Config field for the device for which you want to view and manage the ACL configuration.
   The ACL Device configuration page appears.
3. Click the Config History tab.
   The ACL configuration history displays in a list below the Config History tab.
4. Click the checkboxes to the left of the Version and Update Date fields of the entries you want to delete.
5. Click Delete.
6. When prompted, click OK to confirm the deletion of the selected ACL configuration history entries.
Baselining a configuration history entry

Defining an ACL configuration history entry as a baseline enables you mark a particular device configuration performed at a certain point in time.

To establish an ACL configuration baseline for the selected device:

1. Navigate to **ACL Devices**:
   a. Click the **Service** tab from the tabular navigation system on the top.
   b. Click the **ACL Management** icon located under the **Resource and Configuration Management** section of the **Service** tab.
   c. Click the **ACL Devices** link located under **ACL Management** on the navigation tree on the left.
      The **ACL Devices** page appears and the deployment **ACL Devices** list displays in this page.

2. Click the icon in the **ACL Config** field for the device for which you want to view and manage the ACL configuration.
   The **ACL Device** configuration page appears.

3. Click the **Config History** tab.
   The ACL configuration history displays in a list below the **Config History** tab.

4. Click the icon in the **Baseline** field for the configuration history entry for which you want to establish as a baseline.

5. Confirm that the entry has been configured as the baseline entry by reviewing the contents of the **Version** field for the entry you designated as the baseline entry.
   Only one entry can serve as a baseline entry.

Managing device flow templates

From the **Flow Template Definitions** tab of the **ACL Device** configuration page, you can view, add, modify, and remove device flow templates.

Viewing the flow template

To view the flow templates for the selected device:

1. Navigate to **ACL Devices**:
   a. Click the **Service** tab from the tabular navigation system on the top.
   b. Click the **ACL Management** icon located under the **Resource and Configuration Management** section of the **Service** tab.
   c. Click the **ACL Devices** link located under **ACL Management** on the navigation tree on the left.
      The **ACL Devices** page appears and the deployment **ACL Devices** list displays in this page.

2. Click the icon in the **ACL Config** field for the device for which you want to view and manage the ACL configuration.
   The **ACL Device** configuration page appears.

3. Click the **Flow Template Definitions** tab.
   The flow templates that already exist on the device display in a list below the **Flow Template Definitions** tab.

Flow template definitions

- **Name**: Contains the name assigned to this flow template.
viewing flow template details

to view the details for an entry in the flow template list for the selected device:

1. navigate to acl devices:
   a. click the service tab from the tabular navigation system on the top.
   b. click the acl management icon located under the resource and configuration management section of the service tab.
   c. click the acl devices link located under acl management on the navigation tree on the left. the acl devices page appears and the deployment acl devices list displays in this page.

2. click the icon in the acl config field for the device for which you want to view and manage the acl configuration. the acl device configuration page appears.

3. click the flow template definitions tab.
   the flow templates that already exist on the device display in a list below the flow template definitions tab.

4. click the icon in the details field of the flow template definitions list associated with the entry you want to view.

   the view template definition page appears.

view template

   o name: contains the name assigned to this flow template.
   o type: identifies the type of flow template. the type can only be basic.
   o parameter name: contains the parameters defined for the flow template.

5. click back when you have finished viewing the flow template to the selected device.

adding flow template definition

to add a flow template to the selected device:

1. navigate to acl devices:
   a. click the service tab from the tabular navigation system on the top.
   b. click the acl management icon located under the resource and configuration management section of the service tab.
   c. click the acl devices link located under acl management on the navigation tree on the left.
The **ACL Devices** page appears and the deployment **ACL Devices** list displays in this page.

2. Click the icon in the **ACL Config** field for the device for which you want to view and manage the ACL configuration.
   The **ACL Device** configuration page appears.

3. Click the **Flow Template Definitions** tab.
   The flow templates that already exist on the device display in a list below the **Flow Template Definitions** tab.

4. Click **Add**.
   The **Add Flow Template Definitions** page appears.

5. Enter a name in **Template Name** field.
   A valid length for a task name is 1-32 characters. The template name cannot begin with a number [0-9] or contain any spaces or question marks.
   The template type, **Basic**, is selected by default.

6. Click the checkboxes ☑ to the left of the parameters that you want to add to the flow template in **Set Parameters** section:
   - **Address Type**: Allows you set the address type.
   - **Precedence Type**: Allows you to set the type of precedence.
   - **Protocol Type**: Allows you to set the protocol type.

7. Click **OK**.

**Modifying flow template definitions**

To modify a flow template to the selected device:

1. Navigate to **ACL Devices**:
   a. Click the Service tab from the tabular navigation system on the top.
   b. Click the **ACL Management** icon located under the Resource and Configuration Management section of the Service tab.
   c. Click the **ACL Devices** link located under **ACL Management** on the navigation tree on the left.
   The **ACL Devices** page appears and the deployment **ACL Devices** list displays in this page.

2. Click the icon in the **ACL Config** field for the device for which you want to view and manage the ACL configuration.
   The **ACL Device** configuration page appears.

3. Click the **Flow Template Definitions** tab.
   The flow templates that already exist on the device display in a list below the **Flow Template Definitions** tab.

4. Click the icon ☑ in the Modify field of the **Flow Template Definitions** list associated with the entry you want to modify.
   The **Modify Flow Template Definition** page appears.

5. In **Set Parameters** section, click the checkbox ☑ to the left of the parameter that you want to add to the flow template or uncheck the boxes to the left of the parameters that you want to remove from the template:
- **Address Type**: Allows you set the address type.
- **Precedence Type**: Allows you to set the type of precedence.
- **Protocol Type**: Allows you to set the protocol type.

6. Click **OK**.

### Deleting flow template definition

To delete a flow template to the selected device:

1. Navigate to **ACL Devices**:
   a. Click the **Service** tab from the tabular navigation system on the top.
   b. Click the **ACL Management** icon located under the **Resource and Configuration Management** section of the **Service** tab.
   c. Click the **ACL Devices** link located under **ACL Management** on the navigation tree on the left. The **ACL Devices** page appears and the deployment **ACL Devices** list displays in this page.

2. Click the icon in the **ACL Config** field for the device for which you want to view and manage the ACL configuration.

   The **ACL Device** configuration page appears.

3. Click the **Flow Template Definitions** tab.

   The flow templates that already exist on the device display in a list below the **Flow Template Definitions** tab.

4. Click the checkbox to the left of the flow template **Names** for every flow template you want to delete.

5. Click **Delete**.

6. When prompted, click **OK** to confirm the deletion of the selected time ranges.

### Managing device flow template applications

From the **Flow Template Applications** tab of the **ACL Device** configuration page, you can view, add, and delete flow template applications.

### Viewing flow template application

To view the flow template applications for the selected device:

1. Navigate to **ACL Devices**:
   a. Click the **Service** tab from the tabular navigation system on the top.
   b. Click the **ACL Management** icon located under the **Resource and Configuration Management** section of the **Service** tab.
   c. Click the **ACL Devices** link located under **ACL Management** on the navigation tree on the left. The **ACL Devices** page appears and the deployment **ACL Devices** list displays in this page.

2. Click the icon in the **ACL Config** field for the device for which you want to view and manage the ACL configuration.

   The **ACL Device** configuration page appears.

3. Click the **Flow Template Applications** tab.
The flow templates that have been applied to the device display in a list below the Flow Template Applications tab.

Flow template

- **Interface Description**: Identifies the interface for the selected device.
- **Template Name**: Contains the name assigned to this flow template.
- **Template Type**: Identifies the type of flow template. The type can only be Basic.
- **Delete**: Contains an icon for deleting this flow template application from the interface.

You can sort the Flow Template Applications list by the Interface Description, Template Name, and Template Type fields by clicking the column label to sort the list by the selected field. The column label is a toggle switch that allows you to toggle between the various sort options specific to each field.

Adding flow template application

To add a flow template application to the selected device:

1. Navigate to ACL Devices:
   - a. Click the Service tab from the tabular navigation system on the top.
   - b. Click the ACL Management icon located under the Resource and Configuration Management section of the Service tab.
   - c. Click the ACL Devices link located under ACL Management on the navigation tree on the left. The ACL Devices page appears and the deployment ACL Devices list displays in this page.

2. Click the icon in the ACL Config field for the device for which you want to view and manage the ACL configuration.
   The ACL Device configuration page appears.

3. Click the Flow Template Applications tab.
   The flow templates that have been applied to the device display in a list below the Flow Template Applications tab.

4. Click Add.
   The Add Flow Template Application page appears.

5. Select a flow template from the Flow Template list.
   For more information about adding a flow template, see "Managing device flow templates" (page 777).

6. Select interfaces from Interface List.

7. Click OK.
   The page updates to Add Flow Template Application list.

Add flow template application

- **Device Name**: Identifies the device name and IP address.
- **Interface Desc**: Identifies the interface to which the flow template is applied.
- **Flow Template Name**: Identifies the name of the flow template that is applied to the interface.
- **Operate Result**: Contains the application result for the interface. If the application is successfully added, the icon appears. If the system fails to add the application, the icon appears. Clicking the icon brings up a message box listing the possible reasons for the failure.
Deleting flow template application

To delete a flow template application from the selected device:

1. Navigate to ACL Devices:
   a. Click the Service tab from the tabular navigation system on the top.
   b. Click the ACL Management icon located under the Resource and Configuration Management section of the Service tab.
   c. Click the ACL Devices link located under ACL Management on the navigation tree on the left. The ACL Devices page appears and the deployment ACL Devices list displays in this page.

2. Click the icon in the ACL Config field for the device for which you want to view and manage the ACL configuration. The ACL Device configuration page appears.

3. Click the Flow Template Applications tab. The flow templates that have been applied to the device display in a list below the Flow Template Applications tab.

4. Click the checkbox to the left of the Interface Description field for every flow template application you want to delete.

5. Click Delete.

6. When prompted, click OK to confirm the deletion of the flow template application.

Deploying ACLs using IMC’s ACL deployment wizard

ACL Management’s ACL Deployment wizard provides you with a step-by-step guide for successfully deploying ACLs by providing you with a facility for viewing all deployment tasks via the ACL Deployment Task List. In addition, there are step-by-step guides for deploying ACLs and ACL uses, for removing ACLs, ACL time ranges, and ACL uses. During the deployment task configuration process for each of these deployment types, IMC evaluates the selected devices and ACLs to determine whether or not the task can be executed successfully, identifies when devices do not match the configuration selections, and displays warning messages and evaluation results to guide the successful deployment of ACL resources. In addition, ACL Management removes devices from the deployment configuration for which the selected action cannot be successfully executed.

The ACL Deployment wizard also gives you the choice to run deployment tasks immediately or to schedule them for a later date, to execute tasks to one or more devices sequentially or in concurrent, and how to handle errors when they arise.

Managing the deployment task list

ACL Management displays all deployment tasks, including tasks that have already been executed and those waiting for execution, in the deployment Task List. This list provides you with a single portal for managing ACL deployment tasks, including navigating to views that display task details and task results, links to modifying a task and the ability to start and stop deployment tasks.

Viewing the deployment task list

To view all deployment tasks in the Task list:

1. Navigate to ACL Resource:
a. Click the **Service** tab from the tabular navigation system on the top.

b. Click the **ACL Management** icon located under the **Resource and Configuration Management** section of the **Service** tab.

c. Click the **ACL Deployment** link located under **ACL Management** on the navigation tree on the left.

The **ACL Deployment** page appears and the deployment **Task List** displays in the lower half of this page.

**Deployment task**

- **Status**: Contains the current status of the deployment task. Possible values include *Waiting*, *Running*, *Completed*, *Paused*, and *Stopping*.

- **Task Name**: Contains the name of the deployment task.

The contents of this field serve as a link to the **View Task** page which provides details for the associated deployment task including basic task information, the deployment strategy and the devices configured in the deployment task. For more information, see “Viewing deployment task detailed information” (page 784).

You can configure the task name when using the **ACL Deployment** wizard to deploy an ACL. Otherwise, IMC provides a default task name that includes a date and time stamp for uniquely identifying deployment tasks.

- **Creation Time**: Identified the date and time stamp for the creation of the associated ACL deployment task.

- **Creator**: Contains the userid of the operator who submitted the task to the deployment **Task List**.

- **Task Type**: Identifies whether or not the deployment task was configured to run immediately or was scheduled for a specific or fixed date and time.

- **Expected Time**: Contains the date and time stamp of the start time of the associated deployment task’s execution.

- **End Time**: Contains the date and time stamp of the end time of the associated deployment task’s completion. This field contains a "-" if the associated task has not been executed.

- **Result**: Contains a summary of the result of the deployment task. The contents of this field serve as a link for navigating to the **Task Result** page. This report provides you with a summary of the task result, cause for failure if the execution of the deployment task failed, and the command that was executed.

- **Modify**: Contains an icon for modifying the configuration parameters of the ACL deployment task. For more information modifying an ACL deployment task, see "Modifying an ACL deployment task" (page 784).

You can sort the deployment **Task List** by the **Status**, **Task Name**, **Creation Time**, **Creator**, **Task Type**, **Expected Time**, and **End Time** fields by clicking the column label to sort the list by the selected field. The column label is a toggle switch that allows you to toggle between the various sort options specific to each field.

If the deployment **Task List** contains multiple entries, the following navigational aids may appear.

- Click **Next** to page forward in the deployment **Task List**.

- Click **End** to page forward to the end of the deployment **Task List**.

- Click **Previous** to page backward in the deployment **Task List**.

- Click **First** to page backward to the front of the deployment **Task List**.
2. Click 8, 15, 50, 100, or 200 from the right side of the main pane to configure how many items per page you want to view.

3. To filter the deployment Task List by task status, select the task status you want to filter for from the Task Status list located in the upper right corner of the Task List.

Viewing deployment task detailed information

To view the details of a deployment task:

1. Navigate to ACL Resource:
   a. Click the Service tab from the tabular navigation system on the top.
   b. Click the \textit{ACL Management} icon located under the Resource and Configuration Management section of the Service tab.
   c. Click the \textit{ACL Deployment} link located under ACL Management on the navigation tree on the left.
      The ACL Deployment page appears and the deployment Task List displays in the lower half of this page.

2. Click the link in the Task Name field associated with the ACL deployment task you want to view details for.
   The View Task page appears.

The basic information of detailed information

- **Task Name**: Contains the name of the deployment task. Operators can configure the task name when using the ACL Deployment wizard to deploy an ACL. Otherwise, IMC provides a default task name that includes a date and time stamp for uniquely identifying deployment tasks.
- **Description**: Contains the description that the creator of this ACL deployment task added.
- **Deployment Order**: Contains the deployment order selected by the creator of this task.
- **Error Handling**: Contains the manner in which ACL Management handles errors in the deployment of the selected ACL and rule set based on the creator’s configuration for error handling.
- **Save to Startup File**: Identifies whether or not ACL Management saves the running config to the startup config on the device after the deployment has been completed.
- **Execute**: Contains the date and time stamp for the execution of this task.

The deploy details of detailed information

- **Device**: Contains the device label for the devices to which the ACL rule set was deployed. This field serves as a link for navigating to the ACL Devices device information page. For more information on this, see “Managing device ACL definitions” (page 759).
- **Category**: Identifies the type of ACL deployment task.
- **Name**: Contains the name of the ACL that was configured for deployment.
- **Operation**: Contains the type of operation configured for execution within the category specified.
- **Preview Commands**: Contains an icon \textcolor{blue}{\texttt{}}for navigating to the dialog box that displays the commands to be executed. If the task has completed, this field is not displayed.

Modifying an ACL deployment task

You can modify any task in the Task List that has not completed or that has paused.

To modify a deployment task:

1. Navigate to ACL Resource:
a. Click the **Service** tab from the tabular navigation system on the top.

b. Click the **ACL Management** icon located under the **Resource and Configuration Management** section of the **Service** tab.

c. Click the **ACL Deployment** link located under **ACL Management** on the navigation tree on the left.

The **ACL Deployment** page appears and the deployment **Task List** displays in the lower half of this page.

2. Click the icon  in the **Modify** field of the deployment task you want to modify.

The **Modify Task** page appears with the default task name displayed in the **Task Name** field.

3. To enter a task name for this deployment task, delete the contents of this field and enter a new task name.

A valid length for a task name is 1 – 32 characters. The task name cannot begin with a number [0-9].

4. Enter a brief description for this deployment task in the **Description** field.

5. Select how you want IMC to execute the deployment of ACLs to every device in the deployment task from the **Deployment Order** section of the **Modify Task** page by clicking the radio button  to the left the appropriate option:

   o Select **Concurrent** if you want ACL Management to deploy the ACL to multiple devices simultaneously, or

   o Select **Sequential** if you want ACL Management to deploy the ACL to one device at a time.

6. Select the strategy you want ACL Management to use should a problem arise in the deployment of ACLs to devices from the **Error Handling** list. Options include:

   o Select **Abort the task** if you want to stop the deployment to pending devices, but not affect devices to which deployments are in progress or to which deployments have successfully completed once an error in deployment arises, or

   o Select **Abort the task and clear data deployed on the error device** if you want to stop the deployment and clear all deployments on the device experiencing a problem once an error in deployment arises, or

   o Select **Skip the error device and continue** if you want to stop all deployments on the device experiencing a problem once an error in deployment arises, or

   o Select **Clear data deployed on the error device and continue** if you want to clear all deployments on the device experiencing a problem once an error in deployment arises.

7. You can choose to save the device’s running configuration as the startup configuration prior to execution:

   o Click the radio button  to the left of **Yes** in the **Save to Startup File** field, or

   o Click the radio button  to the left of **No** if you do not want to save the current configuration.

8. Select when you want ACL Management to deploy the selected ACL and rule list to the selected devices:

   o To deploy the ACL and rule set immediately, click the radio button  to the left of **Immediately**, or

   o To schedule a time for ACL Management to deploy the ACL and rule set, click the radio button  to the left of **At Scheduled Time**.

   If you selected **At Scheduled Time**:

   a. Click on the calendar function  to the right of the **At Scheduled Time** field to populate the date and time for the execution of this task.
A popup calendar appears.

b. Select the date from the calendar.
c. Alternatively, you can enter the date and time manually.

Valid date and time format for this entry is YYYY-MM-DD hh:mm where YYYY denotes the four digit year, MM denotes the two digit month, DD denotes the two digit day and hh denotes the two digit hour, and mm denotes the two digit minute.

9. To preview the commands of the ACL rule set that deploys, click the icon 📐 in the Preview Commands field of the Deploy Details list.

The Preview Commands dialog box appears and the contents of the rule list configured for deployment to the selected device appear.

10. Review the contents to verify that these are the rules you want to deploy for every device.
11. Click OK when you have finished reviewing the rules.
12. Click OK to accept the deployment and task modification and to submit this request to the deployment task queue.

Starting an ACL deployment task

To re-start a deployment task that has been paused:

1. Navigate to ACL Resource:
   a. Click the Service tab from the tabular navigation system on the top.
   b. Click the 📐ACL Management icon located under the Resource and Configuration Management section of the Service tab.
   c. Click the 📐ACL Deployment link located under ACL Management on the navigation tree on the left.

   The ACL Deployment page appears and the deployment Task List displays in the lower half of this page.

2. Click the checkbox ☐ to the left of the Status and Task Name fields for the deployment tasks you want to start. Note that you can only start deployment tasks that have been paused.
3. Click the Start button located at the top of the Task List.

   The Status for the deployment task indicates that the task is now in a waiting status.

Stopping an ACL deployment task

To stop a deployment task:

1. Navigate to ACL Resource:
   a. Click the Service tab from the tabular navigation system on the top.
   b. Click the 📐ACL Management icon located under the Resource and Configuration Management section of the Service tab.
   c. Click the 📐ACL Deployment link located under ACL Management on the navigation tree on the left.

   The ACL Deployment page appears and the deployment Task List displays in the lower half of this page.

2. Click the checkbox ☐ to the left of the Status and Task Name fields for the deployment task you want to stop.
3. Click the **Stop** button located at the top of the **Task List**.

   The **Status** for the deployment task indicates that the task has been paused.

### Managing deployments using the ACL deployment wizard

The ACL Deployment wizard provides you with a step-by-step guide for successfully deploying and removing ACLs and ACL uses. During the deployment task configuration process, IMC evaluates the selected devices and ACLs to determine whether or not the task can be executed successfully, identifies when devices do not match the configuration selections, displays warning messages and evaluation results to guide the successful deployment of ACL resources, and removes devices from the deployment configuration for which the selected action cannot be successfully executed.

You can choose to run deployment tasks immediately or to schedule them for a later date and you can also choose to execute tasks to one or more devices sequentially or in concurrent. Operators can also choose how ACL Management handles errors when they arise.

### Deploying ACLs to devices

You can use ACL Management’s ACL Deployment wizard to deploy an ACL rule set to one or more devices.

To deploy an ACL to one or more devices:

1. **Navigate to ACL Resource**:
   a. Click the **Service** tab from the tabular navigation system on the top.
   b. Click the **ACL Management** icon located under the **Resource and Configuration Management** section of the **Service** tab.
   c. Click the **ACL Deployment** link located under **ACL Management** on the navigation tree on the left.

   The **ACL Deployment** page appears.

2. Click the **Deploy ACLs** link located under the **Deploy Wizard** section of the **ACL Deployment** page.

   The **Settings** step of the **Deploy ACLs** wizard appears.

3. To select the devices you want to deploy ACLs to, click the **Select** button located under the **Select Devices** section of the page.

   The **Select Devices** dialog box appears.

   You can add devices by using either the **View** or **Advanced** query option. See "Adding devices by View" (page 85) and "Adding devices by Advanced query" (page 85).

4. To select the ACL you want to add, click the **Select** button located under the **Select ACL Resource** section of the page.

   The **Select ACL Resource** dialog box displays with all ACLs displayed in the list.

5. Select a rule set from the **Select Rule Set to Deploy** list associated with the ACL that contains the rule set you want to deploy.

6. Click **OK** to accept your ACL and rule set choice.

7. Confirm that the rule set from the ACL you selected now appears in the **Select ACL Resource** list.

8. To delete the ACL and rule set you have selected, click the icon **X** in the **Delete** field associated with the rule set want to delete. Repeat the instructions in this step to re-select a rule list from an ACL.

9. Click **Next**.
The Summary step of the Deploy ACLs wizard appears with the ACLs to Deploy list that contains all devices to which the selected ACL and rule set are deployed.

10. Review the entire contents of the ACLs to Deploy list to verify that the deployment is configured as intended.

11. In particular, select from the Deploy Strategy field, the deploy strategy you want to employ for every device you have selected for ACL deployment.

   Deployment strategies include:
   - Select Not Deploy if you have decided after reviewing the deployment information that you do not want to deploy the selected rule list to the associated device.
   - Select Add if you want to deploy the selected ACL and rule list to the device. If an ACL with the same name already exists on the device, the existing ACL is deleted and replaced with the ACL and rule list to be deployed.
   - Select Append if you want to append the contents of the selected ACL and rule list to an ACL with the same name that already exists on the device. This option is only selectable if there is already an existing ACL with the same name or identifier.

   △ CAUTION:
   If an ACL with the same name exists, the match order of the ACL for the Add or Append operation must match that of the existing ACL.

   If a device does not support ACLs, then the devices do not appear on the list.

12. Click Deploy to accept your ACL deployment configuration.

   The Add Task page appears.

   The default task name is displayed in the Task Name field.

13. To enter a task name for this deployment task, delete the contents of this field and enter a new task name.

   A valid length for a task name is 1 – 32 characters. The task name cannot begin with a number [0-9].

14. Enter a brief description for this deployment task in the Description field.

15. Select how you want IMC to execute the task to every device from the Deployment Order section of the Add Task page by clicking the radio button ☑ to the left of the appropriate option:

   - Select Concurrent if you want ACL Management to execute the task to multiple devices simultaneously, or
   - Select Sequential if you want ACL Management to execute the task to one device at a time.

16. Select the strategy you want ACL Management to use should a problem arise in the execution of the task from the Error Handling list. Options include:

   - Select Abort the task if you want to stop the deployment to pending devices, but not affect devices to which deployments are in progress or to which deployments have successfully completed once an error in deployment arises, or
   - Select Abort the task and clear data deployed on the error device if you want to stop the deployment and clear all deployments on the device experiencing a problem once an error in deployment arises, or
   - Select Skip the error device and continue if you want to stop all deployments on the device experiencing a problem once an error in deployment arises, or
   - Select Clear data deployed on the error device and continue if you want to clear all deployments on the device experiencing a problem once an error in deployment arises.
17. Choose to save the device’s running configuration as the startup configuration prior to execution:
   o Click the radio button ☑ to the left of Yes in the Save to Startup File field, or
   o Click the radio button ☐ to the left of No if you do not want to save the current configuration.

18. Select when you want ACL Management to execute the task to the selected devices:
   o To execute the task immediately, click on the radio button ☑ to the left of Immediately, or
   o To schedule a time for ACL Management to execute the task, click the radio button ☐ to the left of
     At Scheduled Time.
     If you selected At Scheduled Time:
     a. Click the calendar function ☘ to the right of the At Scheduled Time field to populate the date and
        time for the execution of this task.
        A popup calendar appears.
     b. Select the date from the calendar.
     c. Alternatively, you can enter the date and time manually.
        Valid date and time format for this entry is YYYY-MM-DD hh:mm where YYYY denotes the four digit
        year, MM denotes the two digit month, DD denotes the two digit day and hh denotes the two digit
        hour, and mm denotes the two digit minute.

19. To preview the commands of the task, click the icon ☯ in the Preview Commands field of the Deploy
    Details list.
    The Preview Commands dialog box appears and the commands of the task to be executed appear.

20. Review the contents to verify that these are the commands you want to execute.

21. Click OK when you have finished previewing the commands.

22. Click OK to accept the deployment and task configuration and to submit this request to the deployment
    task queue.
    If the task is scheduled to run immediately, the Task Result dialog box appears. This dialog box
    provides you with a real time status of the deployment task.

23. Click Close on the Task Result dialog box when the task has finished executing.

24. To review the results of the task in the Result field of the Task List, click the Refresh button located at the
    top of the Task List to reload the page with the most current information for all tasks in the list.

25. Review the results of your deployment task in the Result field of the deployment Task List.
    The contents of this field serve as a link to the Task Result page that contains more detailed information
    the result and causes for a failed deployment. From this page, you can also review the commands
    executed by the deployment task.

Removing ACLs from devices

You can use the ACL Deployment wizard to remove ACLs from selected devices.

To remove an ACL from one or more devices:

1. Navigate to ACL Resource:
   a. Click the Service tab from the tabular navigation system on the top.
   b. Click the ACL Management icon located under the Resource and Configuration Management
      section of the Service tab.
c. Click the **ACL Deployment** link located under **ACL Management** on the navigation tree on the left.

The **ACL Deployment** page appears.

2. Click the **Delete ACLs on Devices** link located under the **Deploy Wizard** section of the **ACL Deployment** page.

The **Select Devices** step of the **Delete ACLs on Devices** wizard appears.

3. To select the devices you want to remove ACLs from, click the **Select Devices** button located under the **Select Devices** step of the **Delete ACLs on Devices** wizard page.

The **Select Devices** dialog box appears.

4. Add devices by using either the **View** or **Advanced** query option. See "Adding devices by View" (page 85) and "Adding devices by Advanced query" (page 85).

5. Click **Next**.

The **Select ACL** step of the **Delete ACLs on Devices** wizard appears.

6. Select the ACL identity type by clicking the radio icon to the left of the **Identity Type** field for the ACL you want to delete.

For more information using ACL Management to view the ACLs on a device and ACL details, see "Managing device ACL definitions" (page 759).

7. Enter the ACL identifier you want to delete in the **ACL Identifier** field.

8. Click **Next**.

The **Summary** step of the **Delete ACLs on Devices** wizard appears.

9. Review the contents of this page to verify the configuration of the **Delete ACLs** task:

   o If the **ACL Exists on Device** field contains the value **No**, then the **Delete ACL** deployment task cannot proceed because the ACL specified in the previous step cannot be found on the selected device.

   o If the **ACL Exists on Device** field contains the value **Yes**, then the **Delete ACL** deployment task can proceed because the ACL specified in the previous step was found on the selected device.

   o If the **ACL Being Used** field contains the value **Yes**, then the **Delete ACL** deployment task cannot proceed because the ACL specified in the previous step is in use.

   o If the **ACL Being Used** field contains the value **No**, then the **Delete ACL** deployment task can proceed because the ACL specified in the previous step is not in use.

10. Click **Finish** when you have finished reviewing the configuration details and are ready to submit the task to the ACL deployment task queue.

The **Delete ACLs on Device Result** page displays with the results of ACL Management’s evaluation of the deployment task. If the delete ACL deployment task can be completed successfully, the **Success** field contains the value **Yes**.

11. Click **Deploy** if the **Success** field contains the value **Yes** to proceed to the next step in the deployment process.

The **Add Task** page appears with the default task name in the **Task Name** field.

12. To enter a task name for this deployment task, delete the contents of this field and enter a new task name.

   A valid length for a task name is 1 – 32 characters. The task name cannot begin with a number [0-9].

13. Enter a brief description for this deployment task in the **Description** field.
14. Select how you want IMC to execute the task to every device from the Deployment Order section of the Add Task page by clicking the radio button \(\bigcirc\) to the left of the appropriate option:
   - Select Concurrent if you want ACL Management to execute the task to multiple devices simultaneously, or
   - Select Sequential if you want ACL Management to execute the task to one device at a time.

15. Select the strategy you want ACL Management to use should a problem arise in the execution of the task from the Error Handling list. Options include:
   - Select Abort the task if you want to stop the deployment to pending devices, but not affect devices to which deployments are in progress or to which deployments have successfully completed once an error in deployment arises, or
   - Select Abort the task and clear data deployed on the error device if you want to stop the deployment and clear all deployments on the device experiencing a problem once an error in deployment arises, or
   - Select Skip the error device and continue if you want to stop all deployments on the device experiencing a problem once an error in deployment arises, or
   - Select Clear data deployed on the error device and continue if you want to clear all deployments on the device experiencing a problem once an error in deployment arises.

16. Save the device’s running configuration as the startup configuration prior to execution:
   - Click the radio button \(\bigcirc\) to the left of Yes in the Save to Startup File field, or
   - Click the radio button \(\bigcirc\) to the left of No if you do not want to save the current configuration.

17. Select when you want ACL Management to execute the task to the selected devices:
   - To execute the task immediately, click on the radio button \(\bigcirc\) to the left of Immediately, or
   - To schedule a time for ACL Management to execute the task, click on the radio button \(\bigcirc\) to the left of At Scheduled Time.

      If you selected At Scheduled Time:
      a. Click on the calendar function \(\bigcirc\) to the right of the At Scheduled Time field to populate the date and time for the execution of this task.
         A popup calendar appears.
      b. Select the date from the calendar.
      c. Alternatively, you can enter the date and time manually.
         Valid date and time format for this entry is YYYY-MM-DD hh:mm where YYYY denotes the four digit year, MM denotes the two digit month, DD denotes the two digit day and hh denotes the two digit hour, and mm denotes the two digit minute.

18. To preview the commands of the task, click the icon \(\bigcirc\) in the Preview Commands field of the Deploy Details list.

      The Preview Commands dialog box appears and the commands of the task to be executed are shown.

19. Review the contents to verify that these are the commands you want to execute.

20. Click OK when you have finished previewing the commands.

21. Click OK to accept the deployment and task configuration and to submit this request to the deployment task queue.

      If the task is scheduled to run immediately, the Task Result dialog box displays with the real time status of the deployment task.

22. Click Close on the Task Result dialog box when the task has finished executing.
23. To review the results of the task in the Result field of the Task List, click the Refresh button located at the top of the Task List to reload the page with the most current information for all tasks in the list.

24. Review the results of your deployment task in the Result field of the deployment Task List.

The contents of this field serve as a link to the Task Result page that contains more detailed information the result and causes for a failed deployment. From this page, you can also review the commands executed by the deployment task.

Deleting time ranges on devices

You can use the ACL Deployment wizard to remove ACL time range configurations from selected devices.

To remove a time range from an ACL one or more devices:

1. Navigate to ACL Resource:
   a. Click the Service tab from the tabular navigation system on the top.
   b. Click the ACL Management icon located under the Resource and Configuration Management section of the Service tab.
   c. Click the ACL Deployment link located under ACL Management on the navigation tree on the left.

   The ACL Deployment page appears.

2. Click the Delete Time Ranges on Devices link located under the Deploy Wizard section of the ACL Deployment page.

   The Config step of the Delete Time Ranges on Devices wizard appears.

3. Enter the name of the time range you want to remove in the Input time ranges to be deleted field.

4. To identify the time ranges that are configured on a device, go to the ACL Devices feature of the ACL Management.

   For more information using ACL Management to view the ACLs on a device and ACL details, see "Managing device ACL definitions" (page 759).

5. To select the devices you want to remove time ranges from, click the Select Devices button located under the Select Devices section of the Config step of the page.

   The Select Devices dialog box appears.

6. Add devices by using either the View or Advanced query option. See "Adding devices by View" (page 85) and "Adding devices by Advanced query" (page 85).

7. Click Next.

   The Summary step of the Delete Time Ranges on Devices wizard appears.

8. Review the contents of this page to verify the configuration of the delete time range task:
   o If the Time Range Exists on Device field contains the value No, then the deployment task cannot proceed because the time range specified in the previous step cannot be found on the selected device, or
   o If the Time Range Exists on Device field contains the value Yes, then the deployment task can proceed because the time ranges specified in the previous step was found on the selected device.

9. Click Finish when you have finished reviewing the configuration details and are ready to submit the task to the ACL deployment task queue.

The Delete Time Ranges on Devices Result page display with the results of ACL Management’s evaluation of the deployment task. If the delete the time range deployment task can be completed successfully, the Success field contains the value Yes.
10. Click **Deploy** if the **Success** field contains the value **Yes** to proceed to the next step in the deployment process.

    The **Add Task** page appears.

    The default task name displays in the **Task Name** field.

11. To enter a task name for this deployment task, delete the contents of this field and enter a new task name.

    A valid length for a task name is 1 – 32 characters. The task name cannot begin with a number [0-9].

12. Enter a brief description for this deployment task in the **Description** field.

13. Select how you want IMC to execute the task to every device from the **Deployment Order** section of the **Add Task** page by clicking the radio button ☑️ to the left of the applicable option:

    o Select **Concurrent** if you want ACL Management to execute the task to multiple devices simultaneously, or

    o Select **Sequential** if you want ACL Management to execute the task to one device at a time.

14. Select the strategy you want ACL Management to use should a problem arise in the execution of the task from the **Error Handling** list. Options include:

    o Select **Abort the task** if you want to stop the deployment to pending devices, but not affect devices to which deployments are in progress or to which deployments have successfully completed once an error in deployment arises, or

    o Select **Abort the task and clear data deployed on the error device** if you want to stop the deployment and clear all deployments on the device experiencing a problem once an error in deployment arises, or

    o Select **Skip the error device and continue** if you want to stop all deployments on the device experiencing a problem once an error in deployment arises, or

    o Select **Clear data deployed on the error device and continue** if you want to clear all deployments on the device experiencing a problem once an error in deployment arises.

15. Save the device’s running configuration as the startup configuration prior to execution:

    o Click the radio button ☑️ to the left of **Yes** in the **Save to Startup File** field, or

    o Click the radio button ☐ to the left of **No** if you do not want to save the current configuration.

16. You can select when you want ACL Management to execute the task to the selected devices:

    o To execute the task immediately, click on the radio button ☑️ to the left of **Immediately**, or

    o To schedule a time for ACL Management to execute the task, click on the radio button ☑️ to the left of **At Scheduled Time**.

    If you selected **At Scheduled Time**:

    a. Click the calendar function 📅 to the right of the **At Scheduled Time** field to populate the date and time for the execution of this task.

    A popup calendar appears.

    b. Select the date from the calendar.

    c. Alternatively, you can enter the date and time manually.

    Valid date and time format for this entry is YYYY-MM-DD hh:mm where YYYY denotes the four digit year, MM denotes the two digit month, DD denotes the two digit day and hh denotes the two digit hour, and mm denotes the two digit minute.

17. To preview the commands of the task, click the icon 📃 in the **Preview Commands** field of the **Deploy Details** list.
The **Preview Commands** dialog box displays and the commands of the task to be executed appear.

18. Review the contents to verify that these are the commands you want to execute.

19. Click **OK** when you have finished previewing the commands.

20. Click **OK** to accept the deployment and task configuration and to submit this request to the deployment task queue.

   If the task is scheduled to run immediately, the **Task Result** dialog box appears, providing you with a real time status of the deployment task.

21. Click **Close** on the **Task Result** dialog box when the task has finished executing.

22. To review the results of the task in the **Result** field of the **Task List**, click the **Refresh** button located at the top of the **Task List** to reload the page with the most current information for all tasks in the list.

23. Review the results of your deployment task in the **Result** field of the deployment **Task List**.

   The contents of this field serve as a link to the **Task Result** page that contains more detailed information the result and causes for a failed deployment.

   From this page, you can also review the commands executed by the deployment task.

### Deploying ACL uses using the deploy ACL uses feature

You can also use the ACL Deployment wizard to deploy specific ACL uses to selected devices. Uses that can be deployed using the Deployment wizard include packet filtering and VLAN packet filtering.

To deploy an ACL use to one or more interfaces on selected devices:

1. Navigate to **ACL Resource**:
   a. Click the **Service** tab from the tabular navigation system on the top.
   b. Click the **ACL Management** icon located under the **Resource and Configuration Management** section of the **Service** tab.
   c. Click the **ACL Deployment** link located under **ACL Management** on the navigation tree on the left.

   The **ACL Deployment** page appears.

2. Click the **Deploy ACL Uses** link located under the **Deploy Wizard** section of the **ACL Deployment** page.

   The **Select Use Type** step of the **Deploy ACL Uses** wizard appears.

3. Select the use type you want to deploy from the list provided.

4. Click **Next**.

5. Click the **Select Device** to the device you want to deploy the selected use type to.

   The **Select Devices** dialog box appears.

6. Add devices by using either the **View** or **Advanced** query option. See "Adding devices by View" (page 85) and "Adding devices by Advanced query" (page 85).

7. Click **Next**.

   The **Select Object** step of the **Deploy ACL Uses** wizard appears.

8. Select the direction that you want the filter to be applied from the **Filter Direction** list.

9. Select the interfaces that you want to apply the filtering to from the **Interface List** column on the left or VLAN interfaces you want to apply the filtering to by choosing from the following:
To select an interface, click the interface to highlight it, and then click the right arrow key \[^\rightarrow\]\ to select it.

To select all interfaces, click the double right arrow key \[^\rightarrow\]^2.

To deselect an interface, click the interface in the Selected Interfaces column to select it and then click the left arrow key \[^\leftarrow\]\ to deselect it.

To deselect all interfaces, click on the double left arrow key \[^\leftarrow\]^2 and then select the VLAN that you want to apply the filter to from the VLAN List column on the left.

To select a VLAN, click on the VLAN to highlight it and click the right arrow key \[^\rightarrow\]\ to select it.

To select all interfaces, click on the double right arrow key \[^\rightarrow\]^2.

To deselect a VLAN, click on the VLAN in the Selected VLANs column to highlight it and click the left arrow key \[^\leftarrow\]\ to deselect it.

To deselect all VLANs, click on the double left arrow key \[^\leftarrow\]^2.

10. Repeat this step for every device you have selected for ACL use deployment.

You can use the same interface for other devices by checking the box to the left of the Same choice for other devices.

11. Click Next when you have finalized your selection of interfaces for all devices to which you apply filtering.

ACL Management displays a warning if one or more of the selected devices do not support the ACL use type selected.

12. Select the ACL type you want apply from the ACL Type list.

13. Select the type of ACL identifier that to be used for filtering by clicking the radio button \[^\square\]\ to the left type in the ACL Identity Type section.

14. To view a list of all ACLs in IMC, navigate to the ACL Resource link located on the left navigation tree under ACL Management.

15. Enter the name or number of the ACL you want to use for filtering in the ACL Identifier field.

16. To view a list of all ACLs in IMC, navigate to the ACL Resource link located on the left navigation tree under ACL Management.

17. Click Next.

The Summary step of the Deploy ACL Uses wizard appears.

18. Review the information provided in the Summary page to ensure that you have configured the wizard according to your needs and that the ACL can be deployed to all interfaces on all devices you have selected.

Specifically, review the contents of the ACL exists field for every entry in the table as the value in this field helps identify whether or not the packet filter can be applied to the associated interface.

- If the ACL Exists field contains the value No, then the Deploy ACL Uses deployment task cannot proceed because the ACL specified in the previous step cannot be found on the selected device.

- If the ACL Exists field contains the value Yes, then the Deploy ACL Uses deployment task can proceed because the ACL specified in the previous step was found on the selected device.

19. Click Finish when you have finished reviewing the configuration details and are ready to submit the task to the ACL deployment task queue.

Packet filters are not deployed if the selected ACL rule number ranges do not match the ACL type for the selected devices. Packet direction is device dependent. If the device does not support the selected direction of the packet filter, the ACL is not deployed to the device.
The **Deploy ACL Uses Result** page appears.

ACL Management evaluates whether or not the selected **Deploy ACL Uses** can be successfully deployed to all of the selected interfaces for all selected devices. The results of this evaluation can be found in the **Result** field on the list displayed in the **Deploy ACL Uses Result** page.

20. **Click OK** to proceed to the next step.

ACL Management lists only those devices and their interfaces to which the ACL Use can be deployed successfully.

The **Add Task** page appears.

The default task name displays in the **Task Name** field.

21. **To enter a task name** for this deployment task, delete the contents of this field and enter a new task name.

A valid length for a task name is 1 – 32 characters. The task name cannot begin with a number [0-9].

22. **Enter a brief description** for this deployment task in the **Description** field.

23. **Select how you want IMC to execute** the task to every device from the **Deployment Order** section of the **Add Task** page by clicking the radio button □ to the left of the applicable option:
   - **Select Concurrent** if you want ACL Management to execute the task to multiple devices simultaneously, or
   - **Select Sequential** if you want ACL Management to execute the task to one device at a time.

24. **Select the strategy** you want ACL Management to use should a problem arise in the execution of the task from the **Error Handling** list. Options include:
   - **Select Abort the task** if you want to stop the deployment to pending devices, but not affect devices to which deployments are in progress or to which deployments have successfully completed once an error in deployment arises, or
   - **Select Abort the task and clear data deployed on the error device** if you want to stop the deployment and clear all deployments on the device experiencing a problem once an error in deployment arises, or
   - **Select Skip the error device and continue** if you want to stop all deployments on the device experiencing a problem once an error in deployment arises, or
   - **Select Clear data deployed on the error device and continue** if you want to clear all deployments on the device experiencing a problem once an error in deployment arises.

25. **Save the device’s running configuration as the startup configuration** prior to execution:
   - **Click the radio button □ to the left of Yes in the **Save to Startup File** field, or
   - **Click the radio button □ to the left of No if you do not want to save the current configuration.**

26. **Select when you want ACL Management to execute** the task to the selected devices:
   - **To execute the task immediately**, click on the radio button □ to the left of **Immediately**, or
   - **To schedule a time** for ACL Management to execute the task, click on the radio button □ to the left of **At Scheduled Time**.

      If you selected **At Scheduled Time**
      a. **Click the calendar function □ to the right of the **At Scheduled Time** field to populate the date and time for the execution of this task.**
      A popup calendar appears.
      b. **Select the date from the calendar.**
      c. **Alternatively, you can enter the date and time manually.**
Valid date and time format for this entry is YYYY-MM-DD hh:mm where YYYY denotes the four digit year, MM denotes the two digit month, DD denotes the two digit day and hh denotes the two digit hour, and mm denotes the two digit minute.

27. To preview the commands of the task, click the icon 📋 in the **Preview Commands** field of the **Deploy Details** list.

The **Preview Commands** dialog box appears and the commands of the task to be executed appear.

28. Review the contents to verify that these are the commands you want to execute.

29. Click **OK** when you have finished previewing the commands.

30. Click **OK** to accept the deployment and task configuration and to submit this request to the deployment task queue.

   If the task is scheduled to run immediately, the **Task Result** dialog box appears. This dialog box provides you with a real time status of the deployment task.

31. Click **Close** on the **Task Result** dialog box when the task has finished executing.

32. To review the results of the task in the **Result** field of the **Task List**, click the **Refresh** button located at the top of the **Task List** to reload the page with the most current information for all tasks in the list.

33. Review the results of your deployment task in the **Result** field of the deployment **Task List**.

   The contents of this field serve as a link to the **Task Result** page that contains more detailed information the result and causes for a failed deployment. From this page, you can also review the commands executed by the deployment task.

**Removing ACL uses from devices**

You can also use the ACL Deployment wizard to remove specific ACL uses previously deployed to devices. Uses that can be removed using the Deployment wizard include packet filtering and VLAN packet filtering.

To remove an ACL use from one or more interfaces on selected devices:

1. **Navigate to ACL Resource**.
   
   a. Click the **Service** tab from the tabular navigation system on the top.

   b. Click the **ACL Management** icon located under the **Resource and Configuration Management** section of the **Service** tab.

   c. Click the **ACL Deployment** link located under **ACL Management** on the navigation tree on the left.

      The **ACL Deployment** page appears.

2. Click the **Delete ACL Uses on Devices** link located under the **Deploy Wizard** section of the **ACL Deployment** page.

   The **Select Use Type** step of the **Delete ACL Uses on Devices** wizard appears.

3. Select the use type you want to remove from the list provided.

4. Click **Next**.

5. Click the **Select Device** to the devices you want to remove the selected use type from.

   The **Select Devices** dialog box appears.

6. Add devices by using either the View or Advanced query option. See "Adding devices by View" (page 85) and "Adding devices by Advanced query" (page 85).

7. Click **Next**.

797
The Select Object step of the Delete ACL Uses on Devices wizard appears.

8. Select the direction that the filter was previously applied from the Filter Direction list. Select the interfaces or VLAN interfaces you want to apply the filtering to by choosing from the following:
   o Select the interfaces that you want to remove the filtering for from the Interface List column on the left.
   a. To select an interface, click the interface to highlight it.
   b. Click the right arrow key to select it.
   c. To select all interfaces, click the double right arrow key.
   d. To deselect an interface, click the interface in the Selected Interfaces column to select it.
   e. Click the left arrow key to deselect it.
   f. To deselect all interfaces, click on the double left arrow key.
   o Select the VLAN that you want to apply the filter to from the VLAN List column on the left.
   g. To select a VLAN, click the VLAN to highlight it.
   h. Click the right arrow key to select it.
   i. To select all interfaces, click the double right arrow key.
   j. To deselect a VLAN, click the VLAN in the Selected VLANs column to highlight it.
   k. Click the left arrow key to deselect it.
   l. To deselect all VLANs, click on the double left arrow key.

9. Repeat this step for every device you have selected for ACL use removal.

10. Click Next when you have finalized your selection of interfaces for all devices to which you are removing filtering.

11. Select the ACL type you want remove from the ACL Type list.

12. Select the type of ACL identifier to remove by clicking the radio button to the left type in the ACL Identity Type section.
   a. To view a list of all ACLs in IMC, navigate to the ACL Resource link located on the left navigation tree under ACL Management.

13. Enter the name or number of the ACL you want remove in the ACL Identifier field.
   a. To view a list of all ACLs in IMC, navigate to the ACL Resource link located on the left navigation tree under ACL Management.

14. Click Next.

   The Summary step of the Delete ACL Uses on Devices wizard appears.

15. Review the information provided in the Summary page to ensure that you have configured the wizard according to your needs and that the ACL can be removed from all interfaces on all devices you have selected.

   Specifically, review the contents of the ACL exists field for every entry in the table as the value in this field helps you identify whether or not the packet filter can be removed from the associated interface.

16. Do one of the following:
17. If the ACL Use Exists field contains the value No, then the Delete ACL Uses on Devices deployment task cannot proceed because the ACL specified in the previous step is not being used on the selected device, or

18. If the ACL Use Exists field contains the value Yes, then the Delete ACL Uses deployment task can proceed because the ACL specified in the previous step is in use on the selected device.

17. Click Finish when you have finished reviewing the contents of the Summary page and are ready to proceed to the next step.

The Delete ACL Uses on Devices Result page appears.

ACL Management evaluates whether or not the selected Deploy ACL Use can be successfully deployed to all of the selected interfaces for all selected devices. The results of this evaluation can be found in the Result field on the list displayed in the Delete ACL Uses on Devices Result page.

18. Click OK to proceed to the next step.

The Add Task page appears.

The default task name displays in the Task Name field.

19. To enter a task name for this deployment task, delete the contents of this field and enter a new task name.

A valid length for a task name is 1 – 32 characters. The task name cannot begin with a number [0-9].

20. Enter a brief description for this deployment task in the Description field.

21. Select how you want IMC to execute the task to every device from the Deployment Order section of the Add Task page by clicking the radio button to the left of the applicable option:

22. Select the strategy you want ACL Management to use should a problem arise in the execution of the task from the Error Handling list. Options include:

23. Save the device’s running configuration as the startup configuration prior to execution:

24. Select when you want ACL Management to execute the task to the selected devices:

If you selected At Scheduled Time:
a. Click the calendar function 📅 to the right of the **At Scheduled Time** field to populate the date and time for the execution of this task.

A popup calendar appears.

b. Select the date from the calendar.

c. Alternatively, you can enter the date and time manually.

Valid date and time format for this entry is YYYY-MM-DD hh:mm where YYYY denotes the four digit year, MM denotes the two digit month, DD denotes the two digit day and hh denotes the two digit hour, and mm denotes the two digit minute.

25. To preview the commands of the task, click the icon 📷 in the **Preview Commands** field of the **Deploy Details** list.

The **Preview Commands** dialog box appears and the commands of the task to be executed appear.

26. Review the contents to verify that these are the commands you want to execute.

27. Click **OK** when you have finished previewing the commands.

28. Click **OK** to accept the deployment and task configuration and to submit this request to the deployment task queue.

If the task is scheduled to run immediately, the **Task Result** dialog box appears. This dialog box provides you with a real time status of the deployment task.

29. Click **Close** on the **Task Result** dialog box when the task has finished executing.

30. To review the results of the task in the **Result** field of the **Task List**, click the **Refresh** button located at the top of the **Task List** to reload the page with the most current information for all tasks in the list.

31. Review the results of your deployment task in the **Result** field of the deployment **Task List**.

The contents of this field serve as a link to the **Task Result** page that contains more detailed information the result and causes for a failed deployment. From this page, you can also review the commands executed by the deployment task.
11 Security control center

The Security Control Center provides you with proactive security monitoring and management, including real
time threat monitoring, detection, and analysis and the ability to define security policies enabling operators
to take manual or automated actions when a security attack occurs. You can manage security attacks from
a choice of two displays, where you can also access attack reports, including their source, destinations, and
the results of actions taken to address the attacks.

IMC can detect and take proactive action on many types of security attacks, including IP Spoofing, WinNuke,
SYN Flood, ICMP Flood, UDP Flood, IP Sweep, TCP Port Scan, UDP Port Scan, IPS Worm, IPS Scan, Tracer, 
Large ICMP, Smurf, ICMP Redirect, ICMP Unreachable, Fraggle, Source Route, Route Record, Land, Teardrop,
TCP Flag, Ping of Death, Frag Flood, IP Fragment, Scan, ARP Overspeed, DHCP Server Detect, and
Duplicate ARP Address.

IMC monitors many of these security threats in real time by receiving and processing Syslog events and
SNMP traps sent by devices. Syslog messages are analyzed by IMC’s Syslog CSU module, which are then
processed and displayed by both IMC’s Fault module and SCC. The Syslog messages that IMC alarms on
include Duplicate Addresses, ARP Overspeed, DHCP Server Detect, and IMC’s attack event. IMC also
processes SNMP traps sent by managed devices when the devices 1) support these trap types; 2) are
configured to send traps to IMC and 3) when IMC is configured to receive traps from the device. The SNMP
traps that SCC currently supports include Duplicate Address/ARP Overspeed/DHCP Server Detect
(1.3.6.1.4.1.2011.10.4.2.8.2.6.22), IMC Alarm (1.3.6.1.4.1.2011.10.4.2.8.2.6.9) for SYSLOG
component, and SecCenter (1.3.6.1.4.1.25506.2.77.6.0 and 1.3.6.1.4.1.8763.6.0). In addition to the
tabular view on security attack alarms, SCC also provides you with a visual display of attacks through the
attack path topology map.

Once IMC has received a Syslog message or SNMP trap and generated an alarm for it, SCC displays the
alarm in the Attack Alarm List. Alternatively, you can use the Realtime Attack Alarm List for viewing the most
recent attack alarms, allowing you to respond to attack alarms by initiating actions. Actions that can be
taken vary by attack type but in general there are six supported actions: 1) shutdown the access port; 2) alert
the administrator by email; 3) isolate the online user to a restricted network; 4) send a warning message to
the online user; 5) kick the online user off; and 6) add the online user to the blacklist.

Through the use of security control policies, you can proactively manage their response to security threats
and attacks. Security control policies allow you to define what actions to be taken in response to attack
alarms. A security control policy combines the identification and alarming of a security attack with an action
that can be taken in response to the security attack. The actions configured for security control policies can
be executed manually or they can be configured to run automatically upon detection of the security attack.

Lastly, SCC provides operators with summarized reporting of security attacks in the last hour. Summary
reports include the Top 10 Attack Alarms Report, the Top 10 Attack Sources Report, the Top 10 Attack
Destinations Report and the Execution Results Report.

Managing security attack alarms

SCC provides you with two views for alarms, the Attack Alarm List and the Realtime Attack Alarm List. The
Attack Alarm List provides operators with visibility into all attack alarms, allowing you to view all alarms and
drill down into the details for the attack alarm. From the Attack Alarm List, you can also perform basic and advanced queries to filter the Attack Alarm List for those attack alarms that meet their search criteria and initiate actions including shutting down interfaces and notifying the appropriate staff of a security event. From this list, operators can also view the results of the actions they have executed against a security attack with a topology map of the attach path. For actions that support it, operators can also restore an action.

The Realtime Attack Alarm List provides operators with a view of the Attack Alarm List filtered for the most recent attack alarms. The Realtime Attack Alarm List offers operators the same functionality as the Attack Alarm List for browsing attack alarms and attack alarm details, taking actions, viewing the results an action, restoring an action, and viewing the topology of an attack path.

**Attack alarm list overview**

You can view all security threats detected by IMC from the Attack Alarm List, providing visibility into the type of attack, its source, destination, and date and time stamp. From the Attack Alarm List, you can navigate to the Alarm Details page to view more information for the associated attack alarm and use a topology view of the attack using the Attack Path option. You can also execute an action for attack alarms from the Attack Alarm List.

**Browsing the attack alarms list**

To browse all attack alarms

1. Navigate to **Alarm→Browse Attack Alarm**:
   a. Click the **Alarm** tab from the tabular navigation system on the top.
   b. Click the **Security Control Center** on the navigation tree on the left.
   c. Click the **Browse Attack Alarm** link located under **Security Control Center** on the navigation tree on the left.

   The Attack Alarm List displays in the main pane of the Browse Attack Alarm page.

**Attack alarm list**

- **Name**: Contains the type of attack that was detected by IMC. The contents of this field serve as a link to the Attack Alarm Details page. The Attack Alarm Details page provides more detailed information on the attack. For more information on this feature, see "Viewing attack alarm details" (page 804).
- **Source**: Contains the IP address of the device that initiated the attack, if known.
- **Destination**: Contains the destination IP address of the attack, or rather the device that the attack was intended for, if known.
- **Time**: Contains a date and time stamp for IMC’s detection of the attack.
- **Correlated Policy**: Contains the security control policy in IMC that is associated with the attack identified in this attack alarm. If there is no security policy associated with the attack alarm, this field contains the value "Undefined."
- **Result**: Contains a status or summary of the result of any action IMC has taken to address the attack.

2. Click **Manual execution required** in the **Result** field to navigate to the Attack Alarm Details page.
- **Manual execution required** indicates that no action, either automatic or manual, was taken for the associated event. From this page you can execute any actions that are associated with this attack alarm type.

- **Success** indicates that the automatic or manual action that was taken for this type of attack was successful.

- **Failure** indicates that the automatic or manual action that was taken for this type of attack failed. Click **Failure** in the **Result** field to navigate to the **Attack Alarm Details** page. From this page you can get the detailed failure reason.

- **Executing policy** indicates that the automatic or manual action that was specified for this type of attack is currently being executed. Note that the contents of the **Result** field do not serve as a navigation link to the **Attack Alarm Details** page when an action is being executed.

- **No matching policy** indicates that the alarm does not match any security control policy. Click **No matching policy** in the **Result** field to navigate to the **Attack Alarm Details** page. From this page you can select one or more actions, if available, that are associated with this attack alarm type.

- **Waiting for policy execution** indicates that the selected action for the associated security attack alarm is in the queue for processing by IMC. Note that the contents of the **Result** field do not serve as a navigation link to the **Attack Alarm Details** page when an action is waiting for policy execution.

- **Acknowledgement required** indicates that the configured action could not be completed successfully because the conditions necessary to complete the action were not met. For example, the configured action was to shut down an interface. If the interface is unreachable and therefore cannot be shut down, the Result field contains the value, **Acknowledgement required**. The value, **Acknowledgement required** in the **Result** field serves as a link for navigating to a page for re-executing the action manually.

- The contents of the **Result** field serve as a link to one of several pages, depending on the result of the action taken for the associated event. If the result is **Failure**, the link navigates you to the **Security Control Policy Result Report**. For more information on this page, see “Viewing the execution result report” (page 815).

- If the result is **No matching policy**, the link navigates you to the **Execute Action** page. For more information on executing an action, see “Executing a manual action for an attack alarm” (page 813).

- **Attack Path**: This field contains a link to a topology map that displays the attack path.

If the **Attack Alarm List** contains multiple entries, the following navigational aids may appear:

- Click **to page forward in the Attack Alarm List.**

- Click ** to page forward to the end of the Attack Alarm List.**

- Click ** to page backward in the Attack Alarm List.**

- Click ** to page backward to the front of the Attack Alarm List.**

3. Click **8, 15, 50, 100,** or **200** from the right side of the main pane to configure how many items per page you want to view.
⚠️ WARNING:
You can sort the Attack Alarm List by the Name, Source, Destination, Time, and Correlated Policy fields, by clicking the column label to sort the list by the selected field. The column label is a toggle switch that allows you to toggle between the various sort options specific to each field.

Viewing attack alarm details

You can view more detailed information for every attack alarm in the Attack Alarm Details page.

To view the details of an attack alarm:

1. Navigate to Alarm→Browse Attack Alarm:
   a. Click the Alarm tab from the tabular navigation system on the top.
   b. Click the Security Control Center on the navigation tree on the left.
   c. Click the Browse Attack Alarm link located under Security Control Center on the navigation tree on the left.

   The Attack Alarm List displays in the main pane of the Browse Attack Alarm page.

2. Click the link in the Name field of the attack alarm for which you want to view details.

   The Attack Alarm Details page appears.

Attack alarm detail

- **Event Name**: Contains the name or type of the attack.
- **Description**: Contains detailed information about the event. For attack alarms generated by Syslog events, this field contains the actual Syslog entry. For attack alarms generated by Traps, this field contains trap details.
- **Generated at**: Contains a date and timestamp for IMC’s detection of the security attack.
- **Access Device IP of the Attack Source**: Contains the IP address of the access device that the attack source connects to, if known.
- **Access Device Port of the Attack Source**: Contains the interface description of the access device that the attack source connects to, if known.
- **Source MAC**: If displayed, contains the MAC address of the attack source that originated the attack.
- **Source IP**: If displayed, contains the IP address of the attack source that originated the attack.
- **Destination IP**: If displayed, contains the IP address of the attack destination, if known.

For example, as shown in Figure 1, if an attack arises from IP address 192.168.1.1 to IP address 192.168.2.1, the Source IP field is 192.168.1.1, the Destination IP field is 192.168.2.1, the Access Device IP of the Attack Source field is 10.8.1.1, and the Access Device Port of the Attack Source field is GE 0/0/1.
805

Figure 40 Schematic diagram for the attack source and attack destination

192.168.1.1/24 192.168.2.1/24
GE 0/0/1

IP network

o Event Description: If displayed, contains additional information about the attack event. Devices must be configured to include event descriptions in order for this field to be populated.

o Attack Initiator: Contains the userid or name of the user who initiated the attack.

Querying the attack alarm list

SCC provides you with two methods for searching the Attack Alarm List, a basic query method and an advanced query method.

Attack alarm basic query

To query for attack alarms using the Basic Query method:

1. Navigate to Alarm → Browse Attack Alarm.
   a. Click the Alarm tab from the tabular navigation system on the top.
   b. Click the Security Control Center on the navigation tree on the left.
   c. Click the Browse Attack Alarm link located under Security Control Center on the navigation tree on the left.

   The Attack Alarm List displays in the main pane of the Browse Attack Alarm page.

   The Basic Query feature, by default, appears above the Attack Alarm List, if the link to the far right is Advanced Query, then you are in the Basic Query mode.

2. Enter one or more of the following search criteria:
   o Name: Allows you to query for attack alarms by name or attack type.
     a. Enter a partial or complete attack alarm name or type in the Name field.
   o Result: Allows you to search by the result of an action taken by IMC to address the attack.
     b. Select the result you want to query for from the Result list.
   c. Select All if you do not want to limit your search by result.

   The default option for the result field is All.
   o Time: Allows you to query for attack alarms using a specific time range.
     d. Select the time range you want to search for from the Time list.

   The default option is All.
   o Attack Destination: Allows you to specify a device IP address in the infrastructure for which the attacks were intended.
     e. Enter the full IP address of the device for which you want to view all attack alarms in the Attack Destination field.

3. Click Query to begin you search.
4. View the results of your query in the Attack Alarm List.
5. Click Reset to reset both the query values and the search results and to restore the full Attack Alarm List.

**Attack alarm advanced query**

To query for alarms using the Advanced Query method:

1. Navigate to Alarm→Browse Attack Alarm:
   a. Click the Alarm tab from the tabular navigation system on the top.
   b. Click the Security Control Center on the navigation tree on the left.
   c. Click the Browse Attack Alarm link located under Security Control Center on the navigation tree on the left.
   The Attack Alarm List displays in the main pane of the Browse Attack Alarm page.

2. Click the Advanced Query link located to the right of the Attack Alarm List.
   If this link says Basic Query, then you are in the Advanced Query mode.

3. Enter one or more of the following search criteria:
   o **Name**: Allows you to query for attack alarms by name or attack type.
   a. Enter a partial or complete attack alarm name or type in the Name field.
   o **Correlated Policy**: Allows you to query for attack alarms that have a security control policy associated with the attack alarm type.
   b. Select the correlated security control policy from the Correlated Policy list.
   o **Result**: Allows you to search by the result of an action taken by IMC to address the attack.
   c. Select the result you want to query for from the Result list.
   d. Select All if you do not want to limit your search by result.
   o **Attack Time: Start**: Allows you to query for attack alarms using a specific start time.
   e. Auto-populate this field by clicking the calendar icon located to the right.
   A popup calendar appears.
   f. Select the start date from the calendar.
   g. Enter the time in the Time fields provided below the calendar.
   o **Attack Time: End**: Allows you to query for attack alarms using a specific end time.
   h. Auto-populate this field by clicking the calendar icon located to the right.
   A popup calendar appears.
   i. Select the start date from the calendar.
   j. Enter the time in the Time fields provided below the calendar.
   o **Attack Source: Start**: Allows you to specify a range of IP addresses for the source of the attacks.
   Enter a full IP address as the starting IP address of the range you want to search for.
   o **Attack Source: End**: Allows you to specify a range of IP addresses for the source of the attacks.
   Enter a full IP address as the ending IP address of the range you want to search for.
o **Attack Destination: Start**: Allows you to specify a range of IP addresses for the destination of the attacks. Enter a full IP address the starting IP address of the range you want to search for.

o **Attack Destination: End**: Allows you to specify a range of IP addresses for the destination of the attacks. Enter a full IP address as the ending IP address of the range you want to search for.

4. Click **Query** to begin your search.

5. View the results of your query in the **Attack Alarm List**.

6. Click **Reset** to reset both the query values and the search results and to restore the full **Attack Alarm List**.

**Refreshing the attack alarm list**

You can refresh the **Attack Alarm List**. Refreshing the **Attack Alarm List** initiates a query to IMC’s database and refreshes the **Attack Alarm List** with any changes to the **Attack Alarm List** since the page was last loaded.

To refresh the Attack Alarm List:

1. Navigate to **Alarm**→**Browse Attack Alarm**:
   a. Click the **Alarm** tab from the tabular navigation system on the top.
   b. Click the **Security Control Center** on the navigation tree on the left.
   c. Click the **Browse Attack Alarm** link located under **Security Control Center** on the navigation tree on the left.

   The **Attack Alarm List** displays in the main pane of the **Browse Attack Alarm** page.

2. Click **Refresh**.

**Deleting attack alarms from the attack alarm list**

You can delete one or more attack alarms from the **Attack Alarm List**. Once an alarm is deleted, it is removed immediately from the IMC database and it cannot be recovered. Use this feature with caution.

To delete one or more attack alarms:

1. Navigate to **Alarm**→**Browse Attack Alarm**:
   a. Click the **Alarm** tab from the tabular navigation system on the top.
   b. Click the **Security Control Center** on the navigation tree on the left.
   c. Click the **Browse Attack Alarm** link located under **Security Control Center** on the navigation tree on the left.

   The **Attack Alarm List** displayed in the main pane of the **Browse Attack Alarm** page.

2. Click the checkbox ☑️ to the left of the attack alarms you want to delete.

3. Click **Delete**.

4. Click **OK** to confirm the deletion of the selected attack alarms.

**Real-time attack alarm overview**

You can view the most recent security threats detected by IMC from the **Realtime Attack Alarm List**. This list filters the **Attack Alarm List** for the most recent alarms only. From this list, you can navigate to the **Alarm**
Details page. You can also navigate to a topology view of the attack using the Attack Path link. You can also execute an action from the Results link available in the Realtime Attack Alarm List.

**Browsing the realtime attack alarm list**

To browse real-time attack alarms:

1. Navigate to Alarm→Realtime Attack Alarm:
   a. Click the Alarm tab from the tabular navigation system on the top.
   b. Click the Security Control Center on the navigation tree on the left.
   c. Click the Realtime Attack Alarm link located under Security Control Center on the navigation tree on the left.

   The Realtime Attack Alarm List displays in the main pane of the Realtime Attack Alarm page.

**Realtime attack alarm list**

- **Name**: Contains the type of attack that was detected by IMC. The contents of this field serve as a link to the Attack Alarm Details page. The Attack Alarm Details page provides more detailed information on the attack. For more information on this feature, see “Viewing attack alarm details” (page 804).
- **Source**: Contains the IP address of the device that initiated the attack, if known.
- **Destination**: Contains the destination IP address of the attack, or rather the device that the attack was intended for, if known.
- **Time**: Contains a date and time stamp for IMC’s detection of the attack.
- **Correlated Policy**: Contains the security control policy in IMC that is associated with the attack found in this attack alarm. If there is no security policy associated with the attack alarm, this field contains the value "Undefined."
- **Result**: Contains a status or summary of the result of any action IMC has taken to address the attack.
  - **Manual execution required** indicates that no action, either automatic or manual, was taken for the associated event.
  - **Success** indicates that the automatic or manual action that was taken for this type of attack was successful.
  - **Failure** indicates that the automatic or manual action that was taken for this type of attack failed.

2. Click **Manual execution required** in the Result field to navigate to the Attack Alarm Details page. From this page you can execute any actions that are associated with this attack alarm type.
   - **Success** indicates that the automatic or manual action that was taken for this type of attack was successful.
   - **Failure** indicates that the automatic or manual action that was taken for this type of attack failed.

3. Click **Failure** in the Result field to navigate to the Attack Alarm Details page. From this page you can get the detailed failure reason.
   - **Executing policy** indicates that the automatic or manual action that was specified for this type of attack is currently being executed. The contents of the Result field do not serve as a navigation link to the Attack Alarm Details page when an action is being executed.
   - **No matching policy** indicates that the alarm does not match any security control policy. Click **No matching policy** in the Result field to navigate to the Attack Alarm Details page. From this page you can select one or more actions, if available, that are associated with this attack alarm type.
Waiting for policy execution indicates that the selected action for the associated security attack alarm is in the queue for processing by IMC. The contents of the Result field do not serve as a navigation link to the Attack Alarm Details page when an action is waiting for policy execution.

Acknowledgement required indicates that the configured action could not be completed successfully because the conditions necessary to complete the action were not met. For example, let's say that the configured action was to shut down an interface. If the interface is unreachable and therefore cannot be shut down, the Result field contains the value, Acknowledgement required. The value, Acknowledgement required in the Result field serves as a link for navigating to page for re-executing the action manually.

The contents of the Result field serve as a link to one of several pages, depending on the result of the action taken for the associated event. If the result is Failure, the link navigates you to the Security Control Policy Result Report. For more information on this page, see "Viewing the execution result report" (page 815).

If the result is No matching policy, the link navigates you to the Execute Action page. For more information on executing an action, see "Executing a manual action for an attack alarm" (page 813).

Attack Path: This field contains a link to a topology map displaying the attack path.

4. Select the number of recent attack alarms you want IMC to display from the Display list located in the far right of the Realtime Attack Alarm List. This option filters the list for the most recent 25, 50, 75, 100, or 125 attack alarms.

Refresh the realtime attack alarm list

You can refresh the Realtime Attack Alarm List. Refreshing the Realtime Attack Alarm List initiates a query to IMC’s database and refreshes the Realtime Attack Alarm List with any changes to the Realtime Attack Alarm List since the page was last loaded.

To refresh the Realtime Attack Alarm List:

1. Navigate to Alarm→Realtime Attack Alarm:
   a. Click the Alarm tab from the tabular navigation system on the top.
   b. Click the Security Control Center on the navigation tree on the left.
   c. Click the Realtime Attack Alarm link located under Security Control Center on the navigation tree on the left.

      The Realtime Attack Alarm List displays in the main pane of the Realtime Attack Alarm page.

2. Click Refresh.

Deleting attack alarms from the realtime attack alarm

You can delete one or more attack alarms from the Realtime Attack Alarm List. Once an alarm is deleted, it is removed immediately from the IMC database and it cannot be recovered. Exercise this feature with caution.

To delete one or more attack alarms from the Realtime Attack Alarm List:

1. Navigate to Alarm→Realtime Attack Alarm:
   a. Click the Alarm tab from the tabular navigation system on the top.
b. Click the **Security Control Center** on the navigation tree on the left.

c. Click the **Realtime Attack Alarm** link located under **Security Control Center** on the navigation tree on the left.
   
The Realtime Attack Alarm List displays in the main pane of the Realtime Attack Alarm page.

2. Click the checkbox ☐ to the left of the attack alarms you want to delete.

3. Click **Delete**.

4. Click **OK** to confirm the deletion of the selected attack alarms.

**Viewing attacks through topology maps**

SCC displays attack alarms in the topology map, providing you with a choice of two visual displays of the locations and network devices, the **Attack Topology** and the **Attack Path**, where attacks have occurred and where security threats exist. The **Attack Topology** view provides you with a single topology map displaying the logical connections for all current attacks. Rendered on the **Attack Topology** map is the source and destination access devices and the originating device and its destination, if known. The **Attack Path** view provides you with a subset of what is shown on the **Attack Topology** view because it displays the physical connections between the source and destination for a single attack only.

**Viewing all attacks using the attack topology map**

To view all current attacks for the entire managed network:

1. Navigate to **Alarm**→**Browse Attack Alarm**:
   
a. Click the **Alarm** tab from the tabular navigation system on the top.

b. Click the **Security Control Center** on the navigation tree on the left.

c. Click the **Browse Attack Alarm** link located under **Security Control Center** on the navigation tree on the left.
   
The Attack Alarm List displays in the main pane of the Browse Attack Alarm page.

2. Click the **Attack Topology** link located in the upper right corner of the **Attack Alarm List**.
   
   A new browser window opens and the **Attack Topology** map displays in the active window.

3. To facilitate use and customization of the topology, the, **Attack Topology** map provides the following functions:
   
a. **Toolbar options**

   ![Toolbar options]

   The **Reload** button enables operators to reload the **Attack Topology** map once it has changed.
   
   All other buttons provides the same functions as they do of IMC’s Network Topology module. For more information on these buttons, see "Topology map toolbar" (page 182).

b. **Device monitoring via the left mouse click**

   Click the selected device on the **Attack Topology** map to display information about the selected device. The information displayed by a left mouse click varies based on the device selected.
For more information on the left mouse click for devices, see "Left & right mouse clicks: Monitoring & management" (page 183).

c. **Link monitoring via the left mouse click**

The term "link" here refers to a virtual path from the attack source to the attack destination, rather than a physical link.

For links, the left mouse click includes the following:

- **Alarm Name**: Contains the type of the attack alarm for the link.
- **Alarm Time**: Contains the time when the attack alarm was generated.
- **Source**: Contains the IP address of the attack source.
- **Destination**: Contains the IP address of the attack destination.

d. **Map configuring via the right mouse click**

Right mouse click menu options for the map are listed below:

- **Set Filter Condition**: Opens the page for setting the filter conditions. After setting the filter conditions, click OK to view the matched attacks.
- **Reload**: Refreshes the page. Once the attack topology map has changed, click Reload to view the changes.
- **Hand**: Enables operators to grab and move the topology view within the confines of the pane. To exit this mode, click in the toolbar.
- **Zoom**: Enables operators to zoom in or out of the topology view or to fit the contents of the topology map into the current window.

e. **Device configuring via the right mouse click**

Click the selected device on the attack topology map to display a list of management options that can be used to manage the selected device.

For more information on the right mouse click for devices, see "Left & right mouse clicks: Monitoring & management" (page 183).

f. **Link configuring via the right mouse click**

The term "link" here refers to a virtual path from the attack source to the attack destination, rather than a physical link.

For links, the right mouse click includes only the **Attack Path** option. This option opens the virtual link topology, which displays the physical links and devices in the virtual link.

**Viewing a single attack using the attack path map**

You can view the topology for a single attack using the **Attack Path** option that is available on both the **Attack Alarm List** and the **Realtime Attack Alarm list**.

To view the attack topology for a single attack from the **Attack Alarm List**:

1. Navigate to **Alarm→Browse Attack Alarm**:
   a. Click the **Alarm** tab from the tabular navigation system on the top.
   b. Click the **Security Control Center** on the navigation tree on the left.
   c. Click the **Browse Attack Alarm** link located under **Security Control Center** on the navigation tree on the left.
The **Attack Alarm List** displays in the main pane of the **Browse Attack Alarm** page.

2. Click the icon in **Attack Path** field for the attack alarm you want to view the attack path for. A new browser window opens and the **Attack Path** map displays in the active window. At the right of the page, the detailed attack path information is displayed, including:
   - **Alarm Name**: Contains the type of the attack alarm for the link.
   - **Alarm Time**: Contains the time when the attack alarm was generated.
   - **Source**: Contains the IP address of the attack source.
   - **Destination**: Contains the IP address of the attack Destination.
   - **Access Device IP of the Attack Source**: Contains the IP address of the access device that the attack source connects to, if known.
   - **Access Device Port of the Attack Source**: Contains the interface description of the access device that the attack source connects to, if known.
   - **Access Device IP of the Attack Destination**: Contains the IP address of the access device that the attack destination connects to, if known.
   - **Access Device Port of the Attack Destination**: Contains the interface description of the access device that the attack destination connects to, if known.

3. To facilitate use and customization of the topology, the **Attack Path** map provides the following functions.
   a. **Toolbar options**
      
      The **Reload** button enables operators to reload the **Attack Path** map once it has changed. All other buttons provides the same functions as they do of IMC's Network Topology module. For more information on these buttons, see “Topology map toolbar” (page 182).

   b. **Device and link monitoring via the left mouse click**
      
      Click to select a device or link on the **Attack Path** map to display information about the selected device or link. The information displayed by a left mouse click varies based on the device or link selected.

      For more information on the left mouse click for devices or links, see "Left & right mouse clicks: Monitoring & management" (page 183).

   c. **Device configuring via the right mouse click**
      
      Click to select a device on the attack path map to display a list of management options that can be used to manage the selected device.

      For more information on the right mouse click for devices, see "Left & right mouse clicks: Monitoring & management" (page 183).

   d. **Link configuring via the right mouse click**
      
      Click to select a link on the topology map to display a list of management options that can be applied to the selected link.

      The right mouse click on the selected link includes one or more of the following management options for links:
- **Link Information**: Provides operators with detailed information on the selected link, including basic information as well as information about the interfaces on either side of the link. Information includes link name, status, device information, the operational and administrative status of each interface, IP address and subnet information and more.

- **Modify Link Name**: Allows operators to apply a label or name in IMC for the selected link.

- **View MAC**: Provides two options, **Interface 1** and **Interface 2**, which represent the interfaces at both ends of the link. Select **Interface 1** or **Interface 2**, a new browser window opens and the MAC addresses learned on the selected interface is displayed in the active window.

## Executing an action for an attack alarm

You can take action on attack alarms displayed in the **Attack Alarm List** or the **Realtime Attack Alarm List**. The actions that can be taken vary by the type of security attack identified but in general SCC supports six actions:

- Shutting down the access port
- Alerting the administrator by email
- Isolating the online user to a restricted network
- Sending a warning message to the online user
- Kicking the online user off
- Adding the online user to the blacklist

The **Execute Action** page for initiating an action for a security alarm can be accessed from the link in the **Result** field of the **Attack Alarm List** and the **Realtime Attack Alarm List** when the **Result** field contains one of the following values, **Manual execution required**, **No matching policy**, and **Acknowledgement required**.

### Executing a manual action for an attack alarm

You can execute a manual action for an attack alarm from both the **Attack Alarm List** and the **Realtime Attack Alarm list**.

To execute a manual action from the **Attack Alarm List**:  
1. Navigate to **Alarm→Browse Attack Alarm**:
   a. Click the **Alarm** tab from the tabular navigation system on the top.
   b. Click the **Security Control Center** on the navigation tree on the left.
   c. Click the **Browse Attack Alarm** link located under **Security Control Center** on the navigation tree on the left.

   The **Attack Alarm List** displays in the main pane of the **Browse Attack Alarm** page.

2. Click the link in the **Result** field of the attack alarm for which you want to view details.

   The **Execute Action** page appears.

   The value in the **Result** field must contain one of the following values in order to execute an action manually: **Manual execution required**, **No matching policy**, and **Acknowledgement required**.

3. Click **Select Action** located at the top of the **Action and Order** section of the **Execute Action** page.

   The **Select Action** dialog box appears.
4. To view the full list of possible actions for this security attack type, do one of the following:
   - Click on the Expand arrow located to the left of Action List, or
   - Click on the Expand all link located in the upper right corner of the Select Action dialog box.

5. Click the checkboxes to the left of the actions you want to execute. The actions that are available vary by attack alarm type.

6. Click OK.

7. To add another action, repeat Step 4 and Step 5.
   Some actions may have parameters that must be configured before IMC can execute them. If they do, the Configure icon displays in the Configure Parameters field of the associated action in the Action and Order list.

8. Click the Configure icon to configure the parameters for the associated action. You are prompted to configure any parameters that have not been configured before you can execute the action you have configured.

9. For the Email action, enter the following configuration parameters in the Parameter configurations for mail sender dialog box:
   - Destination Mail Address: Enter the fully qualified email address of the recipient of this email alert in the Destination Mail Address field.
   - Mail Subject: Enter a brief subject for this email in the Mail Subject field.
   - Mail Content: Enter the content that you want to appear in the main body of the email in the Mail Content field.

10. Click OK.

11. For the Warn action, enter the following configuration parameters in the Send Message dialog box.

12. Enter the message that you want to appear on the online user’s browser in the Send Message field. The message length is limited 60 characters.

13. Click OK to send the message to the online user.

   For the Warn option to become visible as an action, the User Access Manager module must be installed and the attack alarm must contain the source IP or source MAC address.

   If you have entered more than one action in the Action and Order list, you can specify the order in which IMC executes them. Otherwise, IMC performs the actions in the order in which they were created.

14. To re-order actions, do one of the following:
   - Click the up arrow key to move an action up in order of execution, or
   - Click the down arrow key to move an action down in order of execution.

15. Click the Delete icon to delete an action from the Action and Order list.

16. When you have completed the configuration of all actions and you are ready to have IMC execute the actions, click Execute.
17. Click **Back** to return to the **Attack Alarm List** and to view the results of the actions you have executed. The results display in the **Result** field. The **Result** field contents also serve as a link to the **Execution Result Report** that displays more detailed information about the actions taken. For more information on the **Execution Result Report**, see “Viewing the execution result report” (page 815).

**Viewing the execution result report**

You can view the **Execution Result Report** from either the **Attack Alarm List** or the **Realtime Attack Alarm list**. To view the results of an action from the **Attack Alarm List**:

1. Navigate to **Alarm → Browse Attack Alarm**:
   a. Click the **Alarm** tab from the tabular navigation system on the top.
   b. Click the **Security Control Center** on the navigation tree on the left.
   c. Click the **Browse Attack Alarm** link located under **Security Control Center** on the navigation tree on the left.

   The **Attack Alarm List** displays in the main pane of the **Browse Attack Alarm** page.

2. Click the link in the **Result** field of the attack alarm for which you want to view details.

   The **Result Report** page appears.

   IMC displays the results of every action configured for the attack alarm in the **Execution Result List** displayed in the lower portion of the **Security Control Policy Result Report**.

**Execution result list**

- **Action Name**: Contains the name of the action that was executed.
- **Action Description**: Contains a description for the action that was taken.
- **Result**: Contains the result of the action.
- **Result Description**: Contains more detailed information about the outcome of the result, including a possible cause if known.
- **Restored**: Contains information about whether or not the action can be undone or restored. The contents of this field serve as a link for restoring conditions prior to the execution of an action. For example, if the action taken was to shut down an interface, restoring the action brings the interface up.
- **Result**: Contains a result for the restore action. This field is empty if no restore action was taken.
- **Result Description**: Contains more detailed information about the outcome of the restore result, including a possible cause if known. This field is empty if no restore action was taken.

3. Click **Refresh** located at the top of the **Execution Result List** to query IMC for any updates to the **Execution Result List**.

4. Click **Back** to return to the **Attack Alarm List**.

**Managing security control policies**

You can proactively manage the response to security threats and attacks using security control policies. A security control policy combines three key pieces of information: 1) the identification and alarming of a security attack; 2) an action that can be taken in response to the security attack; and 3) identification of the
portion of the network to be protected by the security control policy. The actions configured for security control policies can be executed manually or they can be configured to run automatically upon detection of the security attack.

Viewing the security control policy list

The Security Control Policy List provides you with a list of all configured security control policies in IMC. From this list, you can view the policy names, descriptions, and execution types for each policy. From this list, you can also modify and delete security control policies.

To view the Security Control Policy List:

1. Navigate to Alarm → Security Control Policy:
   a. Click the Alarm tab from the tabular navigation system on the top.
   b. Click the Security Control Center on the navigation tree on the left.
   c. Click the Security Control Policy link located under Security Control Center on the navigation tree on the left.


Security control policy list

- **Policy Name**: Contains the name of the security control policy. This field contains a link to the Security Control Policy Details page that contains more detailed information on the associated security control policy.
- **Policy Description**: Contains a description for the association security control policy.
- **Execution Type**: Contains the type of action for the associated security control policy. Possible values include Manual for actions that can be executed manually and Auto for actions that can be executed automatically.
- **Modify**: Contains an icon for modifying the associated security control policy.
- **Delete**: Contains an icon for deleting the associated security control policy.

⚠️ **WARNING:**

You can sort the Security Control Policy List by the Policy Name, Policy Description, and Execution Type fields by clicking the column label to sort the list by the selected field. The column label is a toggle switch that allows you to toggle between the various sort options specific to each field.

Adding a security control policy

To add a security control policy:

1. Navigate to Alarm → Security Control Policy:
   a. Click the Alarm tab from the tabular navigation system on the top.
   b. Click the Security Control Center on the navigation tree on the left.
c. Click the Security Control Policy link located under Security Control Center on the navigation tree on the left.


2. Click Add.


3. Enter the name for this policy in the Policy Name field.

The maximum length for a policy name is 32 characters.

4. Enter a brief description for this policy in the Policy Description field.

5. Select the type of execution you want to apply to this policy from the Execution Type list:
   - Select Auto if you want IMC to apply this policy automatically when a matching security attack is detected, or
   - Select Manual if you want to apply this policy manually when a matching security attack is detected.

6. Click Select Event to the right of the Event to Process field to select the type of security attack you want to define this policy control event for.

The Select Attack Alarm dialog box appears.

7. Do one of the following:
   - To view the list of possible event types under each attack alarm group, click the Expand arrow located to the left of the attack alarm group name, or
   - To view all attack alarm groups, click Expand all link located in the upper right corner of the Select Attack Alarm dialog.

8. Click the radio button to the left of the attack alarm type you want to create this security control policy for.

9. Click OK.

The security event you selected for processing displays in the Event to Process field.

10. If you want to apply this security control policy to the entire network, click the checkbox to the left of Set it as the default policy to take effect on the whole network. If you select this option, skip to Step 12.

11. If you want to specify the IP address range to apply this security control policy to, enter the first IP address for the IP address range you want to apply this security control policy to in the Start IP field.
   - Enter the last IP address for the IP address range you want to apply this security control policy to in the End IP field.
   - Click Add to add the IP address range to the Configured Segments list.
   - To add more IP address ranges, repeat Step 11 for each IP address range you want to add.

12. Click Select Action located at the top of the Action and Order section.

The Select Action dialog box appears.

13. To view the full list of possible actions for this security attack type:
   - Click the Expand arrow located to the left of Action List, or
Click the Expand all link located in the upper right corner of the Select Action dialog box.

14. Click the checkboxes to the left of the actions you want to execute. Actions that are available vary by attack alarm type.

15. Click the checkbox to the right of the Action List to select all Actions.

The IMC base platform supports the following actions:
- **Shut down port**: Shut down the access port.
- **Email**: Alert the administrator by email.

For organizations that have also deployed IMC’s User Access Manager module, the following actions are also supported:
- **Isolate**: Isolate the online user to a restricted network.
- **Warn**: Send a warning message to the online user.
- **Kick off**: Kick the online user off.
- **Blacklist**: Add the online user to the blacklist.

For these four options to become visible as actions, the User Access Manager module must be installed and the attack alarm must contain the source IP or source MAC address.

Actions that IMC displays in the Select Action dialog box vary based on the type of attack, as not all actions are available for all attack types.

16. Click OK.

17. To add another action, repeat Steps 13 through 14.

18. Some actions may have parameters that must be configured before IMC can execute them. If they do, the Configure icon displays in the Configure Parameters field of the associated action in the Action and Order list.

19. Click the Configure icon to configure the parameters for the associated action. You are prompted to configure any parameters that have not been configured before you can create the security control policy.

   a. For the Email action, enter the following configuration parameters in the Parameter configurations for mail sender dialog box.

      - **Destination Mail Address**: Enter the fully qualified email address of the recipient of this email alert in the Destination Mail Address field.
      - **Mail Subject**: Enter a brief subject for this email in the Mail Subject field.
      - **Mail Content**: Enter the content that you want to appear in the main body of the email in the Mail Content field.

   b. Click OK.

   c. For the Warn action, enter the following configuration parameters in the Send Message dialog box.

      - Enter the message that you want to appear on the online user’s browser in the Send Message field. Note that message length is limited to 60 characters.

   d. Click OK to send the message to the online user.
20. If you have entered more than one action in the Action and Order list, you can specify the order in which IMC executes them
   - Click the up arrow key to move an action up in order of execution, or
   - Click the down arrow key to move an action down in order of execution, or
   - Click the Delete icon to delete one or more actions from the Action and Order list.
21. Click OK to create the security control policy.

Modifying a security control policy

To modify a security control policy:

1. Navigate to Alarm → Security Control Policy:
   a. Click the Alarm tab from the tabular navigation system on the top.
   b. Click the Security Control Center on the navigation tree on the left.
   c. Click the Security Control Policy link located under Security Control Center on the navigation tree on the left.


2. Click the Modify icon associated with the security control policy you want to modify.

   The Modify Security Control Policy page appears.

3. Modify the name for this policy in the Policy Name field as needed.

   The maximum length for a policy name is 32 characters.

4. Modify the description for this policy in the Policy Description field.

5. Change the type of execution you want to apply to this policy by making a new selection from the Execution Type list.
   - Select Manual if you want to apply this policy manually when a matching event arises, or
   - Select Auto if you want IMC to apply this policy automatically when a matching event arises.

6. Click Select Event to the right of the Event to Process field to select the type of security attack you want to define this policy control event for.

   **WARNING:** Changing the event or attack alarm type deletes all actions previously configured.

   The Select Attack Alarm dialog box appears.

7. To view the list of possible event types under each attack alarm group,
   - Click the Expand arrow located to the left of the attack alarm group name, or
   - Click the Expand all link located in the upper right corner of the Select Attack Alarm dialog box to expand all attack alarm groups.
a. Click the radio button □ to the left of the attack alarm you want to create this security control policy for.

b. Click OK.

The results of your selection display in the Event to Process field.

8. If you want to apply this security control policy to the entire network, click the checkbox □ to the left of Set it as the default policy to take effect on the whole network. If you select this option, skip to Step 9.

9. To add more IP address ranges, enter the first IP address for the IP address range you want to apply this security control policy to in the Start IP field.

a. Enter the last IP address for the IP address range you want to apply this security control policy to in the End IP field.

b. Click Add to add the IP address range to the Configured Segments list.

c. To add more IP address ranges, repeat Step 9 for each IP address range you want to add.

d. To delete an IP address range, click the IP address range you want to delete.

e. Click Delete located to the right of the Configured Segments field.

10. If you selected a new attack alarm or event type to process, re-enter all actions for this policy.

To do so, click Select Action located at the top of the Action and Order section.

The Select Action dialog box appears.

11. To view the full list of possible actions for this security attack type:

   o Click the Expand arrow located to the left of Action List, or
   o Click the Expand all link located in the upper right corner of the Select Action dialog box.

12. Click the checkboxes □ to the left of the actions you want to execute.

The actions available vary by attack alarm type.

13. Click the checkbox □ to the right of the Action List to select all Actions.

14. Click OK.

15. To add another action, repeat Steps 10 through 12.

Some actions may have parameters that must be configured before IMC can execute them. If they do, the Configure icon displays in the Configure Parameters field of the associated action in the Action and Order list.

16. Click the Configure icon to configure the parameters for the associated action.

You are prompted to configure any parameters that have not been configured before you can save your modifications to the security control policy.

17. For the Email action, enter the following configuration parameters in the Parameter configurations for mail sender dialog box.

   o Destination Mail Address: Enter the fully qualified email address of the recipient of this email alert in the Destination Mail Address field.
   o Mail Subject: Enter a brief subject for this email in the Mail Subject field.
Mail Content: Enter the content that you want to appear in the main body of the email in the Mail Content field.

a. Click OK.

b. For the Warn action, enter the following configuration parameters in the Send Message dialog box.

c. Enter the message that you want to appear on the online user’s browser in the Send Message field. The message length is limited to 60 characters.

d. Click OK to send the message to the online user.

18. If you have entered more than one action in the Action and Order list, specify the order in which IMC executes them, by:

   o Click the up arrow key to move an action up in order of execution, or

   o Click the down arrow key to move an action down in order of execution, or

   o Click the Delete icon to delete one or more actions from the Action and Order list.

19. Click OK to accept the changes to the security control policy.

Deleting a security control policy

To delete a security control policy:

1. Navigate to Alarm → Security Control Policy:

   a. Click the Alarm tab from the tabular navigation system on the top.

   b. Click the Security Control Center on the navigation tree on the left.

   c. Click the Security Control Policy link located under Security Control Center on the navigation tree on the left.


2. Click the Delete icon associated with the security control policy you want to delete.

3. Click OK to confirm the deletion of the selected security control policy.

Executing a security control policy

SCC provides two options for executing a security control policy; automatic and manual. When the Auto option is selected in the configuration of a security control policy, IMC automatically executes the action when the matching security alarm is generated. For more information on configuring a security control policy to run automatically, see “Adding a security control policy” (page 816).

When the Manual option is selected in the configuration of a security control policy, IMC does not automatically execute the action when the matching security alarm is generated. Rather, the operator must navigate to the Execution Result Report and manually initiate the execution of the action when a matching event is detected and an alarm is generated in SCC. For more information on executing an action manually, see “Executing an action for an attack alarm” (page 813).
Viewing SCC reports

SCC provides you with a quick snapshot of security events from four perspectives for the last hour. Each of these four reports is described below.

1. Navigate to Alarm → Report:
   a. Click the Alarm tab from the tabular navigation system on the top.
   b. Click the Security Control Center on the navigation tree on the left.

   The four perspectives display in the main pane of the Report page.

Top 10 attack alarms report

The Top 10 Attack Alarms report provides you with a brief bar graph of the number of attacks summarized by attack type, as shown below.

Figure 41 Top 10 attack alarms

To hide this graph, click the Collapse icon located in the upper right corner of the graph.

To view a hidden graph, click the Expand icon located in the upper right corner of the graph.

Top 10 attack sources report

The Top 10 Attack Sources report provides you with a pie chart displaying the distribution of attacks by the attack source IP address.
Figure 42 Top 10 attack sources

To hide this graph, click the **Collapse** icon located in the upper right corner of the graph.

To view a hidden graph, click the **Expand** icon located in the upper right corner of the graph.

**Top 10 attack destinations report**

The *Top 10 Attack Destinations* report provides you with a pie chart displaying the distribution of attacks by the attack destination IP address.

Figure 43 Top 10 attack destinations

To hide this graph, click the **Collapse** icon located in the upper right corner of the graph.

To view a hidden graph, click the **Expand** icon located in the upper right corner of the graph.

**The execution results report**

The *Execution Result of Security Control Policy* report provides you with a pie chart displaying the distribution of execution results.
Integrating SCC with SMS

The Security Management System (SMS) software is designed for network security monitoring and management, enabling operators to obtain the status information and alarms from the security devices on the network and manage the entire network security status in real time.

For unified management, you can integrate SCC with SMS and enter the SMS management page in SCC to monitor the network-wide security devices.

Integrating SCC with SMS

SCC supports SMS 3.1.0.7607 and later versions.

SMS plug-in installation

1. Install the SMS plug-in.
2. Launch the CLI of the server installed with SCC, and go to the IMC installation directory `\iMC\client\bin\` directory.
3. Execute `installsms.bat`. For Linux operating systems, execute `./installsms.sh`.
4. Enter the IP address of the SMS plug-in in the `https://smsip` format.
5. Enter the username and password for the SMS administrator.

Figure 45 (page 825) shows an example of the SMS screen when the plug-in is successful installed.
6. Restart jserver.
7. Open the **Intelligent Deployment Monitoring Agent**, and click the **Process** tab.
8. Right-click the jserver process and select **Stop Process** from the shortcut menu.
9. When the jserver process stops, right-click the process, and select **Start Process** from the shortcut menu.

### The SMS management page in SCC

1. Navigate to **Alarm**→**SMS Management**:
   a. Click the **Alarm** tab from the tabular navigation system on the top.
   b. Click the **Security Control Center** on the navigation tree on the left.
   c. Click the **SMS Management** link located under **Security Control Center** on the navigation tree on the left.

   The **SMS Management** page appears.

**SMS list**

- **Device Label**: Contains the IMC name and the IP address for the SMS. The contents of the device label field serve as an active link for drilling down into the **Device Details** page.
- **IP Address**: Contains the IP address of SMS.
- **Operation**: Contains an active link. Click the link to display five actions: **Launch SMS Client**, **Display All Attack Alarms**, **Modify Login information**, **Display All Managed TP IPSs**, and **Display Report**. You can click any link to open the SMS management page, and view or edit information.

### SMS and managed devices in the topology

1. Navigate to **My Network View** topology:
   a. Click the **Resource** tab from the tabular navigation system on the top.
   b. Click **View Management** on the navigation tree on the left.
   c. Click **Network Topology** under **View Management** from the navigation system on the left.

   The topology window appears.

2. Click the expand icon 👉 to the left of **Custom Topology** from the navigation system on the left.
3. Click **My Network View**.

   The **My Network View** topology appears.

4. Click 🖼 in the toolbar at the top of the topology.

   At the right of the topology page, an SMS area is displayed, containing SMS entries and their IP addresses.

5. Click an SMS in the SMS area.
Then in the topology map, the SMS and the IPS devices managed by the SMS light up, and other devices are grayed out, as shown in Figure 46.

**Figure 46 An SMS and IPS devices managed by the SMS**

6. Right-click the SMS and select any of the following items from the shortcut menu:
   - **Open SMS Client**: Opens the SMS management page.
   - **Browse Events**: Views alarms collected by SMS.
   - **Browse Reports**: Views reports in the SMS.

7. Right-click an IPS device and select any of the following items from the shortcut menu:
   - **Open IPS Device**: Opens the IPS device and view its details.
   - **Browser IPS Events**: Views alarms generated on the IPS device.
12 VLAN management

With IMC, you have a convenient facility for managing VLANs globally or on a per device basis. With IMC’s **Global VLAN** option, you can simplify the process of creating standardized VLANs across devices in the infrastructure. Using the **Global VLAN** option, you can create VLANs and select from the list of all managed devices, which devices to add the VLAN to or remove the VLAN from.

With IMC’s **Batch Deploy** option, you can create and configure VLANs on one or more devices, including configuring access, trunk, or hybrid ports.

For individual device VLAN management, you can select the device they want to configure VLANs for. From the VLAN configuration page, you can configure a VLAN for the selected device as well as configure virtual interfaces, access ports, trunk ports, or hybrid ports for each VLAN.

In addition, you can view histories of VLAN management operations using IMC’s **VLAN Deployment Task** option.

Finally, with IMC’s **VLAN Topo** option, you can launch a network topology view that highlights devices for the selected VLAN and grays out devices that are not part of the VLAN. You can actively monitor and manage devices in the selected VLAN from the topology map.

Global VLAN management

IMC’s **Global VLAN** management feature makes it simple and easy to create standardized VLANs for one, some, or all devices in the network infrastructure. With the **Global VLAN** option, you can add a VLAN to all switches in the network simply by defining the VLAN ID, the VLAN name and by selecting the devices to add the VLAN to. In addition, you can easily add, modify or delete VLANs on selected devices.

Viewing the global VLAN list

The **Global VLAN List** provides you with a list of all VLANs configured on devices managed by IMC that IMC is aware of.

To view the VLANs in the network infrastructure:

1. Navigate to **VLAN Management** → **Global VLAN**:
   a. Click the **Service** tab from the tabular navigation system on the top.
   b. Click the **VLAN Management** on the navigation tree on the left.
   c. Click **Global VLAN** link located under **VLAN Management** on the navigation tree on the left.

   The global **VLAN List** appears.

**VLAN**

  o **VLAN ID**: Contains the ID for the associated VLAN.
  o **VLAN Name**: Contains the name for the associated VLAN.
  o **Include VLAN Interfaces**: Identifies whether or not the associated VLAN has a virtual interface configured for it.
  o **Member Operation**: Contains a link to the **VLAN Device List** for the associated VLAN.
The **VLAN ID** and **Member Operation** fields for VLAN 1 or VLAN 001 are grayed out because this VLAN serves as a management VLAN for most switch manufacturers. The **VLAN Device List**, which is accessed through the **Member Operation** link, is gray and unavailable because all devices are by default, a member of VLAN 1 or 001

- **Modify VLAN Name**: Contains a link for modifying the name of the associated VLAN.

If the **VLAN List** contains multiple entries, the following navigational aids may appear:

- Click to page forward in the **VLAN List**.
- Click to page forward to the end of the **VLAN List**.
- Click to page backward in the **VLAN List**.
- Click to page backward to the front of the **VLAN List**.

2. Click 8, 15, 50, 100, or 200 from the right side of the main pane to configure how many items per page you want to view.

3. Click **Refresh** to reload this web page.

4. You can sort the **VLAN List** can by **VLAN ID**, **VLAN Name**, and **Include VLAN Interfaces** fields by clicking the column label to sort the list by the selected field. The column label is a toggle switch that allows you to toggle between the various sort options specific to each field.

## Global VLAN query

Using the global or **Overall VLAN Query** option, you can quickly identify which devices have a specific VLAN configured on it. You can search by VLAN ID or VLAN name.

1. Navigate to **VLAN Management**→**Global VLAN**:
   a. Click the **Service** tab from the tabular navigation system on the top.
   b. Click the **VLAN Management** on the navigation tree on the left.
   c. Click **Global VLAN** link located under **VLAN Management** on the navigation tree on the left.

   The global **VLAN List** appears.

2. Move the pointer over **Query** at the upper right corner of VLAN list, and a search criteria dialog box appears.

3. Enter one or both of the following search criteria:
   - **VLAN ID**: Enter a partial or complete VLAN ID for the VLAN you wish to locate in the **VLAN ID** field.
   - **VLAN Name**: Enter a partial or complete name for the VLAN you wish to locate in the **VLAN Name** field.

   The result of your query displays in the **VLAN List**.

4. Click **Reset** to restore the **VLAN List**.

## Creating a global VLAN

With the **Global VLAN** feature in IMC, you can create a VLAN and add it to one or more devices.

To create a global VLAN:

1. Navigate to **VLAN Management**→**Global VLAN**:
a. Click the **Service** tab from the tabular navigation system on the top.
b. Click the **VLAN Management** on the navigation tree on the left.

c. Click the **Global VLAN** link located under **VLAN Management** on the navigation tree on the left.

The global VLAN List appears.

2. Click **Add**.

3. Enter the ID for this VLAN in the **VLAN ID** field. A valid range for a VLAN ID is 2-4094.

4. Enter the name for this VLAN in the **VLAN Name** field.

   Question marks (?) and non-ASCII characters are not permitted in VLAN names. Maximum length is 32 characters.

5. Click **Add** to select the devices to which you add to the VLAN.

6. Add devices by using either the **View** or **Advanced** query option. See "Adding devices by View" (page 85) and "Adding devices by Advanced query" (page 85).

7. Click **Submit**.

8. Review the results of the VLAN creating task by reviewing the **Adding global VLAN Summary Report** that display upon completion of the task.

   Once you have created the VLAN and added devices to it as you have completed in the previous steps, you must then add ports from the selected devices to the VLAN. For more information on adding ports to VLAN, see "VLAN device management" (page 830).

### Deleting a global VLAN

With the **Global VLAN** feature in IMC, you can also remove one or more VLANs from one, some, or all devices on the VLAN’s device list with just a few clicks.

To remove a VLAN from all devices in the VLAN’s device list:

1. Navigate to **VLAN Management** → **Global VLAN**:
   a. Click the **Service** tab from the tabular navigation system on the top.
   b. Click the **VLAN Management** on the navigation tree on the left.

   c. Click the **Global VLAN** link located under **VLAN Management** on the navigation tree on the left.

   The global VLAN List appears.

2. Click the checkboxes [ ] to the left of the VLANs that you want to remove.

3. Click **Delete**.

4. Click **OK** to confirm deletion of the selected VLANs.

### Adding devices to a global VLAN

Once you have created a global VLAN, you can then use the **Global VLAN** option to add it to one or more devices.

To add a VLAN to one or more devices:

1. Navigate to **VLAN Management** → **Global VLAN**:
   a. Click the **Service** tab from the tabular navigation system on the top.
   b. Click the **VLAN Management** on the navigation tree on the left.
c. Click **Global VLAN** link located under **VLAN Management** on the navigation tree on the left. The global **VLAN List** appears.

2. Click the **Member Operation** link associated with the VLAN you want to add devices to.
3. Click **Add**.
4. Add devices by using either the **View** or **Advanced** query option. See "Adding devices by View" (page 85) and "Adding devices by Advanced query" (page 85).
5. Click **Submit** to add the selected devices to the VLAN.

Once you have added the VLAN to devices, you can then add individual ports to the VLAN on each device. For more information on adding individual ports to a VLAN on a particular device, see "VLAN device management" (page 830).

### Deleting a VLAN from devices

You can also easily remove a VLAN from one or more devices using the **Global VLAN** feature.

To delete a VLAN from one or more devices:

1. Navigate to **VLAN Management**→**Global VLAN**:
   a. Click the **Service** tab from the tabular navigation system on the top.
   b. Click the **VLAN Management** on the navigation tree on the left.
   c. Click **Global VLAN** link located under **VLAN Management** on the navigation tree on the left. The global **VLAN List** appears.
2. Click the **Member Operation** link associated with the global VLAN you want to remove from devices.
3. Click the checkbox □ to the left of the devices you want to remove the VLAN from.
4. Click **Delete**.
5. Click **OK** to confirm deletion of the VLAN from the selected devices.

### VLAN device management

IMC offers you a convenient facility for managing VLANs on the selected device, allowing you to select the device to configure VLANs for. From the VLAN configuration page, you can configure a VLAN for the selected device as well as configure virtual interfaces, access ports, trunk ports, or hybrid ports for each VLAN.

### Viewing the VLAN device list

The **VLAN Device List** displays all devices that IMC can manage VLANs for. Devices that are VLAN capable but do not appear on this list are devices that use a proprietary VLAN protocol. IMC supports the 802.1q standard for VLANs.

To view devices that IMC can manage VLANs for:

1. Navigate to **VLAN Management**→**VLAN Devices**:
   a. Click the **Service** tab from the tabular navigation system on the top.
   b. Click the **VLAN Management** on the navigation tree on the left.
c. Click VLAN Devices link located under VLAN Management on the navigation tree on the left. The VLAN Device List appears.

VLAN device list

- **Device Status:** Contains the most current status of the device. Status is determined by the highest severity or alarm level for the device, when a device has more than one current alarm that has not been cleared or recovered. Device icons with the color gray denote that the device is unmanaged.
- **Device Name:** Contains the IMC name for the device, which, by default, is the name assigned to it in its device configuration. If the device is configured with a sysName, IMC uses this as the Device Name unless a Device Name has been manually configured, and contains the IP address of the device.
- **Device Type:** Contains the device series information for the associated device.
- **VLAN:** Displays all VLAN IDs added to the device.
- **VLAN Configuration:** Contains a link to configure VLANs for the associated device.

If the VLAN Device List contains multiple entries, the following navigational aids may appear:

- Click to page forward in the VLAN Device List.
- Click to page forward to the end of the VLAN Device List.
- Click to page backward in the VLAN Device List.
- Click to page backward to the front of the VLAN Device List.

2. Click 8, 15, 50, 100, or 200 from the right side of the main pane to configure how many items per page you want to view.

3. Click the checkbox to the left of a device and click Synchronize. IMC queries the device for the most current VLAN configuration for the selected devices.

4. Click Refresh to reload the web page.

You can sort the VLAN Device List by all fields with the exception of the VLAN Configuration and VLAN field by clicking the column label to sort the list by the selected field. The column label is a toggle switch that allows you to toggle between the various sort options specific to each field.

**Query device**

To query a device:

1. Navigate to VLAN Management→VLAN Devices:
   a. Click the Service tab from the tabular navigation system on the top.
   b. Click the VLAN Management on the navigation tree on the left.
   c. Click VLAN Devices link located under VLAN Management on the navigation tree on the left. The VLAN Device List appears.

2. Move the pointer over Query at the upper right corner of VLAN Device list, and a search criteria dialog box appears.

3. Enter the following search criteria:
Device Name: Enter a partial or complete device name for the device you wish to locate in the Device Name field.

The result of your query displays in the VLAN Device List.

4. Click Reset to restore the VLAN Device List.

VLAN device details

The VLAN Device page enables you to view and configure many facets of a VLAN on the selected device. There are five tabs on the VLAN Devices page. Each tab provides you with VLAN viewing and configuration options.

- Device VLAN
- Virtual Interface
- Access Port
- Trunk Port
- Hybrid Port

To access the VLAN details for a particular device:

1. Navigate to VLAN Management → VLAN Devices:
   a. Click the Service tab from the tabular navigation system on the top.
   b. Click the VLAN Management on the navigation tree on the left.
   c. Click VLAN Devices link located under VLAN Management on the navigation tree on the left. The VLAN Device List appears.

2. To view or configure VLAN details for an individual device, click the VLAN Configuration link associated with the device you want to view or configure.

   Information for the selected device is displayed in the upper portion of the page. This information includes Device Type, Device IP, Device Status, and IP Mask.

   There are also five tabs for managing various aspects of VLANs for the selected device: Device VLAN, Virtual Interface, Access Port, Trunk Port, and Hybrid Port. The VLAN Devices tab enables you to view, add, and delete VLANs for the selected device.

Viewing VLANs

To view the VLANs for a specific device:

1. Navigate to VLAN Management → VLAN Devices → Device Name.
   a. Click the Service tab from the tabular navigation system on the top.
   b. Click the VLAN Management on the navigation tree on the left.
   c. Click VLAN Devices link located under VLAN Management on the navigation tree on the left. The Device VLAN List appears.

2. Click the VLAN Configuration link associated with the device to which you want to view VLANs for.

   Five tabs for managing VLANs for the selected device display in the below the device information.

3. Click the Device VLAN tab.
Details for the VLANs display in the VLAN list for the selected device.

- **VLAN ID**: Contains the VLAN ID.
- **VLAN Name**: Contains the name of the VLAN.
- **Allowed Port List**: Contains a link to the list of ports assigned to the associated VLAN.
- **Modify VLAN Name**: Contains a link for modifying the name of the associated VLAN.
- **Virtual Interface List**: Contains a link for modifying the virtual interface of the associated VLAN.

If the **Device VLAN List** contains multiple entries, the following navigational aids may appear:

- Click to page forward in the **Device VLAN List**.
- Click to page forward to the end of the **Device VLAN List**.
- Click to page backward in the **Device VLAN List**.
- Click to page backward to the front of the **Device VLAN List**.

4. Click 8, 15, 50, 100, or 200 from the right side of the main pane to configure how many items per page you want to view.

5. For device VLAN lists that have more than one page, click on 1, 2, 3, 4, 5, 6, 7, 8, 9, 10… from the bottom right side of the main pane to jump to a particular page of the list.

You can sort the **Device VLAN List** by the **VLAN ID** and **VLAN Name** fields by clicking the column label to sort the list by the selected field. The column label is a toggle switch that allows you to toggle between the various sort options specific to each field.

### Creating a VLAN

To create a VLAN on a specific device:

1. Navigate to **VLAN Management** → **VLAN Devices** → **Device Name**:
   a. Click the **Service** tab from the tabular navigation system on the top.
   b. Click the **VLAN Management** on the navigation tree on the left.
   c. Click **VLAN Devices** link located under **VLAN Management** on the navigation tree on the left. The **Device VLAN List** appears.

2. To access the VLAN configuration page, click the **VLAN Configuration** link associated with the device to which you want to add a VLAN.

3. Click the **Device VLAN** tab.

4. Click **Add**.

5. Enter the ID for this VLAN in the **VLAN ID** field.
   A valid range is 2 – 4094. **VLAN 1** has special significance and therefore is not a valid VLAN ID option.

6. Enter the name for this VLAN in the **VLAN Name** field.
   Question marks (?) and non-ASCII characters are not permitted in VLAN names. The maximum length is 32 characters.

7. Click **Submit**.

8. Verify that the VLAN you have just configured now appears in the **VLAN List**.
Modifying a VLAN

To modify an existing VLAN:

1. Navigate to VLAN Management→VLAN Devices→Device Name:
   a. Click the Service tab from the tabular navigation system on the top.
   b. Click the VLAN Management on the navigation tree on the left.
   c. Click VLAN Devices link located under VLAN Management on the navigation tree on the left. The VLAN Device List appears.

2. Click the VLAN Configuration link associated with the device on which you want to modify an existing VLAN.

3. Click the Device VLAN tab.

4. Click the Modify VLAN Name field associated with the VLAN you want to modify.

5. Delete the contents of the VLAN name field. Enter the new VLAN name.

6. Click Submit.

7. Verify that the VLAN name you have just modified now appears in the VLAN List.

Deleting a VLAN

To delete a VLAN:

1. Navigate to VLAN Management→VLAN Devices→Device Name:
   a. Click the Service tab from the tabular navigation system on the top.
   b. Click the VLAN Management on the navigation tree on the left.
   c. Click VLAN Devices link located under VLAN Management on the navigation tree on the left. The VLAN Device List appears.

2. Click the VLAN Configuration link associated with the device on which you want to modify an existing VLAN.

3. Click the Device VLAN tab.

4. Click the checkbox to the left of the VLANs you want to delete. Note that VLAN 1 has special significance and cannot be deleted.

5. Click Delete.

6. Click OK to confirm deletion of the selected VLANs.

7. Verify that the VLANs you selected been removed from the Device VLAN list.

Virtual interface tab

You can assign one virtual interface to a VLAN using the features found under the Virtual Interface tab of the VLAN Devices page. The Virtual Interface tab option is available only for devices that support virtual interfaces.

Viewing virtual interface

To view the virtual interfaces for a specific switch:

1. Navigate to VLAN Management→VLAN Devices→Device Name:
a. Click the Service tab from the tabular navigation system on the top.
b. Click the VLAN Management on the navigation tree on the left.
c. Click VLAN Devices link located under VLAN Management on the navigation tree on the left. The Device VLAN List appears.

2. Click the VLAN Configuration link associated with the device to which you want to view virtual interfaces for.

3. Click the Virtual Interface tab.
Details for all virtual interfaces for the selected device display in the Virtual Interface List.

**Virtual interface**
- **VLAN ID**: Contains ID of the VLAN.
- **IP Address Type**: Contains the IP address Type of the virtual interface, including Primary IP and Sub IP. You can add multiples sub IP addresses for one primary IP address. The Sub IP option is only available for the device that supports sub IP addresses.
- **IP Address**: Contains the IP address of the virtual interface.
- **Mask**: Contains the IP subnet mask for the virtual interface.

If the Device VLAN List contains multiple entries, the following navigational aids may appear:

- Click to page forward in the Virtual Interface List.
- Click to page forward to the end of the Virtual Interface List.
- Click to page backward in the Virtual Interface List.
- Click to page backward to the front of the Virtual Interface List.

4. Click 8, 15, 50, 100, or 200 from the right side of the main pane to configure how many items per page you want to view.

5. For lists that have more than one page, click on 1, 2, 3, 4, 5, 6, 7, 8, 9, 10… from the bottom right side of the main pane to jump to a particular page of the list.

You can sort the Virtual Interface List by all fields, by clicking the column label to sort the list by the selected field. The column label is a toggle switch that allows you to toggle between the various sort options specific to each field.

**Adding a virtual interface**

To add a virtual interface to a specific switch:

1. Navigate to VLAN Management→VLAN Devices→Device Name:
   a. Click the Service tab from the tabular navigation system on the top.
   b. Click the VLAN Management on the navigation tree on the left.
   c. Click VLAN Devices link located under VLAN Management on the navigation tree on the left. The Device VLAN List appears.

2. Click the VLAN Configuration link associated with the device to which you want to add a virtual interface to.
3. Click the Virtual Interface tab.
4. Click **Add**.
5. Select the VLAN ID that this interface belongs to from the **VLAN ID** list. The VLAN must exist before a virtual interface can be added to it. For more information on creating a VLAN, see "Creating a VLAN" (page 833).
6. Select the IP address type from the **IP Address Type** list. The Sub IP option is only available for the device that supports sub IP addresses.
7. Enter the IP address for the virtual interface in the **IP Address** field.
8. Enter the IP subnet mask for the virtual interface in the **Mask** field. Masks can be entered using either CIDR or dotted decimal notation. For example, a valid subnet mask entry using CIDR notation would be 24 where 24 represents the number of bits allocated to the network portion of the address and implying that the remaining bits are allocated to the host portion. Alternatively, a valid subnet mask using dotted decimal notation would be 255.255.255.0
9. Click **Submit**.

**Deleting a virtual interface**

To delete one or more virtual interfaces from a specific switch:
1. Navigate to **VLAN Management**→**VLAN Devices**→**Device Name**:
   a. Click the **Service** tab from the tabular navigation system on the top.
   b. Click the **VLAN Management** on the navigation tree on the left.
   c. Click **VLAN Devices** link located under **VLAN Management** on the navigation tree on the left. The **Device VLAN List** appears.
2. Click the **VLAN Configuration** link associated with the device to which you want to add a virtual interface to.
3. Click the **Virtual Interface** tab.
4. Click the checkbox to the left of the virtual interfaces you want to delete.
5. Click **Delete**.
6. Click **OK** to confirm deletion of the selected virtual interfaces.

**Access port tab**

You can also move access ports between existing VLANs using the features found under the **Access Port** tab on the **VLAN Devices** page.

**Viewing access ports**

To view the access ports assigned to a VLAN for a specific switch:
1. Navigate to **VLAN Management**→**VLAN Devices** **Device Name**:
   a. Click the **Service** tab from the tabular navigation system on the top.
   b. Click the **VLAN Management** on the navigation tree on the left.
c. Click VLAN Devices link located under VLAN Management on the navigation tree on the left. The Device VLAN List appears.

2. Click the VLAN Configuration link associated with the device to which you want to view virtual interfaces for.

3. Click the Access Port tab.

Details for all ports for the selected device display in the Access Port List.

**Access port**

- **Port Status**: Contains the current status for the associated port.
- **Port Name**: Contains the port name.
- **PVID**: Contains the port VLAN ID of the VLAN.

If the Access Port List contains multiple entries, the following navigational aids may appear:

- Click to page forward in the Access Port List.
- Click to page forward to the end of the Access Port List.
- Click to page backward in the Access Port List.
- Click to page backward to the front of the Access Port List.

4. Click 8, 15, 50, 100, or 200 from the right side of the main pane to configure how many items per page you want to view.

5. For Access Port Lists that have more than one page, click on 1, 2, 3, 4, 5, 6, 7, 8, 9, 10… from the bottom right side of the main pane to jump to a particular page of the list.

You can sort the Access Port List by all fields by clicking the column label to sort the list by the selected field. The column label is a toggle switch that allows you to toggle between the various sort options specific to each field.

**Modify PVID**

To modify one or more port's PVID:

1. Navigate to VLAN Management → VLAN Devices → Device Name:
   a. Click the Service tab from the tabular navigation system on the top.
   b. Click the VLAN Management on the navigation tree on the left.
   c. Click VLAN Devices link located under VLAN Management on the navigation tree on the left. The Device VLAN List appears.

2. Click the VLAN Configuration link associated with the device to which you want to view access ports for.

3. Click the Access Port tab.

Details for all ports for the selected device display in the Access Port List.

4. Click the checkboxes to the left of the ports you want to modify.

5. Click the Modify PVID button, the Modify PVID dialog appears.
6. Select the VLAN ID from the PVID list. Only VLANs that exist in IMC and have been added to the device can be displayed in the list.

7. Click OK.

8. Review the results of the change by clicking the Allowed Port List for the associated VLAN under the Device VLAN tab.

Trunk port tab

You can also view and configure trunk ports for a VLAN using the features available under the Trunk Port tab of the VLAN Devices page.

Viewing trunk ports

To view the trunk ports assigned to a VLAN:

1. Navigate to VLAN Management → VLAN Devices → Device Name:
   a. Click the Service tab from the tabular navigation system on the top.
   b. Click the VLAN Management on the navigation tree on the left.
   c. Click VLAN Devices link located under VLAN Management on the navigation tree on the left. The Device VLAN List appears.

2. Click the VLAN Configuration link associated with the device to which you want to view virtual interfaces for.

3. Click the Trunk Port tab.
   Details for all ports for the selected device display in the Trunk Port List.

Trunk port

- **Port Status**: Contains the current status for the associated port.
- **Port Name**: Contains the port name.
- **PVID**: Contains the default VLAN ID of this trunk port.
- **Allowed VLAN**: Contains the list of VLANs permitted for this trunk port.
- **Modify**: Contains a link for modifying the associated trunk port.

If the Trunk Port List contains multiple entries, the following navigational aids may appear:

- Click to page forward in the Trunk Port List.
- Click to page forward to the end of the Trunk Port List.
- Click to page backward in the Trunk Port List.
- Click to page backward to the front of the Trunk Port List.

4. Click 8, 15, 50, 100, or 200 from the right side of the main pane to configure how many items per page you want to view.

5. For Port Trunk Lists that have more than one page, click on 1, 2, 3, 4, 5, 6, 7, 8, 9, 10... from the bottom right side of the main pane to jump to a particular page of the list.
You can sort the Port Trunk List by the Port Status, Port Name, PVID, and Permitted VLAN fields by clicking the column label to sort the list by the selected field. The column label is a toggle switch that allows you to toggle between the various sort options specific to each field.

Adding a trunk

To add a trunk port to a VLAN:

1. Navigate to VLAN Management→VLAN Devices→Device Name:
   a. Click the Service tab from the tabular navigation system on the top.
   b. Click the VLAN Management on the navigation tree on the left.
   c. Click VLAN Devices link located under VLAN Management on the navigation tree on the left. The Device VLAN List appears.

2. Click the VLAN Configuration link associated with the device to which you want to view trunk ports for.
3. Click the Trunk Port tab.
   Details for all ports for the selected device display in the Trunk Port List.
4. Click Add.
5. Select the port to be used for the trunk port from the Port Name list.
6. Enter the port VLAN ID for the trunk port in the PVID field.
7. Enter the permitted VLAN IDs for the trunk port in the Allowed VLAN field.
8. Click Submit.
9. View the results of this task in the Trunk Port List.

Modifying a trunk

To modify an existing trunk port:

1. Navigate to VLAN Management→VLAN Devices→Device Name:
   a. Click the Service tab from the tabular navigation system on the top.
   b. Click the VLAN Management on the navigation tree on the left.
   c. Click VLAN Devices link located under VLAN Management on the navigation tree on the left. The Device VLAN List appears.

2. Click the VLAN Configuration link associated with the device to which you want to view trunk ports for.
3. Click the Trunk Port tab.
   Details for all ports for the selected device display in the Trunk Port List.
4. Click the Modify icon associated with the trunk port you want to modify.
5. Select the port to be used for the trunk port from the Port Name list.
6. Modify the port VLAN ID for the trunk port in the PVID field.
7. Modify the permitted VLAN IDs for the trunk port in the Allowed VLAN field.
8. Click Submit.
9. View the results of this task in the Trunk Port list.
Deleting a trunk port

To delete an existing trunk port:

1. Navigate to **VLAN Management**→**VLAN Devices**→**Device Name**:
   a. Click the **Service** tab from the tabular navigation system on the top.
   b. Click the **VLAN Management** on the navigation tree on the left.
   c. Click **VLAN Devices** link located under **VLAN Management** on the navigation tree on the left. The **Device VLAN List** appears.

2. Click the **VLAN Configuration** link associated with the device to which you want to view trunk ports for.
3. Click the **Trunk Port** tab.
   Details for all ports for the selected device display in the **Trunk Port List**.

4. Click the checkbox ✅ to the left of the trunk ports that you want to delete.
5. Click **Delete**.
6. Click **OK** to confirm the deletion of the selected trunk ports.

Hybrid port tab

You can also view and configure hybrid ports for a VLAN using the features available under the **Hybrid Port** tab of the **VLAN Devices** page.

Viewing hybrid ports

To view the hybrid ports assigned to a VLAN:

1. Navigate to **VLAN Management**→**VLAN Devices**→**Device Name**:
   a. Click the **Service** tab from the tabular navigation system on the top.
   b. Click the **VLAN Management** on the navigation tree on the left.
   c. Click **VLAN Devices** link located under **VLAN Management** on the navigation tree on the left. The **Device VLAN List** appears.

2. Click the **VLAN Configuration** link associated with the device to which you want to view hybrid ports for.
3. Click the **Hybrid Port** tab.
   Details for all ports for the selected device display in the **Hybrid Port List**.

Hybrid port

- **Port Status**: Contains the current status for the associated port.
- **Port Name**: Contains the port name.
- **PVID**: Contains the port VLAN ID of the VLAN.
- **Tagged VLAN**: Contains the list of tagged VLANs for this port.
- **Untagged VLAN**: Contains the list of untagged VLANs for this port.
- **Modify**: Contains a link ✏ for modifying the associated hybrid port.
If the **Hybrid Port List** contains multiple entries, the following navigational aids may appear:

- Click 🔄 to page forward in the **Hybrid Port List**.
- Click 🔄 to page forward to the end of the **Hybrid Port List**.
- Click 🔄 to page backward in the **Hybrid Port List**.
- Click 🔄 to page backward to the front of the **Hybrid Port List**.

4. Click 8, 15, 50, 100, or 200 from the right side of the main pane to configure how many items per page you want to view.

5. For **Hybrid Port Lists** that have more than one page, click on 1, 2, 3, 4, 5, 6, 7, 8, 9, 10… from the bottom right side of the main pane to jump to a particular page of the list.

You can sort the **Hybrid Port List** by the Port Status, Port Name, PVID, Tagged VLAN, and Untagged VLAN fields by clicking the column label to sort the list by the selected field. The column label is a toggle switch that allows you to toggle between the various sort options specific to each field.

**Adding a hybrid port**

To add a hybrid port to a VLAN:

1. Navigate to **VLAN Management**→**VLAN Devices**→**Device Name**:
   - Click the **Service** tab from the tabular navigation system on the top.
   - Click the **VLAN Management** on the navigation tree on the left.
   - Click **VLAN Devices** link located under **VLAN Management** on the navigation tree on the left. The **Device VLAN List** appears.

2. Click the 🔄 **VLAN Configuration** link associated with the device to which you want to view virtual interfaces for.

3. Click the **Hybrid Port** tab. Details for all ports for the selected device display in the **Hybrid Port List**.

4. Click **Add**.

5. Select the port to be used for the hybrid port from the **Port Name** list.

6. Enter the port VLAN ID for the hybrid port in the **PVID** field.

7. Enter the all of the VLAN IDs to be tagged in the **Tagged VLAN** field.
   
   A valid VLAN ID is 1 – 4096.

8. Enter the all of the VLAN IDs to be untagged in the **Untagged VLAN** field.
   
   A valid VLAN ID is 1 – 4096.

9. Click **Submit**.

10. View the results of this task in the **Hybrid Port** list.

**Modifying a hybrid port**

To modify an existing hybrid port:

1. Navigate to **VLAN Management**→**VLAN Devices**→**Device Name**:
   - Click the **Service** tab from the tabular navigation system on the top.
   - Click the **VLAN Management** on the navigation tree on the left.
c. Click VLAN Devices link located under VLAN Management on the navigation tree on the left. The Device VLAN List appears.

2. Click the VLAN Configuration link associated with the device to which you want to view hybrid ports for.

3. Click the Hybrid Port tab.
   Details for all ports for the selected device display in the Hybrid Port List.

4. Click the Modify icon associated with the hybrid port you want to modify.

5. Select the port to be used for the hybrid port from the Port Name list.

6. Modify the port VLAN ID for the hybrid port in the PVID field.

7. Modify the VLAN IDs to be tagged in the Tagged VLAN field.

8. Modify the VLAN IDs to be untagged in the Untagged VLAN field.

9. Click Submit.

10. View the results of this task in the Hybrid Port list.

Deleting a hybrid port

To delete one or more hybrid ports:

1. Navigate to VLAN Management→VLAN Devices→Device Name:
   a. Click the Service tab from the tabular navigation system on the top.
   b. Click the VLAN Management on the navigation tree on the left.
   c. Click VLAN Devices link located under VLAN Management on the navigation tree on the left. The Device VLAN List appears.

2. Click the VLAN Configuration link associated with the device to which you want to view hybrid ports for.

3. Click the Hybrid Port tab.
   Details for all ports for the selected device display in the Hybrid Port List.

4. Click the checkbox to the left of the hybrid ports that you want to delete.

5. Click Delete.

6. Click OK to confirm the deletion of the selected hybrid ports.

VLAN deployment task

You can search deployment task by date, to view the results of VLAN deployment task and to view details for individual VLAN deployment task.

Viewing deployment task

To view all deployment task entries for VLANs:

1. Navigate to VLAN Management→VLAN Deployment Task:
   a. Click the Service tab from the tabular navigation system on the top.
b. Click the **VLAN Management** on the navigation tree on the left.

c. Click **VLAN Deployment Task** link located under **VLAN Management** on the navigation tree on the left.
   
The **VLAN Deployment Task** appears.

**VLAN report**

- **Operation**: Contains a summary of the VLAN management task being reported.
- **Result**: Contains the result of the operation.
- **Time**: Contains a date and timestamp for the task.
- **Details**: Contains a link for viewing details for the associated operation or task.

2. To view the details for a VLAN report entry, click the **Details** icon associated with the report entry you want to view.
   
   This report provides you with the name of the device, the IP address, the configuration task, and the results of the configuration task.

   - Click **[ ]** to page forward in the **VLAN Deployment Task**.
   - Click **[ ]** to page forward to the end of the **VLAN Deployment Task**.
   - Click **[ ]** to page backward in the **VLAN Deployment Task**.
   - Click **[ ]** to page backward to the front of the **VLAN Deployment Task**.

3. Click 8, 15, 50, 100, or 200 from the right side of the main pane to configure how many items per page you want to view.

4. For **VLAN Deployment Task** that have more than one page, click on 1, 2, 3, 4, 5, 6, 7, 8, 9, 10… from the bottom right side of the main pane to jump to a particular page of the list.
   
   You can sort the **VLAN Deployment Task** list by the **Operation**, **Result**, **Time** and **Details** fields by clicking the column label to sort the list by the selected field. The column label is a toggle switch that allows you to toggle between the various sort options specific to each field.

### Searching the VLAN deployment task

To search the VLAN report:

1. Navigate to **VLAN Management→VLAN Deployment Task**:
   
   a. Click the **Service** tab from the tabular navigation system on the top.
   
   b. Click the **VLAN Management** on the navigation tree on the left.
   
   c. Click **VLAN Deployment Task** link located under **VLAN Management** on the navigation tree on the left.
      
      The **VLAN Deployment Task** appears.

2. Move the pointer over **Query** at the upper right corner of **VLAN Deployment Task List**, and a search criteria dialog box appears.

3. Enter the start date for your search in the **Started at** field.
   
   To use the calendar to auto populate this field:
a. Click the calendar icon located to the right of the Started at field.

b. Select the start date from the displayed calendar.

If you do not specify the hour, minutes, and seconds for your search, IMC auto populates this value using the current time, possibly limiting your search results.

c. Enter the end date for your search in the Ended at field.

To auto populate this field, see steps 3a – 3c, above.

4. Select the result of the operation from the Result list.

5. Click Query to begin your search.

6. Click Reset when you have completed your search to return to the full VLAN report.

Deleting VLAN deployment task entries

To delete one or more VLAN report entries:

1. Navigate to VLAN Management→VLAN Deployment Task:
   a. Click the Service tab from the tabular navigation system on the top.
   b. Click the VLAN Management on the navigation tree on the left.
   c. Click VLAN Deployment Task link located under VLAN Management on the navigation tree on the left.

   The VLAN Deployment Task appears.

2. Click the checkbox to the left of the entry or entries you want to delete.

3. Click Delete.

4. Click OK to confirm the deletion of the selected VLAN report entries.

5. Click Add Task, select Deploy Access Ports, Deploy Trunk Ports, Deploy Hybrid Ports, Deploy VLANs to enter the batch deployment window for each port.

For more information, see “Deploying VLANs using batch mode” (page 845).

VLAN topology maps

IMC provides you with a graphical view of devices in a VLAN. The VLAN Topo option launches IMC’s Custom View, which includes a VLAN view. When you select an individual VLAN, the My Network View map updates to gray out all devices that are not part of the selected VLAN. All devices in the VLAN view for the selected VLAN remain active.

Viewing VLAN topo maps

To view VLAN topo maps:

1. Navigate to VLAN Management→My Network View:
   a. Click the Service tab from the tabular navigation system on the top.
   b. Click the VLAN Management on the navigation tree on the left.
   c. Click VLAN Topo link located under VLAN Management on the navigation tree on the left.

   A new browser window opens and the custom map displays in the new browser window.
A VLAN View table displays to the right of My Network View topology map that lists all VLANs, including the VLAN name and VLAN ID.

2. To view the devices for a specific VLAN, click the VLAN entry in the VLAN View table.

   Devices that are not part of the VLAN are grayed out. Devices that are part of the VLAN display color values associated with their most current alarm status.

3. To add a device to a VLAN through VLAN Topo

4. Click the VLAN entry in the VLAN View table.

5. Select Add to current VLAN from the right-click menu.

   The Add to current VLAN dialog box appears.

6. If you click the checkbox ☐ to the left of the Add VLAN to all Trunk and Hybrid ports, and click OK to add the VLAN to all the trunk and hybrid ports of the device. The VLAN added to the hybrid port must be tagged by default. Otherwise, you can only add the VLAN to all the access ports of the device.

7. Click OK.

8. Confirm the device display color values associated with their most current alarm status.

9. To delete the device from a VLAN

10. Click the VLAN entry in the VLAN View table.

11. Select Remove from the current VLAN from the right-click menu of the device.

   The device is deleted from the VLAN and grayed out.

12. To search for a particular VLAN in the VLAN View table, enter the VLAN ID in the Search field and press Enter to execute the search.

   IMC supports fuzzy matching for this field, allowing you to enter a complete or partial VLAN ID. IMC displays all VLAN IDs that match the search criteria.

13. Click Close when you are finished with the VLAN View table.

14. VLAN device monitoring and management features are available on IMC’s topology maps are accessed through left and right mouse clicks.

   For more information on the monitoring and management features of topology maps, see “Viewing devices via the Network Topology” (page 181).

---

Deploying VLANs using batch mode

Using the Batch Deploy option, you can configure access ports, trunk ports, hybrid ports, or create VLANs for one or more devices.

Batch deployment for VLAN creation

You can configure a VLAN on one or more devices using the Batch Deploy option for VLANs.

To use batch deployment to create a VLAN:

1. Navigate to VLAN Management→Batch Deploy.

   a. Click the Service tab from the tabular navigation system on the top.

   b. Click the VLAN Management on the navigation tree on the left.

   c. Click 🔄 Batch Deploy link located under VLAN Management on the navigation tree on the left.

   The Batch Deploy page appears.
2. Click **VLAN** option.
   
   The window for batch deploying new VLANs appears.

3. Enter the VLAN ID for the VLAN you want to add access ports to in the **VLAN ID** field.

4. Enter the name for the VLAN in the **VLAN Name** field.
   
   Question marks (?) and non-ASCII characters are not permitted in VLAN names.

5. Click **Next**.

6. Click **Add** to select the devices to which you want to add the VLAN you specified in Step 2.

7. Add devices by using either the **View** or **Advanced** query option. See "Adding devices by View" (page 85) and "Adding devices by Advanced query" (page 85).

8. Click **Submit**.

9. Review the results of your batch deploy configuration task in the **Deploying VLAN Summary Report** that display upon completion.

Batch deployment for access ports

Using batch deployment for access ports, you can configure one or more access ports for an existing VLAN.

To use batch deployment to configure access ports for an existing VLAN:

1. Navigate to **VLAN Management**→**Batch Deploy**:
   
   a. Click the **Service** tab from the tabular navigation system on the top.
   
   b. Click the **VLAN Management** on the navigation tree on the left.
      
   c. Click **Batch Deploy** link located under **VLAN Management** on the navigation tree on the left.
      
      The **Batch Deploy** page appears.

2. Click **Access ports** option.

   The window for batch deploying access ports appears.

3. Enter the port VLAN ID for the VLAN you want to add access ports to in the **PVID** field.

4. Click **Next**.

   The PVID you enter in this field must already exist on all of the access devices that you want to add access ports from. To add the PVID to one or more access devices, use the VLAN Batch Deploy option.

   For more information on the VLAN Batch Deploy option, see "Batch deployment for VLAN creation" (page 845).

5. Click **Add** to select the interfaces from which you want to add access ports to the PVID you specified in Step 2.

6. Add interfaces by **View** or by the **Advanced** query method.

   See "Adding devices by View" (page 85) and "Adding devices by Advanced query" (page 85) which both function like the adding interfaces by view and query.

7. Click **Submit**.

8. Review the results of your batch deploy configuration task in the **Deploying Access Ports Summary Report** that displays upon completion.
Batch deployment for trunk ports

Using batch deployment for trunk ports, you can configure one or more trunk ports for an existing VLAN. To use batch deployment to configure trunk ports for an existing VLAN:

1. Navigate to VLAN Management→Batch Deploy:
   a. Click the Service tab from the tabular navigation system on the top.
   b. Click the VLAN Management on the navigation tree on the left.
   c. Click Batch Deploy link located under VLAN Management on the navigation tree on the left.
      The Batch Deploy page appears.

2. Click Trunk ports option.
   The window for batch deploying trunk ports appears.

3. Enter the port VLAN ID in the PVID field.

4. Enter the existing allowed VLAN ID in the Allowed VLAN field.

5. Click Next.
   The PVID you enter in this field must already exist on all trunk devices that you want to add trunk ports from.

6. Click Add to select the interfaces from which you want to add trunk ports to the PVID you specified in Step 2.

7. Add interfaces by View or by the Advanced query method.
   See "Adding devices by View" (page 85) and "Adding devices by Advanced query" (page 85) which both function like the adding interfaces by view and query. Click Submit.

8. Review the results of your batch deploy configuration task in the Deploying Trunk Ports Summary Report that displays upon completion.

Batch deployment for hybrid ports

Using batch deployment for hybrid ports, you can configure one or more hybrid ports for an existing VLAN. To use batch deployment to configure hybrid ports for an existing VLAN:

1. Navigate to VLAN Management→Batch Deploy:
   a. Click the Service tab from the tabular navigation system on the top.
   b. Click VLAN Management on the navigation tree on the left.
   c. Click the Batch Deploy link located under VLAN Management on the navigation tree on the left.
      The Batch Deploy page appears.

2. Click Hybrid ports option.
   The window for batch deploying hybrid ports appears.

3. Enter the port VLAN ID for the VLAN you want to add hybrid ports to in the PVID field.

4. Enter the VLAN ID for the tagged VLAN in the Tagged VLAN field.
   If you do not enter any value, all tagged VLAN IDs on the selected interfaces are cleared.
5. Enter the VLAN ID for the untagged VLAN in the **Untagged VLAN** field.
   
   If you do not enter any value, all untagged VLAN IDs on the selected interfaces are cleared.

6. Enter the VLAN ID for the forbidden VLAN in the **Forbidden VLAN** field.
   
   If you do not enter any value, all forbidden VLAN IDs on the selected interfaces are cleared.
   
   The PVID as well as the Tagged Untagged, and Forbidden VLANs you enter in these fields must already exist on all of the devices that you want to add hybrid ports from.

7. Click **Add** to select the interfaces from which you want to add hybrid ports to the PVID you specified in **Step 2**.

8. Add interfaces by **View** or by the **Advanced** query method.
   
   See "Adding devices by View" (page 85) and "Adding devices by Advanced query" (page 85) which both function like the adding interfaces by view and query.
   
   Click **Submit**.

9. Review the results of your batch deploy configuration task in the **Deploying Hybrid Ports Summary Report** that displays upon completion.
From the Report tab, you can quickly and easily access IMC’s template driven reports on network assets, configuration and configuration changes, network device and link status and events, alarms, and network device health. In addition, you can access reports on network user and service activity and device and link details.

There are two types of report categories: Real Time and Quick Custom. The Real Time category offers resource statistics, configuration and change, fault or alarm and performance reporting on network devices and interfaces, users and services. You can schedule Real Time reports with format options including PDF, CSV, or Microsoft Excel. Scheduled reports are stored on the IMC server for later viewing and downloading.

Quick Custom reports are informational only. There are two types of Quick Custom reports – device and link. Device detail reports include information on device label, status, IP address, MAC address, device type, model, vendor, location, contact, SysOID, hardware version, software version, serial number and product number for managed devices. Quick custom reports based on link details include information on devices connected to either end of a link. This information includes device name, port, IP address, and port speed.

All reporting under the Report tab is template driven with reports being generated from the system or from user-defined templates. For Real Time reports, IMC provides many system-defined templates that you can use to create their custom report views as well as to schedule reports.

Templates are also used for Quick Custom reports. You can create your own templates for Quick Custom reports through the use of step-by-step configuration and include the reports based on the created templates in your report views.

The Report main page, accessed via the Report tab is a blank page that can be customized to meet individual reporting needs. Using the Add My Real Time Report and the Add My Quick Report links, you can customize the Report main page to include those reports that are most useful to you. Once a report is added to the Report main page, you can access them by clicking the report name link and entering report parameters, including date and time, to access the information they need quickly. Note, however, that you must first create the reports using the report templates for Real Time reports or create the templates for Quick reports before you can add them to your customized My Reports page.

In addition to web views of reports, you can also schedule Real Time reports that are written to Adobe Acrobat, Microsoft Excel, or Comma Separated Value formats. Scheduled reports can also be sent via email in Adobe Acrobat, Microsoft Excel, or Comma Separated Value formats.

Finally, you can incorporate data from other IMC sources for inclusion in Real Time reporting and you can also add your own name or company name and logo to all Real Time reports.

My real time reports

The base version of IMC provides a number of pre-defined reports that provide you with a wide range of information about the health and performance of network resources from network discoveries and topology reports to capacity and optimization reports. Base installation reports also include information on alarms as well as network performance. The list of pre-defined reports expands as IMC modules are added to the base installation of IMC. These reports are available to you from the My Real Time Reports page.
Resource statistics report

Reports found under the **Resource Statistics Reports** section of **My Real Time Reports** provide you with information about devices managed by IMC including device summaries, port utilization and capacity, device connectivity, device changes, and device type. Specifically, the **Resource Statistics Reports** section of the **My Real Time Reports** includes the following pre-defined reports:

- **Capacity Report**: Provides a list of total and available ports for each device managed by IMC.
- **Changes Report**: Identifies device changes that have occurred since the last discovery. The report reports on the old settings as well as the current or changed settings.
- **Device Asset Report**: Shows device asset information including stack information and slot information.
- **Device Category Statistic Report**: Provides a distribution of devices by IMC category or type. For more information on device categories, see "Configuring device categories" (page 99).
- **Device History Report**: Provides a history of configuration changes to devices including device label changes and configuration changes to interface status.
- **Device Summary Report**: Provides a statistical summary of devices managed by IMC. It reports on the distribution of devices by device category, by status, and by vendor. It also provides you with a distribution of device alarm status by IP segment.
- **Discovery Report**: Provides a list of problems that IMC encountered while performing a network discovery.
- **Inventory Report**: Lists all devices discovered by IMC by MAC address and by the IP address of the access device that the MAC address is associated with.
- **Misconfigurations and Optimizations Report**: Identifies devices that are configured with the default SNMP read and write community strings.
- **Topology Report**: Provides a list of all devices managed by IMC and the devices they connect to. For both devices, IMC provides the device name, IP address, device type, port information, and the status of this link.
- **User Tracking Report**: Describes MAC information on the switch devices managed by IMC.

Alarm analysis reports

Reports found under the **Alarm Analysis Reports** section of **My Real Time Reports** provide you with information about failures on devices, interfaces, and links managed by IMC including availability statistics, outage durations, distribution statistics on outage durations, and causes when the cause is available. Statistics can be collected for all **Alarm Analysis Reports**. Specifically, the **Alarm Analysis Reports** section of the **My Real Time Reports** includes the following pre-defined reports:

- **Device Connectivity Detail Report**: Provides details for devices that reported availability problems. This report includes statistics on the duration of downtime, distribution of the length of the outage in minutes, and the cause for the outage when available.
- **Device Connectivity Summary Report**: Provides availability statistics for devices managed by IMC. This report also includes statistics on outage duration and a distribution of outage durations for each device.
- **Interface Connectivity Detail Report**: Provides details for interfaces that reported availability problems. This report includes statistics on the duration of downtime, distribution of the length of the outage in minutes, and the cause for the outage when available.
- **Interface Connectivity Summary Report**: Provides availability statistics for the interfaces of devices managed by IMC. This report also includes statistics on outage duration and a distribution of outage durations for each interface.
- **Link Connectivity Detail Report**: Provides details for links that reported availability problems. This report includes statistics on the duration of downtime, distribution of the length of the outage in minutes, and the cause for the outage when available.

- **Link Connectivity Summary Report**: Provides availability statistics for the links managed by IMC. This report also includes statistics on outage duration and a distribution of outage durations for each link.

- **Node Connectivity Summary Report**: Provides distribution statistics for faults reported by nodes in the network infrastructure. Faults are classified by device, power, channel, or other. This report also provides node and channel availability statistics.

### Performance analysis summary reports

- **Custom View Data Summary Report**: Provides you with a template for the historical reporting of a single performance metric for devices in the selected Custom View. You select the metric or monitor index to be reported on, the Custom View that contains the devices to be reported on, and the date and time range. The contents of the Detail field provide you with a link to viewing more detailed information for the associated entry.

- **Performance View Summary Report**: Provides you with a template for the historical reporting for devices by performance metric. You must select the performance metric or monitor index to be reported on, the date and time range as well as the devices to be included in the report by selecting on the Performance View that contains the devices. The contents of the Detail field provide you with a link to viewing more detailed information for the associated entry.

- **Performance View All Summary Report**: Provides you with a template for the historical reporting for all monitor indexes. You must select the date and time range as well as the devices to be included in the report by selecting on the Performance View that contains the devices. The contents of the Detail field provide you with a link to viewing more detailed information for the associated entry.

For operators who have already customized their *My Real Time Reports* page, some of these reports may no longer be visible.

To reset your *My Real Time Reports* page, click the ![Reset My Reports](image) link located in the far right corner of the *My Real Time Reports* page. For more information on this feature, see "Customizing my real time report page" (page 851).

### Customizing my real time report page

Every IMC operator has a report view that they can customize to meet their individual reporting needs and to provide them with quick access to the reports they use most frequently. You can include any report that is available under the Report tab in your custom view. This custom view is the main report page that is accessed by clicking the Report tab. You can add both Real Time and Quick Custom reports to this main Report view. This view gives you quick and easy access to the reports most relevant for them.

For managing Real Time reports in your Report main page, see "Adding a real time report" (page 855).

For managing Quick Custom reports in your Report main page, see "Adding a quick custom report" (page 870).

### Resetting my report

Upon account creation, the Report main page is blank for all operators. However, you can elect to have IMC populate your Report main page with all Real Time and Quick Custom reports.
1. Click the **Report** tab from the tabular navigation system on the top.

2. Click the "Reset My Reports" link located in the upper right corner of the **Report** main page.

   If you have the IMC base platform installed, the page updates to display pre-defined reports described in the **My Real Time Reports** section of this manual.

   If you have additional modules installed, reports for these modules are also displayed on this page.

   For more information on managing and customizing the **My Real Time Reports** page, see "Modifying a real time report" (page 857) and "Deleting a real time report" (page 857).

3. Click **OK**.

   ┌──────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────┐
   │ WARNING:                                                                                                       │
   │ Resetting **My Report** deletes all existing reports and add all reports available under the **Report** tab.   │
   └──────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────┘

**Real time reports**

You can configure your **Report** main page to include any of the Real Time reports IMC offers for quick and easy access to the report. In addition, you can schedule Real Time reports with format options including PDF, CSV, or XLS. Scheduled reports are stored on the IMC server for later viewing and downloading.

Real Time reports are template driven and IMC comes with templates already created for reporting on resource statistics, alarms, reporting on 300 performance metrics as well as reports on configuration and change management. In addition, IMC allows you to define new templates as needed.

Using these templates, you can run reports directly from templates or you can customize their **Report** main page with those reports you need most. And, you can schedule any Real Time report for historical review and analysis.

**Real time report templates**

Templates drive report creation for Real Time reports, the heart of IMC reporting. IMC provides templates for resource statistics, alarm analysis, performance analysis and change and configuration reporting. IMC also supports the creation of user-defined templates for Real Time reports in IMC v.5.0.

**Accessing the real time report template list**

To access the Real Time report template list:

1. Navigate to **Report**→**Report Template List <IMC Instance>**:
   a. Click the **Report** tab from the tabular navigation system on the top.
   b. Click **Reports** on the navigation tree on the left.
   c. Click **Report Template List** under **Reports** from the navigation system on the left.


**Report template**

- **Template Name**: Contains the name of the system-defined or user-defined template.
- **Type**: Contains the type of report that is generated by the associated template. There are five types of report templates that the IMC base platform offers. As additional service modules are added, report templates for those service modules are added. The base platform report templates include:
  - **Overall Report**: All of the unknown types of user-defined reports.
- **Performance Analysis Report**: Provide measurements for almost 300 different performance metrics.
- **Resource Statistics Report**: Provide distribution statistics of network devices, network device change reports, device history, device misconfiguration and optimization reports, as well as basic device information reports.
- **Alarm Analysis Report**: Provide fault or alarm statistics including device, interface, and node connectivity issues.
- **Intelligent Configuration Report**: Available when you install the iCC module. You can customize the intelligent configuration reports and add them to this type.
- **Definition Type**: Identifies the source of the template. Template sources include Custom or Pre-defined reports.
- **Details**: Provides an active link to view additional details for the associated template.
- **Modify**: Contains an active link for modifying the associated template.
- **Delete**: Contains an active link, if permitted, for deleting the associated template. System or pre-defined templates cannot be deleted.

You can sort the **Report Template List** by the **Template Name**, **Type**, or **Definition Type** fields by clicking the column label to sort the list by the selected field. The column label is a toggle switch that allows you to toggle between the various sort options specific to each field.

1. Click **to page forward in the Report Template List**.
2. Click **to page forward to the end of the Report Template List**.
3. Click **to page backward in the Report Template List**.
4. Click **to page backward to the front of the Report Template List**.

2. **Click 8, 15, 50, 100, or 200** from the right side of the main page to configure how many items per page you want to view.

**Running a report using a real time report template**

To run an ad hoc report via a Real Time report template:

1. Navigate to **Report → Report Template List <IMC Instance>**:
   a. Click the **Report** tab from the tabular navigation system on the top.
   b. Click **Reports** on the navigation tree on the left.
   c. Click **Report Template List** under **Reports** from the navigation system on the left.

   The **Report Template List** displays in the main page.

2. Click the active link in the **Template Name** field for the report you want to run.

   For some reports, you may be prompted to enter a starting time and an ending time for the report as well as other report configuration parameters.
   a. Enter all required parameters.
   b. Click **OK**.

   The report displays in an **Intelligent Analysis Report Viewer** window.

**Printing a real time report to PDF**

To print the report to PDF:
1. Click the Print icon located on the toolbar on the top of the report.
2. Select the desired pages from Page Range.
3. Click Export.

Exporting a real time report

To export the Real Time report:

1. Click the Export icon located on the toolbar on the top of the report.
2. Select the desired export file format from the File Format list.
   Options include, Crystal Reports (RPT), Adobe Acrobat (PDF), Microsoft Excel (97-2003), Microsoft Excel (97-2003) Data-Only, Microsoft Word (97-2003) – Editable, Rich Text Format (RTF), and Comma Separated Values (CSV).
3. Select the desired pages from Page Range.
4. Click Export.

Modifying a real time report template

To modify a Real Time report template:

1. Navigate to Report → Report Template List <IMC Instance>:
   a. Click the Report tab from the tabular navigation system on the top.
   b. Click Reports on the navigation tree on the left.
   c. Click Report Template List under Reports from the navigation system on the left.
2. Click the Modify icon associated with the report template you want to modify.
3. Modify the name for the template in the Template Name field.
4. Verify that the name is unique.
5. Modify the type of report by selecting a new template type in the Type field.
6. To add or remove group names, do one of the following:
   o Click the checkbox next to the group names you want to add, or
   o Click the checked box next to the group names you want to remove.
7. Click OK.

You cannot modify a Real Time template’s Location or Report Data Source.

Adding a real time report template

You can create user-defined templates for Real Time reports (usually of the Overall Report type) by importing iAR report templates.

To add a Real Time report template:

1. Navigate to Report → Add Report Template:
   a. Click the Report tab from the tabular navigation system on the top.
   b. Click Reports on the navigation tree on the left.
   c. Click Add Report Template under Reports from the navigation system on the left.
2. Click the Upload button.
The **Upload Template** window appears.

3. Click **Browse** located to the right of the **Template File** field to select a template file.
   
   This step is required and you can only select an RPT file with the file name consisting of letters, digits, and underscores (_).

4. Click **Browse** located to the right of the **Parameter File** field to select a parameter file.
   
   This step is optional and you can only select an XML file with the file name consisting of letters, digits, and underscores (_).

5. Click **OK**.

6. Select the data source from the **Report Data Source** list.

7. If you have not defined multiple data sources, select **Local (127.0.0.1)**.
   
   For more information on data source, see "Managing real time report data sources" (page 858).

8. Enter the name for the template in the **Template Name** field.

9. Verify that the name is unique.

10. Select the type of report by selecting a template type in the **Type** field.

11. If you are not sure about the template type, select the **Overall Report** type.

12. Select the groups to have access to this report by clicking the checkbox next to the group names you want to add.

13. Click **OK**.

   The Adding Real Time report template function is available without the need of a license in IMC trial versions. To use this function in an IMC retail version, you must purchase a license.

---

**Managing real time reports**

Real Time reports are those reports that offer resource statistics, configuration and change, fault or alarm and performance reporting on network devices and interfaces, users and services. You can schedule Real Time reports with PDF, CSV, or Microsoft Excel report formatting as options. Scheduled reports are stored on the IMC server for retrieval access.

You can incorporate data from other IMC sources for inclusion in Real Time reporting and also add your own name or company name and logo to all Real Time reports.

Real Time reports are template driven as reports are generated from pre-defined system templates. IMC provides many system-defined templates that you use to create your custom report views as well as to schedule reporting. User-defined templates are available for Real Time reports in IMC v5.0. Operators can use user-defined templates to create their custom report views as well as to schedule reporting.

**Adding a real time report**

Adding a report simply makes the report template available on the operators **Report** page for quick access. Once it is added to the **Report** main page, operators can run the report, entering the required parameters, if any, before viewing the report’s contents.

To Add a Real Time report:

1. Click the **Report** tab from the tabular navigation system on the top.

2. Click the **Add My Real Time Report** link located below and to the right of the tabular navigation system.

3. Locate the template you want to use for this Real Time report.
Click ⏷ to page forward in the Template List.
Click ⏷ to page forward to the end of the Template List.
Click ⏷ to page backward in the Template List.
Click ⏷ to page backward to the front of the Template List.

4. Click 8, 15, 50, 100, or 200 from the right side of the main page to configure how many items per page you want to view.

5. Select from one of the following:
   - To more quickly access the template you want to create a Real Time report for, sort the template list by clicking Template Name or Type. The column labels are a switch for toggling between the various sort of options available for each column.
   - To search by template name, enter the name of the template in the Template Name field of the Query Template section and click Query to begin your search.
   - To search by template type, select the template type you want to create a report for from the Type list and click Query to begin your search.
   - If you don’t know what report you want to select, consider the type of report you want. There are five types of reports (which can be found in the Type field) that the IMC base platform offers. They include:
     - Overall Report: All of the unknown types of user-defined reports.
     - Performance Analysis Report: Provide measurements for almost 300 different performance metrics.
     - Resource Statistics Report: Provide distribution statistics of network devices, network device change reports, device history, device misconfiguration and optimization reports as well as basic device information reports.
     - Alarm Analysis Report: Provide you with a fault or alarm statistics including device, interface, and node connectivity issues.
     - Intelligent Configuration Report: Available when you install the iCC module. You can customize the intelligent configuration reports and add them to this type.

6. Click the checkboxes ☑ next to the template names you want to create Real Time reports for.

7. Click OK.

   The templates you selected appear categorized by Report Template type under My Real Time Reports in the main pane of the Report page.

Viewing a real time report

To view a Real Time report:

1. Click the Report tab from the tabular navigation system on the top.

2. Click the report name you want to view under the My Real Time Reports [Edit Mode] section heading.

3. Verify that this link displays [Edit Mode] as this confirms that you are in view mode.

The My Real Time Reports [Edit Mode] section heading appears only after you have added Real Time reports.

In addition, the [Edit Mode/View Mode] link is a toggle switch between editing and viewing Real Time reports.

Use the [Edit Mode/View Mode] link to toggle between viewing and editing Real Time reports.
4. Set any parameters, if any, that you are prompted to set in the Set Parameters dialog box.
5. Click OK to view the selected report.

The report displays in an Intelligent Analysis Report Viewer window.

**Printing a real time report**

To print a Real Time report:
1. Click the Report tab from the tabular navigation system on the top.
2. Click the report name you want to view under the My Real Time Reports [Edit Mode] section heading.
3. Verify that this link displays [Edit Mode] as this confirms that you are in view mode.
4. Set any parameters, if any, that you are prompted to set in the Set Parameters dialog box.
5. Click OK to view the selected report.

The report displays in an Intelligent Analysis Report Viewer window.

**Printing a real time report to PDF**

1. Click the Print icon located on the toolbar on the top of the report.
2. Select the desired page range from Page Range.
3. Click Export.

**Exporting a real time report**

1. Click the Export icon located on the toolbar on the top of the report.
2. Select the desired export file format from the File Format list.
   Options include: Crystal Reports (RPT), Adobe Acrobat (PDF), Microsoft Excel (97-2003), Microsoft Excel (97-2003) Data-Only, Microsoft Word (97-2003) – Editable, Rich Text Format (RTF), and Comma Separated Values (CSV).
3. Click Export.

**Modifying a real time report**

Only the report name and description of a Real Time report can be modified. To modify these fields:
1. Click the Report tab from the tabular navigation system on the top.
2. Click [Edit Mode] to the right of My Real Time Reports [Edit Mode]. Verify that this link displays [View Mode] as this confirms that you are in edit mode.
3. Click the Edit icon to the right of the report you want to modify.
4. To modify the display name, delete the existing value in the Display Name field and enter the new report name.
5. To modify the report description, delete the existing description in the Description field and enter a new description.
6. Click OK to accept changes.

**Deleting a real time report**

To delete a Real Time report:
1. Click the Report tab from the tabular navigation system on the top.
2. Click [Edit Mode] to the right of My Real Time Reports [Edit Mode]. Verify that this link displays [View Mode] as this confirms that you are in edit mode.

3. Click the Delete icon to the right of the report you want to delete.
4. Click OK to confirm deletion.

Managing real time report data sources

IMC enables you to configure other instances of IMC as a data source for reporting, allowing you to centralize your reporting.

Viewing current report data sources

To view current report data sources:

1. Navigate to Report → Reporting Data Source:
   a. Click the Report tab from the tabular navigation system on the top.
   b. Click Reports on the navigation tree on the left.
   c. Click Report Data Source under Report from the navigation system on the left.

   IMC displays all report data sources entries in the Report Data Source pane displayed in the main pane of the Report → Report Data Source window.

   Report data

   - **Data Source Name**: Contains the name of the data source as defined in IMC. The name given for the data source in IMC may different from the actual hostname of the device that serves as the data source.
   - **Data Source IP**: Contains the IP address of the data source host.
   - **Description**: Produces a description for the data source host.
   - **Modify**: Contains a link for modifying the associated Data Source.
   - **Delete**: Contains a link, if permitted, for deleting the associated Data Source. Pre-defined data sources cannot be deleted.

You can sort the Report Data Source list by the Data Source Name, Data or Source IP fields by clicking the column label to sort the list by the selected field. The column label is a toggle switch that allows you to toggle between the various sort options specific to each field.

If your Report Data Source list contains multiple entries, the following navigational aids may appear:

- Click to page forward in the Report Data Source List.
- Click to page forward to the end of the Report Data Source List.
- Click to page backward in the Report Data Source List.
- Click to page backward to the front of the Report Data Source List.

2. Click 8, 15, 50, 100, or 200 from the right side of the main page to configure how many entries per page to display.

3. Do one of the following:
   - To search by data source name, enter the name of the data source in the Data Source Name field of the Query section and click Query to begin your search, or
To search by data source IP address, enter the IP address of the data source in the **Data Source IP** field of the **Query** section and click **Query** to begin your search.

### Adding a report data source

To add a report data source:

1. Navigate to **Report** → **Reporting Data Source**:
   a. Click the **Report** tab from the tabular navigation system on the top.
   b. Click **Reports** on the navigation tree on the left.
   c. Click **Report Data Source** under **Reports** from the navigation system on the left.
2. Click **Add**.
3. Enter the IP address of the IMC server to serve as the data source in the **Data Source IP** field.
4. If the IMC database has been installed on a standalone server, enter the IP address of the database server.
5. Enter the name of the data source as defined in IMC in the **Data Source Name** field.
6. Enter a description for this data source in the **Description** field.
7. Click **OK**.

**Data Source DB Name** is report_db, and cannot be modified.

### Modifying a report data source

To modify a report data source:

1. Navigate to **Report** → **Reporting Data Source**:
   a. Click the **Report** tab from the tabular navigation system on the top.
   b. Click **Reports** on the navigation tree on the left.
   c. Click **Report Data Source** under **Reports** from the navigation system on the left.
2. Click the **Modify** icon associated with the data source you want to modify.
3. Modify the IP address of the IMC server to serve as the data source in the **Data Source IP** field.
   The IP address of the pre-defined data source cannot be modified.
4. Modify the host name of the IMC server in the **Data Source Name** field.
5. Modify the description for this data source in the **Description** field.
6. Click **OK**.

**Data Source DB Name** is report_db, and cannot be modified.

### Deleting a report data source

To delete a report data source:

1. Navigate to **Report** → **Reporting Data Source**:
   a. Click the **Report** tab from the tabular navigation system on the top.
   b. Click **Reports** on the navigation tree on the left.
   c. Click **Report Data Source** under **Reports** from the navigation system on the left.
2. Click the **Delete** icon associated with the data source you want to delete.
3. Click **OK** to confirm deletion of the data source.

### Real time report options

You can add your company name and logo to IMC reports.

To add a company name and logo:

1. Navigate to **Report→Options**:
   a. Click the **Report** tab from the tabular navigation system on the top.
   b. Click **Reports** on the navigation tree on the left.
   
   *c. Click 📌**Options** under **Reports** from the navigation system on the left.*

2. Enter the name you want displayed on all IMC reports in the **Vendor Name** field.

3. Click **OK** to accept the **Vendor Name**.

4. Click **Upload**.

   The **Upload** window appears.

5. Click **Browse**, select the image to be used as the vendor logo, and then click **OK** to upload the image to the IMC server.

   A JPG file with the max file size of 100K, max dimensions of 128 pixels by 128 pixels, and a file name consisting of letters, digits, and underscores (_) is allowed and the image overwrites the old file to become effective, depending on the RPT file.

### Scheduling real time reports

You can schedule any Real Time report to run daily, weekly, monthly, quarterly, semi-annually, or annually and define the start dates of data collection for generating scheduled reports and the end dates and times for the corresponding scheduled report tasks. In addition, you can configure the report formats with options for PDF, CSV, or XLS and include email recipients for all scheduled reports.

When reports are scheduled, IMC generates the reports in the specified report format, emails them to specified recipients and stores the reports for future access.

IMC retains all scheduled reports indefinitely. Therefore, you need to manage the retention of all historical reports manually.

You can also access reports generated by IMC scheduling, or modify, delete, suspend and resume scheduled reports.

### Viewing all scheduled reports

To view all scheduled reports:

1. Navigate to **Report→All Scheduled Reports**:
   a. Click the **Report** tab from the tabular navigation system on the top.
   b. Click **Scheduled Reports** on the navigation tree on the left.
   
   *c. Click 📌**All Scheduled Reports** under **Scheduled Reports** from the navigation system on the left.*

   IMC displays all scheduled report entries in the **Scheduled Report List** displayed in the main pane of the **Report→All Scheduled Reports** window.
Scheduled Report Name: Contains the name of the scheduled report. The Scheduled Report Name field contains an active link to the detailed information on the scheduled report, including last and next execution time.

Template Name: Contains template source for the scheduled report.

Type: Identifies the type of the report.

Status: Provides information on the status of the associated report.

History Report: Provides a link to access previously generated reports for the associated report.

Operation: Provides you with the ability to suspend or resume scheduled report generation for the associated report.

Modify: Provides you with a link to modify the associated report.

Delete: Contains a link for deleting the associated report.

You can sort the Report Template List by the Scheduled Report Name, Template Name, Type or Status fields by clicking the column label to sort the list by the selected field. The column label is a toggle switch that allows you to toggle between the various sort options specific to each field.

If Scheduled Report List contains multiple entries, the following navigational aids may appear:

- Click to page forward in the Scheduled Report List.
- Click to page forward to the end of the Scheduled Report List.
- Click to page backward in the Scheduled Report List.
- Click to page backward to the front of the Scheduled Report List.

2. Click 8, 15, 50, 100, or 200 from the right side of the main pane to configure how many items per page you want to view.

Filtering the scheduled report list

You can filter the Scheduled Report List in these ways:

- Daily
- Weekly
- Monthly
- Quarterly
- Half Yearly
- Yearly

1. You can also use the Query Report option located above the Scheduled Report List or filter the Scheduled Report List by the template used in the scheduled report. This filters the list for only those reports that use the selected template. Do one of the following:

- Enter the name of the template in the Template Name field of the Query Report section, or
- Search by scheduled report name by entering it in the Scheduled Report Name field of the Query Report section.

2. Click Query to begin your search.

Adding a scheduled report

To add a scheduled report:
1. **Navigate to Report→All Scheduled Reports:**
   a. Click the **Report** tab from the tabular navigation system on the top.
   b. Click **Scheduled Reports** on the navigation tree on the left.
   c. Click **All Scheduled Reports** under **Scheduled Reports** from the navigation system on the left.

2. **Click Add.**

3. Click **Select** to choose the template you want to schedule a Real Time report for.

4. Click the radio button to the left of the **Template Name** you want to schedule a report for.
   - Click \( \rightarrow \) to page forward in the **Scheduled Report List**.
   - Click \( \rightarrow \) to page forward to the end of the **Scheduled Report List**.
   - Click \( \rightarrow \) to page backward in the **Scheduled Report List**.
   - Click \( \rightarrow \) to page backward to the front of the **Scheduled Report List**.

5. Click **8**, **15**, **50**, **100**, or **200** to configure how many items per page you want to view.

6. To search for the template:
   - Enter the template name in the **Template Name** field of the **Query Template** portion of the dialog box, or
   - Search by template type by selecting the type of template you want to select from the **Type** list.

7. Click **OK** once you have made your template selection.

   You cannot modify the **Template Name** and the **Scheduled Report Name** once you have created it.

8. Enter the name for the scheduled report in the **Scheduled Report Name** field.

   It is useful to include the frequency as well as the report type in the **Scheduled Report Name**.

9. Select the data collection period for the scheduled report by clicking the radio button to the left of the schedule frequency you want to apply to this report in the **Schedule Type** section. Options include **Daily**, **Weekly**, **Monthly**, **Quarterly**, **Half Yearly**, and **Yearly**.

10. Select the start date for the scheduled report by clicking the **Calendar** icon located to the right of the **Report Start date** field in the **Schedule Type** section.

11. Select the date from the displayed calendar.

    Once you have added a scheduled report, a scheduled report task is added in IMC. IMC checks all scheduled report tasks at 4:00 a.m. every day, and generates scheduled reports for tasks whose data collection periods are met.

    For example, if you added at 9:00 a.m. on 2010-12-15 a monthly report with the start date of data collection on 2010-10-10, IMC would generate at 4:00 a.m. on 2010-12-16 scheduled reports with data collection periods from 2010-10-10 00:00 to 2010-11-10 00:00 and from 2010-11-10 00:00 to 2010-12-10 00:00.

12. If you want to configure an end date and time for a scheduled report task, click the checkbox \( \square \) to the left of **End by** in the **Schedule Time Settings** section.

    The **Add Scheduled Report** window updates to include an **End by** field.

13. Select the end date and time for the scheduled report task by clicking the **Calendar** icon located to the right of the **End by** field.

14. Select the date and enter the time from the displayed calendar.

862
Once you have defined the end date and time for a scheduled report task, no new scheduled report is generated for the task after the end date and time.

15. Select the report file format for the scheduled report by selecting it from the Report File Format list in the Delivery Options section. Options include PDF, CSV, MS Excel, and MS Excel (Data-Only).

16. If you want to configure an email recipient for the scheduled report, click the checkbox to the left of Send by Email.

   The Add Scheduled Report window updates to include a field to the right of Send by Email to enter the email address for the Email recipient.

   Enter the full email address of the recipient in this field.

   IMC sends an email to the email recipient (if specified) when generating a scheduled report.

   For IMC to send scheduled reports to email recipients, the SMTP mail server settings for IMC must be configured. For more information on configuring IMC’s mail server settings, see “Configuring IMC for email notification” (page 135).

17. Set parameters, if any, located at the bottom of the Add Scheduled Report window.

   Parameters include:
   - View Name: Sets the view for which a report is generated.
   - Begin Time: Sets the start time for the specific time range in a data collection period.
   - End Time: Sets the end time for the specific time range in a data collection period.

18. Click the Set Parameter icon in the Set Parameter field.

   If the parameter was set, this Set Parameter field is updated to icon.

19. If you want to modify the parameter, click .

   Begin Time must be earlier than End Time.

20. Click OK.

   Quick Custom reports cannot be scheduled. Only Real Time reports can be scheduled.

Modifying a scheduled report

To modify a scheduled report:

1. Navigate to Report→All Scheduled Reports:
   a. Click the Report tab from the tabular navigation system on the top.
   b. Click Scheduled Reports on the navigation tree on the left.
   c. Click All Scheduled Reports under Scheduled Reports from the navigation system on the left.

2. Click the Modify icon associated with the scheduled report you want to modify.

   You cannot modify the Template Name and the Scheduled Report Name once you have created it.

3. Change the data collection period for the scheduled report by clicking the radio button to the left of the schedule frequency you want to apply to this report in Schedule Type section.

   Options include Daily, Weekly, Monthly, Quarterly, Half Yearly, and Yearly.

4. Modify the start date for the scheduled report by clicking the Calendar icon located to the right of the Report Start date field in the Schedule Type section.

5. Select the new date from the displayed calendar.
IMC checks all scheduled report tasks at 4:00 a.m. every day, and generates scheduled reports for tasks whose data collection periods are met.

For example, if you modified at 9:00 a.m. on 2010-12-16 an existing monthly scheduled report with the start time of data collection on 2010-10-05, IMC would generate at 4:00 a.m. on 2010-12-17 scheduled reports with data collection periods from 2010-10-05 00:00 to 2010-11-05 00:00 and from 2010-11-05 00:00 to 2010-12-05 00:00.

6. If you want to add an end date and time for a scheduled report task, click the checkbox to the left of End by in the Schedule Time Settings section.

The Modify Scheduled Report window updates to include an End by field.

7. Select the end date and time for a new or an existing scheduled report task by clicking the Calendar icon located to the right of the End by field.

8. Select the date and enter the time from the displayed calendar.

Once you have defined the end date and time for a scheduled report task, no new scheduled report is generated for the task after the end date and time.

9. Change the report file format for the scheduled report by selecting it from the Report File Format list in the Delivery Options section.

Options include PDF, CSV, MS Excel, and MS Excel (Data-Only).

10. If you want to add an email recipient for the scheduled report, click the checkbox to the left of Send by Email. The Modify Scheduled Report window updates to include a field to the right of Send by Email to enter the email address for the Email recipient.

11. Enter the email address of the recipient in this field.

12. To remove an Email recipient, simply delete the entry in the email recipient field.

IMC sends an email to the email recipient (if specified) when generating a scheduled report. If you modify the email recipient, IMC sends an email to the new email address.

13. Modify the parameters, if any, located at the bottom of the Modify Scheduled Report window. Parameters include:
   - View Name: Sets the view for which a report is generated.
   - Begin Time: Sets the start time for the specific time range in a data collection period.
   - End Time: Sets the end time for the specific time range in a data collection period.

14. Click the icon in the Set Parameter field.

15. Modify the parameter setting and click OK.

16. Click OK.

Accessing scheduled report histories

IMC stores the histories of scheduled reports. To access scheduled report histories:

1. Navigate to Report→All Scheduled Reports:
   a. Click the Report tab from the tabular navigation system on the top.
   b. Click Scheduled Reports on the navigation tree on the left.
   c. Click All Scheduled Reports under Scheduled Reports from the navigation system on the left.
2. Click the History Report icon associated with the scheduled report you want to access histories for.
   - Click to page forward in the History Report List.
   - Click to page forward to the end of the History Report List.
   - Click to page backward in the History Report List.
   - Click to page backward to the front of the History Report List.
3. Click 8, 15, 50, 100, or 200 to configure how many items per page you want to view.
4. Click the View link located to the far right that is associated with the History Report you want to view.
5. Follow the online instructions to download and open the history report.

The file naming conventions for historical reports are YYYYMMDD.ext where YYYY is the four-digit value for year, MM is the two-digit value for month, DD is the two-digit value for day, and ext is the three-character value for the file format type.

Deleting scheduled report histories

To delete scheduled report histories:
1. Navigate to Report→All Scheduled Reports:
   a. Click the Report tab from the tabular navigation system on the top.
   b. Click Scheduled Reports on the navigation tree on the left.
   c. Click All Scheduled Reports under Scheduled Reports from the navigation system on the left.
2. Click the History Report icon associated with the scheduled report you want to access histories for.
   - Click to page forward in the History Report List.
   - Click to page forward to the end of the History Report List.
   - Click to page backward in the History Report List.
   - Click to page backward to the front of the History Report List.
3. Click 8, 15, 50, 100, or 200 to configure how many items per page you want to view.
4. Click the checkbox to the left of the File Name of the reports you want to delete.
5. Click Delete.
6. Click OK to confirm deletion of the history reports you want to delete.

Suspending and resuming scheduled reports

To suspend and resume scheduled reports:
1. Navigate to Report→All Scheduled Reports:
   a. Click the Report tab from the tabular navigation system on the top.
   b. Click Scheduled Reports on the navigation tree on the left.
   c. Click All Scheduled Reports under Scheduled Reports from the navigation system on the left.
2. If the scheduled report is suspended, click the Resume icon in the Operation field to resume the execution of the scheduled report. This Operation field updates to include the Suspend icon.
If the scheduled report is active, click the **Suspend** icon in the **Operation** field to suspend the execution of the scheduled report. The **Operation** field updates to include the **Resume** icon.

### Deleting scheduled reports

To delete a scheduled report:

1. Navigate to **Report**→**All Scheduled Reports**:
   a. Click the **Report** tab from the tabular navigation system on the top.
   b. Click **Scheduled Reports** on the navigation tree on the left.
   c. Click **All Scheduled Reports** under **Scheduled Reports** from the navigation system on the left.
2. Click the **Delete** icon associated with the scheduled report you want to delete.
3. Click **OK** to confirm deletion of the scheduled report.

### Quick custom reports

Quick Custom reports allow you to generate reports based on templates they create that contain details about devices and links. Reports based on devices details allow you to generate reports that include information on device status, label, IP address, MAC address, device type, model, vendor, location, contact, sysOID, hardware version, software version, serial number and product number for managed devices.

Quick custom reports based on link details include information on devices connected to either end of a link. This information includes device name, port, IP address, and port speed.

To generate quick custom reports for device or link details, you must first create templates based on one of these two report types, device or link. Once quick custom templates have been created, the templates become available in the **Add My Quick Report** dialog box. This enables you to add quick custom reports to their **Report** main page for quick and efficient access to device and link detailed reports.

### Quick custom report templates

Before a quick custom report can be added to each operator’s **Report** main page, custom report templates must be created. Once created, the custom templates become available as the foundation reports added to an operator’s main **Report** page via the **My Quick Report** link.

### Accessing the quick custom report template list

To access the quick custom report template list:

1. Navigate to **Report**→**Quick Custom Report Template List**:
   a. Click the **Report** tab from the tabular navigation system on the top.
   b. Click **Quick Custom Reports** on the navigation tree on the left.
   c. Click **Report Template List** under **Quick Custom Reports** from the navigation system on the left.

   IMC displays all quick custom report templates in the **Quick Custom Report Template List**.

### Quick custom report template

- **Template Name**: Contains the name of the user-defined template.
- **Type**: Contains the type of report that is generated by the associated template.
There is just one type of report that the Quick Custom Reports offers: reports based on resource information, or the Resource Statistics Report.

- **Template Content**: Indicates on which type the template is based: Device Details or Link Details.
- **Details**: Contains a link to more detailed information on the template.
- **Modify**: Contains a link for modifying the associated template.
- **Delete**: Contains a link, if permitted, for deleting the associated template.

You can sort the Report Template List by the Template Name, Type, or Template Content field by clicking the column label to sort the list by the selected field. The column label is a toggle switch that allows you to toggle between the various sort options specific to each field.

If there are multiple entries in the Quick Custom Report Template List, the following navigation aids may appear:

- Click to page forward in the Quick Custom Report Template List.
- Click to page forward to the end of the Quick Custom Report Template List.
- Click to page backward in the Quick Custom Report Template List.
- Click to page backward to the front of the Quick Custom Report Template List.

2. Click 8, 15, 50, 100, or 200 from the right side of the main pane to configure how many items per page you want to view.

3. Do one of the following:
   - To search by template name, enter the name of the template in the Template Name field of the Query Template section and click Query to begin your search, or
   - To search by template type, select the template type you want to create a report for from the Type list and click Query to begin your search.

### Running a report via the quick custom report template

To run an ad hoc report via a quick custom report template:

1. Navigate to Report → Quick Custom Report Template List:
   a. Click the Report tab from the tabular navigation system on the top.
   b. Click Quick Custom Reports on the navigation tree on the left.
   c. Click Report Template List under Quick Custom Reports from the navigation system on the left.

   The Quick Custom Report Template List displays in the main page.

2. Click the active link in the Template Name field for the quick custom report you want to run.

   The report displays in an Intelligent Analysis Report Viewer window.

### Exporting a quick custom report

To export a Quick Custom report

1. Click the icon for the file type you want to export located on the toolbar in the upper left corner of the report.

2. Select the type of file you want to export.
   - Click for Adobe Acrobat Reader.
Adding a quick custom report template

To add a quick custom report template:

1. Navigate to Report→Quick Custom Report Template List:
   a. Click the Report tab from the tabular navigation system on the top.
   b. Click Quick Custom Reports on the navigation tree on the left.
   c. Click Report Template List under Quick Custom Reports from the navigation system on the left.

2. Click Add.

3. Select the template metadata type you want to create by clicking the radio button ☑ to the left of the metadata Name in the Quick Report Metadata List.
   - Device Details: Information available from this metadata type includes device label, status, IP address, MAC address, device type, model, vendor, location, contact, sysOID, hardware version, software version, serial number and product number.
   - Link Details: Information available from this metadata type includes device name, port, IP address, and port speed for each side of a link.

4. Click Next.

5. Select the columns you want to add to the report template by clicking the checkboxes ☑ to the left of the column names you want to add.

6. Change column order of appearance as needed:
   - To change report column order of appearance, move a column down click the down arrow key ▼ associated with the column you want to move down until you have moved it to the desired position.
   - To move a column up, click the up arrow key ► associated with the column you want to move up until you have moved it to the desired position.

7. Click Next.

8. Enter a unique name for this quick custom template in the Template Name field.
   You cannot change the name of a template once you have created it.

9. Enter a brief description for this quick custom template in the Description field.

10. To grant access to this report template, click the checkboxes ☑ to the left of the operator groups you want to grant access to.

11. Click Finish.

Now that you have created a quick custom report template, you can add the report to their Report main page for quick access.
Modifying a quick custom report template

To modify a quick custom report template:

1. Navigate to Report→Quick Custom Report Template List:
   a. Click the Report tab from the tabular navigation system on the top.
   b. Click Quick Custom Reports on the navigation tree on the left.
   c. Click Report Template List under Quick Custom Reports from the navigation system on the left.

2. Click the Modify icon associated with the report template you want to modify.

3. Do one of the following:
   o To remove columns from the template, click the checked boxes next to the column names, or
   o To add columns from the template, click the checkboxes next to the column names, or
   o To change report column order of appearance, move a column down click the down arrow key associated with the column you want to move down until you have moved it to the desired position, or
   o To move a column up, click the up arrow key associated with the column you want to move up until you have moved it to the desired position.

4. Click Next.

5. Modify the description as needed in the Description field.

6. Do one of the following:
   o To change access to this report template, click the checkboxes to the left of the operator groups you want to grant access to, or
   o To remove operator groups, click the checked boxes to the left of the operator groups you want to revoke access for.

7. Click Finish.

Deleting a quick custom report template

To delete a quick custom report template:

1. Navigate to Report→Quick Custom Report Template List:
   a. Click the Report tab from the tabular navigation system on the top.
   b. Click Quick Custom Reports on the navigation tree on the left.
   c. Click Report Template List under Quick Custom Reports from the navigation system on the left.

2. Click the Delete icon associated with the report template you want to delete.

3. Click OK to confirm deletion of the selected template.

Managing quick custom reports

Once custom report templates have been created, they become available for adding to each operator’s custom My Quick Reports view. You add custom reports to this view via user-defined templates. For more information on creating Quick Custom Report Template, see "Quick custom report templates" (page 866).
Adding a report simply makes the report template available on the operators Report page for quick access. Once it is added to the Report main page, you can run the report, entering the required parameters, if any, before viewing the report’s contents.

Adding a quick custom report

To add a Quick Custom report:
1. Click the Report tab from the tabular navigation system on the top.
2. Click the Add My Quick Report link located below and to the right of the tabular navigation system.
3. Locate the template you want to use for this Quick Custom report.
4. If your Quick Custom Report Template List contains multiple entries, the following navigation aids may appear:
   - Click ▶ to page forward in the Template List.
   - Click ▶ to page forward to the end of the Template List.
   - Click ◀ to page backward in the Template List.
   - Click ◀ to page backward to the front of the Template List.
5. To more quickly access the template you want to create a Quick Custom report for, do one of the following:
   - Sort the template list by clicking Template Name, Type, or Template Content, or
   - Search by template name by entering the name of the template in the Template Name field of the Query Template section and clicking Query to begin your search, or
   - Click Reset to reset the search.
6. Click the checkboxes □ next to the template names you want to create Quick Custom reports for.
7. Click OK.
   The templates you selected now appear categorized by Report Template type under My Quick Reports in the main pane of the Report page.

Viewing a quick custom report

To view a Quick Custom report:
1. Click the Report tab from the tabular navigation system on the top.
2. Click the report name you want to view under the My Quick Reports [Edit Mode] section heading.
3. Verify that this link displays [Edit Mode] as this confirms that you are in View Mode.
   The My Quick Reports [Edit Mode] section heading appears only after you have added Quick Custom reports.
   In addition, the [Edit Mode/View Mode] link is a toggle switch between editing and viewing Quick Custom reports.
   Use the [Edit Mode/View Mode] link to toggle between viewing and editing Quick Custom reports.
4. Click OK to view the selected report.
   The report displays in an Intelligent Analysis Report Viewer window.
Exporting a quick custom report

To export a Quick Custom report:
1. Click the Report tab from the tabular navigation system on the top.
2. Click the report name you want to view under the My Quick Reports [Edit Mode] section heading.
3. Verify that this link displays [Edit Mode] as this confirms that you are in view mode.
4. Click OK to view the selected report.
The report displays in an Intelligent Analysis Report Viewer window.
5. To export a Quick Custom report, click the icon for the file type you want to export located on the toolbar in the upper left corner of the report:
   - Click for Adobe Acrobat Reader.
   - Click for Microsoft Excel.
   - Click for Comma Separated Values.
   - Click for HTML.
6. Follow the download or export instructions for each file format.
7. Click OK.

Modifying a quick custom report

Only the report name and description of a Quick Custom report can be modified. To modify these fields:
1. Click the Report tab from the tabular navigation system on the top.
2. Click [Edit Mode] to the right of My Quick Reports [Edit Mode].
3. Verify that this link displays [View Mode] as this confirms that you are in edit mode.
4. Click the Edit icon to the right of the report you want to modify:
   - To modify the display name, delete the existing value in the Display Name field and enter the new report name, or
   - To modify the report description, delete the existing description in the Description field and enter a new description.
5. Click OK to accept your changes.

Deleting a quick custom report

To delete a Quick Custom report:
1. Click the Report tab from the tabular navigation system on the top.
2. Click [Edit Mode] to the right of My Quick Reports [Edit Mode].
3. Verify that this link displays [View Mode] as this confirms that you are in edit mode.
4. Click the Delete icon to the right of the report you want to delete.
5. Click OK to confirm deletion.
14 Support and other resources

Contacting HP

For worldwide technical support information, see the HP support website:
http://www.hp.com/support

Before contacting HP, collect the following information:
- Product model names and numbers
- Technical support registration number (if applicable)
- Product serial numbers
- Error messages
- Operating system type and revision level
- Detailed questions

Subscription service

HP recommends that you register your product at the Subscriber’s Choice for Business website:
http://www.hp.com/go/wwalerts

After registering, you will receive email notification of product enhancements, new driver versions, firmware updates, and other product resources.

Related information

Documents

To find related documents, browse to the Manuals page of the HP Business Support Center website:
http://www.hp.com/support/manuals
- For related documentation, navigate to the Networking section, and select a networking category.
- For a complete list of acronyms and their definitions, see HP A-Series Acronyms.

Websites

- HP.com: http://www.hp.com
- HP Networking: http://www.hp.com/go/networking
- HP manuals: http://www.hp.com/support/manuals
- HP download drivers and software: http://www.hp.com/support/downloads
- HP software depot: http://www.software.hp.com
Conventions

This section describes the conventions used in this documentation set.

GUI conventions

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Boldface</strong></td>
<td>Window names, button names, field names, and menu items are in bold text. For example, the <strong>New User</strong> window appears; click <strong>OK</strong>.</td>
</tr>
<tr>
<td>→</td>
<td>Multi-level menus are separated by arrows. For example, <strong>File→Create→Folder</strong>.</td>
</tr>
</tbody>
</table>

Symbols

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>△ <strong>CAUTION</strong></td>
<td>An alert that calls attention to important information that if not understood or followed can result in data loss, data corruption, or damage to hardware or software.</td>
</tr>
<tr>
<td><strong>NOTE</strong></td>
<td>An alert that contains additional or supplementary information.</td>
</tr>
</tbody>
</table>

Port numbering in examples

The port numbers in this document are for illustration only and might be unavailable on your device.

About HP IMC documents

The following are the documents available for HP IMC:

<table>
<thead>
<tr>
<th>Documents</th>
<th>Purposes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Hardware specifications and installation</strong></td>
<td></td>
</tr>
<tr>
<td>HP IMC Getting Started Guide</td>
<td>Quickly guides you through the IMC main features and troubleshooting common problems.</td>
</tr>
<tr>
<td>HP IMC Installation Guide</td>
<td>Provides a complete guide to IMC platform and component installation and deployment.</td>
</tr>
<tr>
<td>HP IMC Probe Installation Guide</td>
<td>Provides a complete guide to IMC Probe installation and deployment.</td>
</tr>
<tr>
<td>SQL Server 2005 Installation and Configuration Guide</td>
<td>Guides you through installing SQL Server 2005 for IMC.</td>
</tr>
<tr>
<td>SQL Server 2008 Installation and Configuration Guide</td>
<td>Guides you through installing SQL Server 2008 for IMC.</td>
</tr>
<tr>
<td>SQL Server 2008 R2 Installation and Configuration Guide</td>
<td>Guides you through installing SQL Server 2008 R2 for IMC.</td>
</tr>
<tr>
<td>Oracle 11g Installation and Configuration Guide(for Linux)</td>
<td>Guides you through installing Oracle 11g on Linux for IMC.</td>
</tr>
<tr>
<td>Oracle 11g R2 Installation and Configuration Guide(for Linux)</td>
<td>Guides you through installing Oracle 11g R2 on Linux for IMC.</td>
</tr>
<tr>
<td>MySQL 5.5 Installation and Configuration Guide (for Linux)</td>
<td>Guides you through installing MySQL 5.5 on Linux for IMC.</td>
</tr>
<tr>
<td>Documents</td>
<td>Purposes</td>
</tr>
<tr>
<td>--------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------</td>
</tr>
<tr>
<td>MySQL 5.5 Installation and Configuration Guide (for Windows)</td>
<td>Guides you through installing MySQL 5.5 on Windows for IMC.</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux 5 Installation Guide</td>
<td>Guides you through installing Red Hat Enterprise Linux 5 for IMC</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux 6.1 Installation Guide</td>
<td>Guides you through installing Red Hat Enterprise Linux 6.1 for IMC</td>
</tr>
<tr>
<td><strong>Software configuration</strong></td>
<td></td>
</tr>
<tr>
<td>HP IMC Base Platform Administrator Guide</td>
<td>Describes operation procedures on the IMC base platform.</td>
</tr>
<tr>
<td>HP IMC Network Traffic Analyzer Administrator Guide</td>
<td>Describes operation procedures on the IMC Network Traffic Analyzer.</td>
</tr>
<tr>
<td>Online Help</td>
<td>Helps you properly use IMC.</td>
</tr>
<tr>
<td><strong>Operations and maintenance</strong></td>
<td></td>
</tr>
<tr>
<td>Readme</td>
<td>Provides latest IMC release information.</td>
</tr>
</tbody>
</table>
Index

access and core device alarm settings
   adding a core device, 605
   adding an access device, 604
   deleting a core device, 605
   deleting an access device, 605
access configuration
   binding multiple terminal interfaces with auto scan, 335
   manually binding a terminal to interfaces, 334
   manually binding terminals, 337
   manually unbinding a terminal from interfaces, 334
   manually unbinding terminals, 338
   refreshing switch access binding list, 338
   refreshing terminal access binding list, 335
   searching switch access bindings, 337
   searching terminal access bindings, 333
   switching binding using auto scan, 338
   switching terminal access binding, 336
   viewing switch access binding list, 336
   viewing terminal access binding list, 332
access control list management
   deploying ACLs using the ACL deployment wizard, 781
   managing ACL resources, 696
   managing ACL templates, 657
   managing device ACL configurations, 753
   simplifying ACL rule creation, 645
   using the ACL assistant, 645
access port tab
   modifying PVID, 836
   viewing access ports, 835
accessing device details
   actions, 215
   actions, delete, 217
   actions, manage/unmanage, 216
   actions, MIB management, 219
   actions, open device panel, 220
   actions, open web manager, 217
   actions, ping, 218
   actions, refresh, 216
   actions, SSH, 221
   actions, switches, 221
   actions, synchronize, 216
   actions, Telnet, 217
   actions, Telnet/SSH proxy, 219
   actions, traceroute, 218
   actions, view topology, 219
   alarms, 214
   configuration center, 230
   configure all device types, 222
   configure monitored services, 214
   configure specific device types, 228
   device management, 231
   device panel chassis menu, 220
   device panel port menu, 221
   interface details, 267
   interface management, 272
   monitored services, 213
   performance monitor, 275
   performance monitoring, 215, 228
   protocol management, 261
   right navigation tree, 215
   service monitoring, 213
   VLAN management, 267
accessing the network assets
   viewing audit history, 346
   viewing interface list, 347
   viewing network asset details, 346
ACL device configurations
   device configuration history, 773
   device configuration page, 757
   device definitions, 758
   device flow template applications, 779
   device flow templates, 776
   packet filtering, 766
   rule sets, 763
   templates, 765
   time ranges, 771
   view ACL page, 762
   VLAN packet filtering, 766
ACL device list management
   ACL device configurations, 756
   customizing polling for devices, 755
   querying the device list, 755
   synchronizing devices, 755
   viewing the device list, 754
adding a rule in a rule set
   advanced rule to an advanced rule set, 744
   basic rule to a basic ACL rule set, 743
   link rule in a link rule set, 746
   user-defined rule to a user-defined rule set, 748
adding a time range
configuring cyclic time ranges, 655
configuring fixed time ranges, 654
adding an email alarm notification rule
  by custom view, 587
  by IP address, 587
  by network segment, 588
adding devices by importing
  exporting devices, 174
  importing devices, 172
  importing devices from NNMi, 175
adding devices in IMC
  auto discovery, 157
  importing, 171
  manually, 153
adding devices manually
  adding, 153
  editing SNMP settings manually, 154
  editing SSH settings manually, 156
  editing Telnet settings manually, 155
  using an existing SSH template, 156
  using an existing Telnet template, 155
  using existing SNMP template, 155
adding rule sets
  advanced rule set, 707
  basic rule set, 705
  link rule set, 711
  user-defined rule set, 714
adding trap definitions
  using macros in the definition field, 546
adding user-defined trap filter rules
  adding interfaces by advanced query, 534
  selecting interfaces by view, 534
address binding
  bind to MAC address port, 239
  configure to global MAC address configuration, 240
  delete MAC port binding, 240
  modify a port MAC address learning management, 240
  modify MAC address port binding configuration, 239
advanced alarm query
  entering search criteria, 571
advanced auto discovery
  editing SNMP settings manually, 162
  editing SSH settings manually, 164
  editing Telnet settings manually, 163
  exporting reports, 165
  importing network segment addresses, 166
  network segment based discovery, 166
  printing reports, 165
  using an existing SNMP template, 163
  using an existing SSH template, 164
  using an existing Telnet template, 163
alarm details
  alarm actions in alarm details page, 568
  alarm relation report, 569
  viewing, 568
alarm performance and resource widgets
  alarm TopN, 33
  bandwidth utilization in % TopN, 37
  bandwidth utilization out % TopN, 38
  CPU utilization % TopN, 34
  custom topology, 42
  customize TopN, 38
  device response time TopN, 36
  device unreachability TopN, 36
  device view, 40
  IP topology, 41
  memory utilization % TopN, 35
  network, 39
  port group, 43
  TopN, alarm, 33
  TopN, bandwidth utilization in %, 37
  TopN, bandwidth utilization out %, 38
  TopN, CPU utilization %, 34
  TopN, customize, 38
  TopN, device response time, 36
  TopN, device unreachability %, 36
  TopN, memory utilization %, 35
alarm relation report
  exporting alarm relation report data, 569
  printing to PDF, 569
alarm sound settings
  disable, 46
  enable custom settings, 46
  enable system-defined settings, 46
alarm statistics
  creating user-defined alarm statistics charts, 585
  viewing alarm statistics charts, 584
allocating IP addresses
  adding an IP segment, 318
  allocating IP addresses using auto scan, 320
  allocating IP addresses using import IP address, 321
  manually allocating IP addresses, 319
  modifying an IP segment, 319
  restoring an IP segment, 319
  restoring IP address allocations, 321
  viewing the IP segment list, 317
asset OID
  adding an asset OID, 350
  deleting an asset OID, 351
modifying an asset OID, 351
querying asset OID list, 350
viewing asset OID list, 349
auditing configurations
backup report, 482
baseline report, 483
software baseline report, 487
software update report, 486
auto discovery
adding devices through basic auto discovery, 157
advanced auto discovery, 160
ARP-based discovery, 160
basic discovery exporting reports, 160
basic discovery printing reports, 159
IPsec-based discovery, 160
PPP-based discovery, 160
routing-based discovery, 160
VPN-based discovery, 160
automatic deployment plan management
accessing the automatic deployment plan page, 452
adding an automatic deployment device, 455
adding an automatic deployment plan, 453
deleting a device from an automatic deployment plan, 468
deleting an automatic deployment plan, 454
importing devices into an automatic deployment plan, 465
manually editing SNMP settings, 458, 463
manually editing SSH settings, 459, 464
manually editing Telnet settings, 458, 463
modifying an automatic deployment device, 459
modifying an automatic deployment plan, 453
modifying the configure device information, 462
modifying the software to deploy information, 460
trigerring automatic deployment on devices, 469
using existing SNMP templates, 458, 463
using existing SSH templates, 459, 464
using existing Telnet templates, 459, 464
viewing automatic deployment execution results, 469
viewing detailed information about automatic deployment devices, 454
automatic device configuration backups
accessing, 474
adding, 475
deleting, 476
disabling, 477
enabling, 477
modifying, 476
viewing backup history, 477
backup history reporting
accessing, 478
backup history detailed information, 480
querying, 479
re-executing a failed backup, 481
re-executing a partially successful backup, 481
backup policy options
setting the alarm generation mode, 141
setting the max backup configuration files, 142
basic alarm query
entering search criteria, 570
browsing alarms
alarm details, 568
alarm statistics, 584
browsing all alarms, 579
browsing real-time alarms, 571
browsing root alarms, 574
faulty devices, 584
querying alarms in IMC, 570
TopN, 585
browsing real-time alarms
alarm actions in all alarms page, 580
customizing all alarms list columns, 582
deleting alarms from root alarms list, 583
deleting alarms from the all alarms page, 583
exporting alarms from all alarms page to Excel, 583
querying alarms in all alarms page, 581
recovering alarms from all alarms page, 582
taking alarm actions in all alarms page, 581
viewing alarm details from all alarms page, 581
viewing alarm relation report, 581
browsing root alarms
deleting alarms from the root alarms list, 578
recovering alarms from the root alarms view, 578
taking actions from the alarms details page, 577
taking actions from the root alarms page, 575
viewing alarm details from the root alarms page, 577
viewing alarm relation report, 577
browsing Syslog entries
export Syslog entries, 554
Syslog list, 554
browsing Syslog to alarm rules
alarm recovery, 564
check task history
delete check task history, 514
query check task history, 513
view check task history, 512
check tasks
adding a check task, 509
deleting a check task, 510
viewing check task details, 508
viewing the check task list, 507
checking device configurations
using batch mode to check SSH settings, 282
using batch mode to check Telnet settings, 282
comparing device configurations
Configuration Center, 440
general compare, 441
compiled MIB
compiling a MIB, 138
removing a compiled MIB, 139
compiling definition file
control initialization, 396
operations element, 386
operations element properties, 387
parameter element, 391
parameter view control, 393
RestAction and Asn1Action, 389
variable element, 387
compiling device capability set definition file
sysOID element, 400
compliance check
check task history, 512
check tasks, 507
compliance policy, 489
configuration check using the display command, 521
fixing violating devices, 510
rule examples, 503
task execution and configuration retrieval report, 514
compliance policy
adding a rule, 493
creating, 493
deleting, 502
disabling a single policy, 502
disabling all policies, 503
enabling all policies, 502
enabling single, 502
modifying, 497
modifying incompliant settings, 495
querying, 493
viewing detailed information about a rule, 491
viewing detailed information about the compliance policy, 490
viewing the compliance policy list, 489
configuration
file transfer mode options, 140
configuration and change management
auditing configurations, 481
auto backup plan, 403
comparing device configurations, 440
compliance check, 403, 489
configuration audit and reports, 403
configuration compare, 403
configuration templates, 402
deploying configurations using the deployment guide, 441
deploying software using the deployment guide, 441
managing automatic backup plans, 474
managing automatic deployment plans, 451
managing deployment tasks, 445
managing device configurations with templates, 419
managing the software library, 433
software library, 402
software update, 403
using the Configuration Center, 404
configuration backup report
accessing, 482
exporting, 483
querying, 482
restoring, 483
configuration baseline report
comparing files the configuration baseline report, 485
querying the configuration baseline report, 484
restoring a configuration file from the baseline report, 485
viewing the configuration baseline report, 483
configuration center
back-up configuration files, 230
backup policy options, 141
device default startup configuration, 231
set auto backup attributes, 230
Configuration Center
configuring the first or left file, 440
configuring the second or right file, 441
Configuration Center device configuration options
backing up configurations from the configuration center, 418
backup history, 409
clean device space, 415
comparing configuration files, 411
comparing device configurations, 417
configuring first configuration file, 417
configuring left configuration file, 417
configuring right configuration file, 417
configuring second configuration file, 417
configuring the first file, 412
configuring the left file, 412
configuring the right file, 413
configuring the second file, 413
creating a configuration template using save as, 414
deploying a file from the configuration center, 419
deploying configurations from the Configuration Center, 418
deploying software from the Configuration Center, 417
establishing a configuration file baseline, 413
establishing a software baseline, 416
management page details, 407
management summary, 408
modifying a backup configuration file, 410
restoring a configuration file, 411
restoring a configuration from the configuration center, 418
software update history, 414
viewing the latest running configuration, 407
viewing the latest startup configuration, 406
viewing the latest startup configuration, stackable devices, 406, 407
configuration check using the display command
accessing the configuration check display command list, 521
adding a configuration check display command, 522
deleting configuration check display commands, 523
modifying configuration check display commands, 522
configuration for all device types
modify system group attributes, 223
modifying ping parameters, 227
modifying poll interval, 227
modifying SNMP settings, 224
modifying SOAP settings, 226
modifying Telnet settings, 225
modifying web manager parameters, 228
using existing SNMP templates, 224
using existing SOAP templates, 227
using existing SSH templates, 226
using existing Telnet templates, 225
configure for all device types
modify SSH settings, 225
configuring alarm notifications
access device alarm settings, 604
core device alarm settings, 604
managing alarm forwarding, 598
managing email alarm notification rules, 586
managing SMS alarm notifications, 593
configuring alarms for Syslog messages
browsing Syslog templates, 557
copying system Syslog templates, 560
copying user-defined Syslog templates, 560
creating user-defined Syslog templates, 558
deleting user-defined Syslog templates, 560
modifying user-defined Syslog templates, 559
using Syslog templates, 557
configuring device categories, 98
configuring IMC for alarm notifications
IMC hierarchical alarm configuration, 136
integrating alarms into other management systems, 136
mail server settings, 134
SMSC settings, 135
configuring IMC for use
configuration center options, 140
group management, 125
managing network resources, 73
MIB management, 137
operator management, 102
resource management, 73
resources, securing and accessing, 72
securing and accessing resources, 72
system settings and maintenance functions, 143
configuring servers in virtual network manager
adding port group, 364
adding vSwitch, 363
refreshing server details page, 364
configuring SNMP settings
editing SNMP settings manually, 276
using existing SNMP templates, 276
configuring SSH settings
editing SSH settings manually, 279
using existing SSH templates, 279
configuring Telnet settings
editing Telnet settings manually, 277
using existing Telnet templates, 278
configuring vendor and device information
device models, 95
device series, 93
device vendor list, 91
configuring virtual machines in virtual network manager
  configuring auto migration, 366
  joining a virtual machine, 365
  manually migrating a virtual machine, 365
  modifying a VM profile, 366
  modifying the advanced properties of a port group, 371
  modifying the advanced properties of a vSwitch, 371
  querying migration recommendations, 368
  querying migration reports, 370
  viewing migration reports of a virtual machine, 369
  viewing virtual machine recommendations, 367

conventions
  command, 872
  GUI, 872
  symbols, 872

creating a configuration template
  adding a configuration template using file import, 424
  adding a template manually, 426
  adding a template using a backup file, 423

creating ACL templates
  advanced, 662
  basic, 660
  link template, 666
  user-defined template, 668

creating user-defined Syslog templates
  guidelines for the template content field, 559

custom view
  deleting custom views, 204

custom views
  accessing, 201
  adding devices, 204
  creating, 202
  managing, 202
  modifying, 203
  removing devices, 204

customizing my real time report page
  resetting my report, 850

customizing topology maps
  right mouse-click management, 186

data analysis management
  managing the data analysis project list, 149

data export
  data export considerations, 148
  export settings, 147
  export triggers, 147
  defining background custom script
    compiling definition file, 386
    compiling device capability set definition file, 399
    registering service operation, 386
    replaceable variable list, 400

defining specific devices
  defining CleanupParser, 382
  defining parser service, 382
  defining software deployment service, 380

deploying ACLs using the ACL deployment wizard
  managing deployments using the ACL deployment wizard, 786
  managing the deployment task list, 781

deploying configurations and software using the deployment guide
  device configuration, 442
  file, 443
  OSM software, 444
  restoring device configuration, 444
  restoring device software, 444
  software, 442

deploying VLANs using batch mode
  for access ports, 845
  for hybrid ports, 846
  for trunk ports, 846
  for VLAN creation, 844

device categories
  adding, 99
  deleting, 99
  modifying, 99
  viewing, 98

device groups
  adding, 127, 128
  adding to groups in ungrouped devices, 130
  deleting, 128
  modifying, 127
  removing, 129
  removing multiple devices, 129
  viewing device groups, 125
  viewing the device list, 126
  viewing ungrouped devices list, 129

device list management options
  adding, 300, 309
  adding monitor, 306, 315
  backup configuration, 307, 316
  canceling monitor, 306, 315
  check SSH settings, 313
  check Telnet settings, 312
  checking SSH settings, 304
  checking Telnet settings, 304
  deleting, 301, 310
  deploying software, 307, 315
  managing, 301, 310
poll interval settings, 305, 314
rebooting device, 306, 314
refreshing, 303, 311
removing, 301, 310
saving configuration, 305, 314
SNMP settings, 303, 312
SSH settings, 304, 313
synchronizing, 302, 311
Telnet settings, 303, 312
unmanaging, 302, 311

device management
adding a mirror group, 235
address binding, 238
configuring MG mirrors, 235
configuring MG monitors, 236
configuring MG reflectors, 236
deleting mirror groups, 238
displaying mirror group information, 234
editing a mirror group, 235
environment monitor, 233
hardware information, 240
interface 802.1X configuration, 245
IPv6 information, 241
mirror group, 234
PoE management for switches, 244
port aggregation, 242
port mode switch, 241
RADIUS server configuration, 245
resetting a device, 232
RMON, 248
saving configuration, 232
setting the MG VLAN ID, 237
switch MPU, 233
system information, 234
virtual connect, 246
device model
adding, 96
deleting, 98
modifying, 97
viewing, 96
device series
adding, 94
deleting, 95
modifying, 95
viewing, 93
device vendor list
adding, 92
deleting, 93
modifying, 93
viewing, 91
device view
accessing the device view, 176
accessing the IP view, 178
accessing the network topology view, 180
customizing topology maps, 186, 188
managing topology maps, 189
manually configuring topology maps, 189
navigating the network topology interface, 180
stack topology, deleting invalid stack members, 198
stack topology, managing stack devices with, 196
topology map toolbar, 181
topology maps, accessing rooms, 191
topology maps, accessing wiring cabinets, 192
 topology maps, adding a building, 191
topology maps, adding a cloud, 190
topology maps, adding a room, 190
topology maps, adding data centers, 190
topology maps, automatically building, 193
topology maps, data center, 189
topology maps, managing devices from, 195
topology monitoring and management, 182
traffic topology, viewing traffic with, 198
vManager topology, viewing physical servers
managed by, 200
VNM topology, viewing virtual network with, 199

EAD. See Endpoint Admission Defense

establishing password strategies
configuring a password strategy, 112
event and alarm management
browsing alarms, 567
configuring alarm notifications, 586
description, 524
Syslog management, 553
trap management, 525
traps, 524
executing actions for attack alarms
executing a manual action for an attack alarm, 812
viewing the execution result report, 814
extending a customized function
defining background custom script, 386
extending an existing function
creating a drive folder, 375
creating a drive index file, 375
creating a vendor folder, 374
creating drive definition file, 376
defining actions for a component, 379
defining CLICommon common service, 378
defining services for a component, 379
defining specific services, 380
defining the Perl script, 384
defining the TCL script, 384
filter traps with existing rules
modifying duplicate trap filter rules, 529
modifying intermittent trap filter rules, 531
modifying unknown trap filter rules, 532
modifying unmanaged device trap filter rules, 533
viewing trap filter rules, 528
filter traps with user-defined rules
adding user-defined trap filter rules, 533
deleting user-defined trap filter rules, 537
modifying user-defined trap filter rules, 536
filtering Syslog entries
 disabling Syslog filtering rules, 557
 enabling Syslog filtering rules, 557
 viewing Syslog filtering rules, 556
 generate alarms from traps
 browsing trap to alarm rules, 537
 copying trap to alarm rules, 540
 creating user-defined trap alarm rules, 538
 disabling trap to alarm rules, 542
 enabling trap to alarm rules, 542
 modifying trap to alarm rules, 540
 trap to alarm upgrade strategy, 539
 global search
 advanced device search, performing, 63
 advanced interface search, performing, 64
 advanced user search, performing, 64
 basic device search, performing, 62
 basic user search, performing, 63
 performing a basic device search, 62
 performing a basic user search, 63
 performing an advanced device search, 63
 performing an advanced interface search, 64
 performing an advanced user search, 64
 global VLAN management
 adding devices to a global VLAN, 828
 creating a global VLAN, 827
 deleting a global VLAN, 828
 deleting a VLAN from devices, 829
 global VLAN query, 827
 viewing the global VLAN list, 826
 group management
 configuring IMC for alarm notifications, 134
 device groups, 125
 user groups, 131
 history access log
 deleting history access logs, 330
 immediately retrieve history access log list, 329
 periodically retrieve data, 329
 querying history access log, 329
 refreshing history access log page, 330
 viewing history access log list, 328
 viewing real-time location, 329
 hybrid port tab
 adding, 840
 deleting, 841
 modifying, 840
 viewing, 839
 IMC
 access control list management, 644
 base platform features, 1
 configuration and change management, 402
 configuration for use, 72
 customization, 374
 event and alarm management, 524
 how it works, 15
 implementation planning, 20
 interface exploration, 29
 introduction, 1
 performance management, 606
 reporting, 848
 resource management, 152
 security control, 800
 security control center, 800
 service modules, 1
 SOA framework, 1, 18
 support for extending and customizing functions to third party devices, 374
 third party device support, 374
 VLAN management, 826
 IMC features
 base platform, 1
 configuration and change management, 4
 global ACL management, 7
 global VLAN management, 8
 My Favorites, 10
 network asset management, 5
 performance monitoring and management, 6
 quick custom reports, 9
 real time fault management, 5
 real time reports, 9
 reporting, 9
 resource management, 3
 role based administrative controls, 2
 security monitoring, 8
 user interface, 10
 virtual network manager, 9
 IMC hierarchical alarm configuration
 configuring hierarchical alarm configuration, 136
 IMC home page operations
 adding a space, 31
 adding new widget to a space, 31
 changing widget layout of space, 32
 collapsing a widget, 32
collapsing all widgets, 32
deleting a space, 31
deleting a widget, 33
display widget in a new window, 33
expanding a widget, 32
expanding all widgets, 32
freezing space tab, 30
manually refresh widget, 33
maximizing widget, 33
new window, display widget, 33
renaming a space, 31
saving a space, 31
setting refresh interval, 33
space, adding, 31
space, deleting, 31
space, renaming, 31
space, saving, 31
switching between spaces, 31
unfreezing space tab, 30
widget, adding new to a space, 31
widget, changing layout space, 32
widget, collapsing, 32
widget, drag & drop, 33
widget, drag & drop widget, 33
widget, expanding, 32
widget, manually refresh, 33
widget, maximizing, 33
widgets, collapsing all, 32
widgets, expanding all, 32
implementation planning
common data requirements, 21
integration requirements, 25
needs, stakeholder, 21
network infrastructure, 23
requirements, 20
stakeholders, network infrastructure, 20
translating requirements, 25
importing ACL rule sets
advanced ACL template to advanced ACL, 731
basic ACL template to basic ACL, 728
link ACL template to link ACL, 736
user-defined ACL template to user-defined ACL, 740
initial configuration file management
accessing the initial configuration file, 470
adding an initial configuration file, 471
configuring the DHCP server, 470
copying an initial configuration file, 472
deleting an initial configuration file, 473
modifying an initial configuration file, 472
viewing detailed information of an initial configuration file, 474
integrating SSC with SMS
SMS and managed devices in the topology, 824
SMS management page in SCC, 824
SMS plug-in installation, 823
interface details
accessing the interface list, 267
accessing the interface details page, 267
change management status, 270
change up/down alarm filter, 271
change user-defined speed, 271
query IP/MAC learning, 272
refresh interface details page, 269
right navigation tree, 269
synchronize interface details page, 269
unmanage interface details page, 270
interface exploration
access device status, 45
alarm performance and resource widgets, 33
alarm sound settings, 46
breadcrumb trails, navigating IMC with, 58
customizing RSS widgets, 45
customizing spaces and system-defined widgets, 43
explore the home page, 29
floating menus, 58
global search, 62
home page basic operations, 30
home page, exploration, 29
IMC functions, navigating, 47
IMC home page, 29
IMC web interface, personalizing, 65
IMC, logout, 71
login, 29
logout of IMC, 71
navigating IMC functions, 47
navigating IMC using breadcrumb trails, 58
navigation tree, floating menus, 58
online help system, 60
personalizing the IMC web interface, 65
quick start, 58
RSS widgets, customizing, 45
settings, alarm sound, 46
spaces and system-defined widgets, customizing, 43
task management, 69
widgets, alarm performance and resource, 33
wizard center, 67
interface management
adding ports to VLANs, 273
interface IP management, 273
loopback testing, 272
port properties, 274
IP address
adding a segment, 318
adding email alarm notification rule by address, 587
allocating using auto-scan, 320
allocating using import, 321
binding multiple addresses using auto-scan, 341
locating using real-time location query, 331
manually allocating, 319
manually binding to a MAC address, 340
manually unbinding from a MAC address, 341
modifying a segment, 319
refreshing IP/MAC binding list, 342
restoring a segment, 319
restoring allocations, 321
searching for IP/MAC bindings, 340
unbinding multiple IP/MAC address bindings, 342
viewing IP/MAC binding list, 339
viewing the segment list, 317
IP to MAC address binding
  binding multiples using auto scan, 341
  manually binding, 340
  manually unbinding, 341
  refreshing the binding list, 342
  searching for bindings, 340
  unbinding multiples, 342
  viewing the binding list, 339
log files
  querying operation logs, 149
  viewing the operation logs, 148
mail server settings
  configuring email notification, 134
management
  access control list, 644
  change management, 402
  configuration, 402
  configuration and change management, 402
  event and alarm, 524
  performance, 606
  resource, 152
  VLAN, 826
managing ACL device definitions
  add use, 761
  adding an ACL to the selected device, 759
  deleting ACLs, 759
  exporting an ACL, 761
  viewing applied ACLs, 762
  viewing the ACL definition list, 758
managing ACL resources
  adding an ACL, 697
  deleting an ACL, 698
  managing ACLs, 696
managing rule sets, 698
managing rules in rule sets, 742
renaming an ACL, 698
viewing the ACL resource list, 696
managing ACL rule sets
  adding, 704
  copying, 727
  deleting, 742
  importing rule sets, 728
  modifying, 717
  viewing, 699
  viewing information for a rule set for an ACL, 700
  viewing rule information for a rule for an ACL resource, 701
  viewing rule list for an ACL resource, 699
  viewing time range information for a rule for an ACL resource, 704
managing ACL templates
  advanced, 657
  basic, 657
  copying templates, 679
  creating templates, 657, 660
  deleting templates, 680
  exporting templates, 680
  link, 657
  managing the rules in a template, 681
  modifying templates, 670
  user-defined, 657
  viewing templates, 658
managing alarm forwarding
  adding an alarm forwarding rule, 598
  copying an alarm forwarding rule, 603
  deleting an alarm forwarding rule, 603
  disabling an alarm forwarding rule, 603
  enabling an alarm forwarding rule, 603
  modifying an alarm forwarding rule, 601
managing asset information in Network Asset Manager
  adding a network asset, 352
  auditing a network asset, 354
  modifying a network asset, 352
  modifying property, 352
  refreshing a network asset details view, 354
  removing a network asset, 354
managing automatic backup plans
  automatic device configuration backups, 474
  backup history reporting, 478
  manual device configuration backups, 478
managing automatic deployment plans
  automatic deployment plan management, 452
  initial configuration file management, 470
managing deployments using the ACL deployment wizard
- deleting time ranges on devices, 791
- deploying ACL uses via deploy ACL uses, 793
- deploying ACLs to devices, 786
- removing ACL uses from devices, 796
- removing ACLs from devices, 788

managing deployment tasks
- accessing, 445
- copying, 449
- deleting a deployment task, 451
- modifying, 448
- resuming a deployment task, 450
- running, 449
- searching, 446
- suspending a deployment task, 450
- viewing execution result page, 447

managing device ACL configurations
- ACL device list management, 754

managing device ACL time ranges
- deleting time ranges, 771

managing device ACL uses for packet filtering
- adding an ACL use, 766
- deleting an ACL use, 769
- viewing the ACL use list, 766

managing device ACL uses for VLAN packet filtering
- adding an ACL use, 766
- deleting an ACL use, 769
- viewing the ACL use list, 766

managing device configuration history
- baselining, 776
- deleting, 775
- modifying, 775
- viewing an ACL configuration history entry, 774
- viewing the ACL configuration history, 773

managing device configurations with templates
- accessing configuration templates, 419
- copying a configuration template, 430
- creating a configuration template, 422
- deleting a configuration template, 433
- deploying a configuration template, 433
- exporting a configuration template, 432
- modifying a configuration template, 428
- organizing configuration templates, 421
- querying configuration templates, 420
- renaming a configuration template, 430

managing device flow template applications
- adding, 780
- deleting, 781
- viewing, 779

managing device flow templates
- adding, 777
- deleting, 779
- modifying, 778
- viewing, 776
- viewing details, 777

managing device monitors
- adding monitor instances, 616
- deleting monitor instances, 620
- displaying monitored devices only, 620
- modifying monitor instances, 618
- modifying the default indices, 621
- saving monitors to a performance view, 621

managing email alarm notification rules
- adding, 586
- copying, 592
- deleting, 592
- enabling, 592
- modifying, 589

managing filters to filter interfaces
- adding a filter, 101
- deleting a filter, 101
- viewing the filter list, 100

managing global index settings
- adding a user defined monitor, 608
- deleting a user defined monitor, 612
- modifying a global monitor, 611

managing IMC operators
- adding an administrator group operator, 115
- adding an IMC maintainer or viewer group operator, 118
- deleting an IMC operator, 123
- modifying a maintainer or viewer group operator, 120
- modifying an administrator group operator, 116
- viewing the operator list, 114

managing individual device monitoring settings
- accessing the monitor list, 613
- managing device monitors, 616
- searching for monitors, 614
- switching the monitor list, 614

managing monitor graphs
- adding, 639
- average value, 639
- current value, 639
- deleting, 641
- displaying, 641
- folding up, 642
- max value, 639
- monitoring, 640
managing rule sets
  deploying ACL rule sets, 728
managing rules in rule sets
  adding a rule in a rule set, 743
  copying a rule in a rule set, 743
  deleting a rule in a rule set, 750
managing security attack alarms
attack alarm list overview, 801
browsing real-time attack alarm list, 807
browsing the attack alarms list, 801
deleting attack alarms from the real-time attack alarm list, 808
deleting the attack alarm list, 806
executing actions for attack alarms, 812
querying the attack alarm list, 804
real-time attack alarm overview, 806
refreshing the attack alarm list, 806
refreshing the real-time attack alarm list, 808
viewing a single attack using the attack path map, 810
viewing all attacks using the attack topology map, 809
viewing attack alarm details, 803
managing security control policies
adding, 815
deleting, 820
executing, 820
modifying, 818
viewing, 815
managing services in a service list
adding, 647
deleting, 648
modifying, 648
viewing a service, 646
viewing the service list, 646
managing SMS alarm notifications
adding an SMS messaging alarm notification rule, 593
 copying an SMS messaging alarm notification rule, 597
deleting an SMS messaging alarm notification rule, 598
disabling an SMS messaging alarm notification rule, 598
enabling an SMS messaging alarm notification rule, 598
modifying an SMS messaging alarm notification rule, 595
managing the deployment task list
modifying an ACL deployment task, 783
starting an ACL deployment task, 785
viewing deployment task detailed information, 783
viewing the deployment task list, 781
managing the rules in a template
adding a link rule to an ACL template, 685
adding a user-defined rule to an ACL template, 687
adding an advanced rule to an advanced template, 682
adding rules to a template, 681
copying a rule in a template, 695
deleting rules from a template, 695
modifying a link rule in an ACL template, 692
modifying a user-defined rule in an ACL template, 694
modifying advanced rules in an ACL template, 689
modifying the rules in an ACL template, 688
managing the software library
adding OSM software to the library, 436
deleting a software library entry, 439
establishing baselines using a software library entry, 439
exporting a software library entry, 439
importing software into the library from a device, 436
importing software into the library from a file, 435
modifying a software library entry, 438
renaming a software library entry, 437
searching for a software library entry, 435
viewing the details of a software library entry, 434
viewing the software library, 433
managing time ranges
adding, 653
deleting, 656
modifying, 655
viewing, 653
viewing the time range list, 652
MIB management
 compiled MIB, 137
modify device configurations
using batch mode to configure device, 292
using batch mode to configure interface, 295
using batch mode to configure LACP, 291
using batch mode to configure management status on interfaces, 285
using batch mode to configure spanning tree protocol on switches, 288
using batch mode to configure trap destinations, 287
using batch mode to implement energy saving policies, 286
using batch mode to reboot devices, 284
using batch mode to save configure spanning tree protocol on interfaces, 290
using batch mode to save device configurations, 283
modifying a rule in a rule set
advanced in an advanced rule set, 744
basic rule in a basic ACL rule set, 743
link rule in a link rule set, 746
user-defined rule in a user-defined rule set, 748
modifying ACL rule sets
  advanced rule set, 719
  basic rule set, 717
  link rule set, 722
  user-defined rule set, 725
modifying ACL templates
  advanced template, 672
  basic template, 670
  link template, 675
  user-defined template, 678
modifying IMC passwords
  managing online operator access, 123
modifying inconsistent policies
  import rule, 497
modifying user-defined Syslog templates
  guidelines for the template content field, 559
modifying user-defined trap definitions
  restore trap conditions, 551
MSTP options for routers and switches
  configuring global MSTP settings, 262
MVM. See MPLS VPN Manager
my real-time reports
  alarm analysis reports, device connectivity detail report, 849
  alarm analysis reports, device connectivity summary report, 849
  alarm analysis reports, interface connectivity detail report, 849
  alarm analysis reports, interface connectivity summary report, 849
  alarm analysis reports, link connectivity detail report, 849
  alarm analysis reports, link connectivity summary report, 849
  alarm analysis reports, node connectivity summary report, 849
  performance analysis summary reports, custom view data summary report, 850
  performance analysis summary reports, performance view all summary report, 850
  performance analysis summary reports, performance view summary report, 850
my real-time reports
  resource statistics reports, capacity report, 849
  resource statistics reports, changes report, 849
  resource statistics reports, device asset report, 849
  resource statistics reports, device category statistic report, 849
  resource statistics reports, device history report, 849
  resource statistics reports, inventory report, 849
  resource statistics reports, misconfiguration and optimizations report, 849
  resource statistics reports, topology report, 849
  resource statistics reports, user tracking report, 849
NAM. See Network Asset Manager
accessing assets page, 345
adding an asset OID, 350
auditing network asset, 354
deleting an asset OID, 351
manually adding a network asset, 352
modifying a network asset, 352
modifying an asset OID, 351
modifying asset property, 352
performing a basic asset audit query, 356
performing advanced asset query, 348
performing an advanced asset audit query, 356
performing basic asset query, 347
querying asset OID, 350
refreshing asset details view, 354
removing an asset, 354
viewing asset audit list, 355
viewing asset list, 344
viewing asset OID list, 349
viewing device level asset details, 345
navigating IMC functions
  alarm tab, 54
  report tab, 55
  resource tab, 49, 52
  service tab, 53
  system tab, 56
  topology map, 50
  user tab, 52
navigating to the device list
  from a custom view, 300
  from the IP view, 300
navigating from a custom view, 309
navigating from the device view, 307
navigating from the IP view, 308
network asset auditing
  network asset global configuration, 357
  querying the asset audit list, 356
  viewing the asset audit list, 355
network asset manager
  asset OID, 349
  managing asset information in Network Asset Manager, 352
network asset auditing, 355
  view network assets, 344
network infrastructure
  access requirements, 24
  device series and models, 24
device vendors, 24
monitoring restrictions, 25
network topology, 23
organizational standards, 24
security policies, 25
network segment based discovery
editing SNMP settings manually, 168
inging SSH settings manually, 169
inging Telnet settings manually, 169
exporting the report, 171
rinting the report, 171
using SNMP template, 168
using SSH template, 170
using Telnet template, 169
NTA. See Network Traffic Analyzer
online help
  context sensitive help, 61
  system-wide help, 60
operator login control templates
  adding, 111
  deleting, 112
  modifying, 111
  viewing, 110
operator management
  authentication services, securing access via, 107
  establishing password strategies, 112
  managing IMC operators, 113
  managing operator groups, 103
  modifying IMC passwords, 123
  password strategies, establishing, 112
  securing access via authentication services, 107
  securing through operator login control templates, 110
organizing configuration templates
  creating, 421
  deleting, 422
  modifying, 421
organizing performance views
  creating a performance view folder, 623
  deleting a performance view folder, 624
  modifying a performance view folder, 623
performance management
  managing individual device monitoring settings, 613
  managing performance monitor settings for topology maps, 632
  managing performance option, 642
  managing performance with global index settings, 606
  managing real-time performance monitor, 634
  viewing performance reports, 621
performance monitoring
  add monitor, 229
  cancel monitor, 229
  delete performance data, 230
  device real-time monitor, 230
  performance-at-a-glance, 229
  refresh monitor instance, 229
personalizing the IMC web interface
  accessing a favorite, 65
  adding a favorite, 65
  deleting a favorite, 66
  modifying a favorite, 66
  sorting favorites, 66
ping
  modify parameters for selected device, 227
PoE management for switches
  modifying PoE port power consumption, 244
polling interval
  modify settings for selected device, 227
  using batch mode to configure, 279
port aggregation
  adding a port aggregation entry, 243
  deleting port aggregation information, 244
  modifying port aggregation information, 243
  viewing port aggregation information, 242
port groups
  adding a port, 208
  customizing columns for interface port list, 208
  deleting a port group, 209
  managing port groups, 205
  modifying a port, 208
  querying port group list, 205
  viewing the interface list of port groups, 206
PowerShell
  device access templates resource management, 86
PowerShell templates
  adding a PowerShell template, 87
  deleting a PowerShell template, 88
  modifying a PowerShell template, 88
  PowerShell template list, viewing, 86
  PowerShell template, adding, 87
  PowerShell template, deleting, 88
  PowerShell template, modifying, 88
  viewing the PowerShell template list, 86
procedure
  accessing a favorite, 65
  accessing automatic backup plans, 474
  accessing batch operations for SNMP settings, 303
  accessing batch operations for SNMP settings for devices from the device list, 312
  accessing batch operations for SSH settings, 304
accessing batch operations for SSH settings for devices from the device list, 313
accessing batch operations for Telnet settings, 303
accessing batch operations for Telnet settings for devices from the device list, 312
accessing configuration template folders, 419
accessing configuration templates, 419
accessing custom views, 201
accessing data center topology map, 189
accessing data shown in topo, 632
accessing faulty devices, 584
accessing global index settings list, 607
accessing initial configuration files, 470
accessing message history, 70
accessing network asset details, 345
accessing real-time report template list, 851
accessing room topology maps, 191
accessing scheduled backup plans, 474
accessing scheduled report histories, 863
accessing server details page, 360
accessing task management, 69
accessing the automatic deployment plan page, 452
accessing the backup history report, 478
accessing the configuration backup report, 482
accessing the Configuration Center, 404
accessing the configuration check display command list, 521
accessing the device details page from device details, 211
accessing the device view, 176
accessing the graphical device panel for the selected device, 220
accessing the interface details page, 267
accessing the interface list page, 267
accessing the IP view, 178
accessing the IP/MAC learning query service, 221
accessing the list of performance views, 621
accessing the monitor list, 613
accessing the network topology, 180
accessing the quick custom report template list, 865
accessing the TopN view, 586
accessing transfer mode options, 140
accessing VLAN devices for specific device, 831
accessing wiring cabinet maps, 192
adding, 636
adding a basic rule in a basic rule set, 743
adding a basic rule set to an ACL resource, 705
adding a check task, 509
adding a configuration check display command, 522
adding a core device, 605
adding a device group, 127
adding a device manually, 153
adding a device model, 96
adding a device series, 94
adding a device vendor, 92
adding a favorite, 65
adding a filter, 101
adding a link rule set to an existing ACL resource, 711
adding a link rule to a link ACL template, 685
adding a link rule to a link rule set, 746
adding a login control template, 111
adding a mirror group for a device, 235
adding a monitor from the device list, 306
adding a monitor graph, 639
adding a monitor to the network topology, 633
adding a network address group, 650
adding a port, 208
adding a port group to a server, 364
adding a PowerShell template, 87
adding a quick custom report, 869
adding a real-time report, 854
adding a report data source, 858
adding a rule to an advanced ACL template, 682
adding a scheduled report, 860
adding a security control policy, 815
adding a service using ACL Assistant, 647
adding a SOAP template, 83
adding a space tab on the home page, 31
adding a SSH template, 80
adding a Telnet template, 77
adding a time range, 653
adding a trunk port, 838
adding a user group, 131
adding a user subgroup, 132
adding a user-defined monitor to the global index settings, 608
adding a user-defined rule set to an existing ACL resource, 714
adding a user-defined rule to a user-defined ACL template, 687
adding a user-defined rule to a user-defined rule set, 748
adding a virtual interface to a specific switch, 834
adding a virtual machine, 365
adding a vSwitch to a server, 363
adding a WMI template, 89
adding an access device, 604
adding an ACL, 697
adding an ACL to the selected device, 759
adding an ACL use for packet filtering, 766
adding an ACL use for VLAN packet filtering, 766
adding an administrator group operator, 115
adding an advanced rule set to an existing ACL resource, 707
adding an advanced rule to an advanced rule set, 744
adding an alarm forwarding rule, 598
adding an asset OID, 350
adding an automatic backup plan, 475
adding an automatic deployment device, 455
adding an automatic deployment task, 453
adding an email alarm notification rule, 586
adding an IMC maintainer group operator, 118
adding an IMC viewer group operator, 118
adding an operator group, 104
adding an SMS messaging alarm notification rule, 593
adding an SNMPv1 or v2c template, 74
adding an SNMPv3 template, 75
adding blocking to an operator account, 124
adding clouds to the data center topology map, 190
adding company logo to real-time reports, 859
adding company name to real-time reports, 859
adding compiled MIB to IMC, 137
adding data centers to the data center topology map, 190
adding device category, 99
adding devices by advanced query, 84
adding devices by view, 84
adding devices to a device group, 128
adding devices to a global VLAN, 828
adding devices to custom views, 204
adding devices to groups in ungrouped devices, 130
adding devices to IMC via ARP-based auto-discovery, 160
adding devices to IMC via basic auto-discovery, 157
adding devices to IMC via importing device information, 172
adding devices to IMC via IPsec VPN-based auto-discovery, 160
adding devices to IMC via PPP-based auto-discovery, 160
adding devices to IMC via routing-based auto-discovery, 160
adding devices to the current custom view, 300, 309
adding flow template applications, 780
adding flow template definitions, 777
adding hybrid ports, 840
adding login types for network devices in batch mode, 280
adding monitor instances, 616
adding monitors to devices from the device list, 315
adding new widgets to a space on the home page, 31
adding OSM software to the software library, 436
adding performance view shortcut to the left navigation tree, 627
adding ping settings for network devices in batch mode, 281
adding poll interval setting for one or more device in batch mode, 279
adding port aggregation entries, 243
adding ports to existing VLANs, 273
adding quick custom report templates, 867
adding real-time monitors, 230
adding real-time report template, 853
adding RMON alarm group entries, 252
adding RMON event group entries, 255
adding RMON extension alarm group entries, 259
adding RMON history group entries, 250
adding RMON statistic group entries, 249
adding rooms to the building topology map, 191
adding rooms to the data center topology map, 190
adding rules to a basic ACL template, 681
adding SNMP setting for one or more device in batch mode, 275
adding SSH setting for one or more device in batch mode, 278
adding switch access binding using auto scan, 338
adding Telnet setting for one or more device in batch mode, 277
adding terminal access binding using auto scan, 335
adding trap definitions, 544
adding user-defined trap filter rule, 533
allocating IP addresses manually, 319
allocating IP addresses using auto scan, 320
allocating IP addresses using import IP addresses, 321
auditing a network asset, 354
automatically building data center topology maps, 193
backing up configurations from the Configuration Center, 418
backing up device configuration files, 230
backing up device configurations for devices from the device list, 316
backing up device configurations from the device list, 307
baselining a configuration history entry, 776
basic operations, customizing RSS widgets, 45
basic operations, customizing spaces and system-defined widgets, 43
basic operations, disabling sound files for alarm levels, 47
basic operations, enabling system-defined sound files for alarm levels, 46
basic operations, freezing a space tab, 30
binding multiple IP/MAC addresses using auto scan, 341
binding to a MAC address port, 239
browsing all alarms, 579
browsing all attack alarms list, 801
browsing real-time alarms, 571
browsing real-time attack alarm list, 807
browsing root alarms, 574
browsing Syslog entries, 553
browsing Syslog template, 557
browsing traps, 526
canceling a monitor from the device list, 306
canceling actions, 326
canceling all monitor instances, 229
canceling monitor to devices from the device list, 315
canceling the transfer mode option for one or more devices, 141
changing the management status of a selected interface to DOWN, 270
changing the management status of a selected interface to UP, 270
changing the UP/DOWN alarm filter status, 271
changing the user-defined speed setting for the selected interface, 271
changing the widget layout of a space, on the home page, 32
checking SSH settings for devices from the device list, 313
checking SSH settings on managed devices, 304
checking Telnet settings for devices from the device list, 312
checking Telnet settings on managed devices, 304
checking the (Cisco)No delay rule, 504
checking the (HPA)Duplex status rule, 505
checking the (HPA)Remote login rule, 506
checking the (HPA)Speed status rule, 506
clearing MSTP statistics entries, 266
collapsing a widget of a space on the home page, 32
collapsing all widgets of a space on the home page, 32
collapsing all widgets of a space on the home page, 32
comparing configuration files, 411
comparing device configurations, 417, 440
comparing files in the configuration baseline report, 485
compiling a MIB in IMC, 138
configuring a mirror group for a device, 235
configuring access ports for existing VLAN using batch deployment, 845
configuring an existing SNMP template, 155
configuring an existing SSH template, 156
configuring an existing Telnet template, 155
configuring an unauthorized access processing policy, 343
configuring auto migration, 366
configuring conflict processing policy, 343
configuring cyclic time ranges, 655
configuring default monitor indices, 150
configuring DNS server setting, 146
configuring existing SNMP templates, 276
configuring external tool settings, 146
configuring fixed time ranges, 654
configuring functions via quick start, 67
configuring global MSTP settings, 262
configuring hybrid ports for existing VLAN using batch deployment, 846
configuring IGMP snooping options for devices, 266
configuring IMC for email notification, 134
configuring IMC for hierarchical alarm configuration, 136
configuring IMC for SMSC messaging, 135
configuring IMC to use LDAP authentication services, 108
configuring IMC to use RADIUS authentication services, 107
configuring Internet connection, 145
configuring MAC address binding for selected device, 238
configuring MG monitors, 236
configuring MG reflectors, 236
configuring monitor settings, 638
configuring monitored services, 214
configuring network asset audit settings, 151
configuring NNMi, 144
configuring password strategies, 112
configuring ping configuration, 144
configuring PoE switches, 244
configuring RADIUS server for access devices, 245
configuring subnet mask type, 656
configuring switch access binding for terminals, 326
configuring terminal access binding for devices, 325
configuring the first file, 412
configuring the global MAC address learning configuration, 240
configuring the IP address for the selected interface, 273
configuring the left file, 412
configuring the right file, 413
configuring the second file, 413
configuring third-party devices, 68
configuring transfer mode options, 140
configuring trunk ports for existing VLAN using batch deployment, 846
configuring undefined access processing policy, 343
configuring VC, 246
copying a configuration template, 430
copying a rule in an ACL template, 695
copying a rule set, 727
copying an alarm forwarding rule, 603
copying an email alarm notification rule, 592
copying an existing ACL template, 679
copying an existing rule to a new rule, 749
copying an initial configuration file, 472
copying an operator group, 105
copying an SMS alarm notification rule, 597
copying link template contents into a link ACL, 736
copying Syslog to alarm rule, 566
copying system Syslog template, 560
copying trap to alarm rule, 540
copying user-defined Syslog template, 560
creating a basic ACL template, 660
creating a compliance policy, 493
creating a configuration template for configuration files, 414
creating a configuration template manually, 426
creating a configuration template using a backup file, 423
creating a configuration template using file import, 424
creating a drive folder, 375
creating a drive index file, 375
creating a global VLAN, 827
creating a global VLAN query, 827
creating a link ACL template, 666
creating a performance view, 624
creating a performance view folder, 623
creating a performance view from monitor settings page, 625
creating a template folder, 421
creating a user-defined ACL template, 668
creating a vendor folder, 374
creating a VLAN, 832
creating alarm relation report, 569
creating an advanced ACL template, 662
creating an alarm relation report, 572, 577
creating custom views, 202
creating drive definition file, 376
creating templates in ACL Management, 657
creating user-defined alarm statistics charts, 585
creating user-defined Syslog template, 558
creating user-defined Syslog to alarm rule, 562
creating user-defined trap to alarm rule, 538
creating VLAN using batch deployment, 844
customizing ACL configuration polling, 755
customizing columns for the interface list, 208
customizing the all alarms list columns, 582
defining background custom script, 386
defining specific services, 380
defining the parser service, 382
deleting a check task, 510
deleting a compliance policy, 502
deleting a configuration history entry, 775
deleting a configuration template, 433
deleting a configuration template folder, 422
deleting a core device, 605
deleting a deployment task, 451
deleting a device category, 99
deleting a device from an automatic deployment plan, 468
deleting a device group, 128
deleting a device model, 98
deleting a device series, 95
deleting a device vendor, 93
deleting a favorite, 66
deleting a filter, 101
deleting a global VLAN, 828
deleting a login control template, 112
deleting a MAC port binding, 240
deleting a mirror group, 238
deleting a monitor, 637
deleting a monitor from the network topology, 634
deleting a monitor graph, 641
deleting a network address group, 652
deleting a performance view, 629
deleting a performance view folder, 624
deleting a port, 209
deleting a PowerShell template, 88
deleting a quick custom report, 870
deleting a report data source, 858
deleting a rule from an ACL template, 695
deleting a rule set from an ACL, 742
deleting a security control policy, 820
deleting a service using ACL Assistant, 648
deleting a SNMP template, 76
deleting a SOAP template, 86
deleting a software library entry, 439
deleting a space on the home page, 31
deleting a SSH template, 82
deleting a Telnet template, 79
deleting a time range, 656
deleting a user group, 133
deleting a user subgroup, 134
deleting a user-defined monitor from the global index settings, 612
deleting a virtual interface from a specific switch, 835
deleting a VLAN, 833
deleting a VLAN from devices, 829
deleting a widget from the space on the home page, 33
deleting a WMI template, 91
deleting ACLs from the selected device, 759
deleting alarms from the real-time alarms page, 573
deleting alarms from the root alarms list, 578
deleting alarms on the all alarms page, 583
deleting an access device, 605
deleting an ACL, 698
deleting an ACL packet filtering use, 769
deleting an ACL template, 680
deleting an ACL VLAN packet filtering use, 769
deleting an alarm forwarding rule, 603
deleting an asset OID, 351
deleting an automatic deployment task, 454
deleting an email alarm notification rule, 592
deleting an existing automatic backup plan, 476
deleting an IMC operator, 123
deleting an initial configuration file, 473
deleting an operator group, 107
deleting an SMS alarm notification rule, 598
deleting attack alarms from the list, 806
deleting attack alarms from the real-time attack alarm list, 808
deleting check task history, 514
deleting configuration display commands, 523
deleting custom views, 204
deleting device ACL time ranges, 771
deleting devices from the current view, 301, 310
deleting flow template applications, 781
deleting flow template definitions, 779
deleting history access logs, 330
deleting hybrid ports, 841
deleting IMC views with current data, 217
deleting invalid stack members from stack topology, 198
deleting monitor instances, 620
deleting performance data for monitor instances, 230
deleting port aggregation information, 244
deleting quick custom report templates, 868
deleting RMON alarm group entries, 253
deleting RMON event group entries, 256
deleting RMON extension alarm group entries, 260
deleting RMON history group entries, 251
deleting RMON statistic group entries, 249
deleting rules from a set, 750
deleting scheduled report histories, 864
deleting scheduled reports, 865
deleting time ranges on devices, 791
deleting unauthorized access entries, 326
deleting user-defined Syslog template, 560
deleting user-defined Syslog to alarm rule, 567
deleting user-defined trap filter rule, 537
deleting VLAN deployment task entries, 843
denying access to operators currently online, 124
deploying a file, 443
deploying ACLs to devices, 786
deploying an ACL use using deploy ACL uses feature, 793
deploying device configuration to a selected device, 442
deploying OSM software, 444
deploying packet filtering with Add Use, 761
deploying software from the device list, 307
deploying software to devices from the device list, 315
deploying system software, 442
deploying VLAN packet filtering with Add Use, 761
disabling 802.1X on interfaces, 245
disabling a single compliance policy, 502
disabling all compliance policies, 503
disabling an alarm forwarding rule, 603
disabling an email alarm notification rule, 592
disabling an existing automatic backup plan, 477
disabling an SMS alarm notification rule, 598
disabling DismanPing configuration, 146
disabling Syslog filtering rules, 557
disabling Syslog to alarm rule, 567
disabling trap to alarm rule, 542
displaying a monitor graph, 641
displaying a widget in a new window on the home page, 33
displaying mirror group information, 234
displaying monitored devices only, 620
drag & drop a widget on the home page, 33
editing SNMP auto discovery parameters manually, 162
editing SNMP settings manually, 154, 168, 276, 463
editing SNMP template settings manually, 458
editing SSH auto discovery parameters manually, 164
editing SSH settings manually, 156, 169, 279
editing SSH template settings manually, 459
editing Telnet auto discovery parameters manually, 163
editing Telnet parameters manually, 155
editing Telnet settings manually, 169, 277
editing Telnet template settings manually, 458
enabling 802.1X on interfaces, 245
enabling a single compliance policy, 502
enabling an alarm forwarding rule, 603
enabling an email alarm notification rule, 592
enabling an existing automatic backup plan, 477
enabling an SMS alarm notification rule, 598
enabling DismanPing configuration, 146
enabling or disabling the (HPA)Syslog rule, 503
enabling Syslog filtering rules, 557
enabling Syslog to alarm rule, 567
enabling trap to alarm rule, 542
establishing a configuration file baseline, 413
establishing a software baseline, 416
establishing baselines using a software library entry, 439
executing a manual action for an attack alarm, 812
executing a Ping test from the IMC server to the selected device, 218
executing actions from the alarm details page, 568
executing actions on the alarm details page, 572
expanding a widget of a space on the home page, 32
expanding all widgets of a space on the home page, 32
exporting a configuration file from the configuration backup report page, 483
exporting a configuration template, 432
exporting a quick custom report, 870
exporting a software library entry, 439
exporting alarms from the all alarms page, 583
exporting an ACL to a text file, 761
exporting device information, 174
exporting IMC event logs, 146
exporting quick custom reports, 866
exporting real-time report, 853, 856
exporting the auto-discovery report, 160
exporting the report, 165, 171
filtering the scheduled report list, 860
fixing violating devices, 510
folding a monitor graph, 642
forcing switch port operation in MSTP mode, 265
importing advanced template contents into an advanced ACL, 731
importing basic template contents into basic ACL, 728
importing device information to IMC via NNMi, 175
importing devices into an automatic deployment plan, 465
importing network segment addresses, 166
importing software into the software library from a device, 436
importing software into the software library from a file, 435
importing trap definitions from a MIB file, 552
importing user-defined template contents into a user-defined ACL, 740
installing SMS plug-in, 823
launching a Telnet session to the selected device, 217
launching an SSH session to the selected device, 221
launching MIB management for the selected device, 219
limiting the export of log files, 147
locating an IP address using real-time location query, 331
locating MAC address using real-time location query, 331
logging into IMC, 29
logging off operators currently online, 124
logout of IMC, 71
maintaining a maintainer group operator, 120
maintaining a viewer group operator, 120
managing custom topology via the right mouse click, 186
managing devices from the current view, 301, 310
managing devices from the data center topology maps, 195
managing IMC views with current data, 216
managing stack devices with stack topology, 196
managing the data analysis project list, 149
manually adding a device to the network asset manager, 352
manually adding an IP segment, 318
manually binding a terminal to interfaces, 334
manually binding an IP address to a MAC address, 340
manually binding interfaces to one or more terminals, 337
manually migrating a virtual machine, 365
manually unbinding a terminal from interfaces, 334
manually unbinding an IP address from a MAC address, 341
manually unbinding one or more terminals from an interface, 338
maximizing a widget on the home page, 33
modifying a backup configuration file, 410
modifying a basic ACL template, 670
modifying a basic rule in a basic rule set, 743
modifying a compliance policy, 497
modifying a configuration history entry, 775
modifying a configuration template, 428
modifying a configuration template folder, 421
modifying a deployment task, 448
modifying a device category, 99
modifying a device group, 127
modifying a device label, 222
modifying a device model, 97
modifying a device series, 95
modifying a device vendor, 93
modifying a favorite, 66
modifying a global monitor to the global index settings, 611
modifying a link ACL template, 675
modifying a link rule in a link rule set, 746
modifying a login control template, 111
modifying a MAC address port binding configuration, 239
modifying a monitor, 636
modifying a monitor graph, 640
modifying a monitor on the network topology, 633
modifying a network address group, 651
modifying a network asset, 352
modifying a performance view, 628
modifying a performance view folder, 623
modifying a port, 208
modifying a port MAC address learning management, 240
modifying a PowerShell template, 88
modifying a quick custom report, 870
modifying a real-time report, 856
modifying a report data source, 858
modifying a scheduled report, 862
modifying a security control policy, 818
modifying a service using ACL Assistant, 648
modifying a SNMP template, 76
modifying a SOAP template, 85
modifying a software library entry, 438
modifying an SSH template, 81
modifying a Telnet template, 78
modifying a time range, 655
modifying a user group, 132
modifying a user subgroup, 133
modifying a user-defined rule in a user-defined rule set, 748
modifying a VLAN, 833
modifying a VM profile, 366
modifying a WMI template, 90
modifying an ACL deployment task, 783
modifying advanced properties of a port group, 371
modifying advanced properties of a vSwitch, 371
modifying advanced rule set of an existing ACL resource, 719
modifying all compliance policies, 502
modifying an administrator group operator, 116
modifying an advanced ACL template, 672
modifying an advanced rule in an advanced rule set, 744
modifying an alarm forwarding rule, 601
modifying an asset OID, 351
modifying an automatic deployment device, 459
modifying an automatic deployment task, 453
modifying an email alarm notification rule, 589
modifying an existing automatic backup plan, 476
modifying an existing IP segment, 319
modifying an existing RADIUS configuration, 108
modifying an existing trunk port, 838
modifying an initial configuration file, 472
modifying an operator group, 106
modifying an SMS alarm notification rule, 595
modifying basic rule set of an existing ACL resource, 717
modifying communication parameters for web manager, 228
modifying configuration & status poll settings on managed devices, 305
modifying configuration display commands, 522
modifying configure device information, 462
modifying custom views, 203
modifying duplicate trap filter rules, 529
modifying flow template definitions, 778
modifying hybrid ports, 840
modifying IMC passwords, 123
modifying incompliant settings, 495
modifying intermittent trap filters, 531
modifying LDAP authentication service configuration, 109
modifying link rule set of an existing ACL resource, 722
modifying monitor instances, 618
modifying MSTI settings, 263
modifying network asset property, 352
modifying new rule, 749
modifying ping parameters, 227
modifying ping settings for network devices in batch mode, 281
modifying PoE switch port power consumption, 244
modifying poll interval setting for one or more device in batch mode, 279
modifying poll settings for devices from the device list, 314
modifying polling interval settings, 227
modifying port aggregation information, 243
modifying port configuration for MSTP settings, 264
modifying port PVIDs, 836
modifying quick custom report templates, 868
modifying real-time report template, 853
modifying rules in a basic ACL template, 688
modifying rules in an advanced ACL template, 689
modifying SNMP setting for one or more device in batch mode, 275
modifying SNMP settings, 224
modifying SOAP settings, 226
modifying software to deploy information, 460
modifying SSH setting for one or more device in batch mode, 278
modifying SSH settings, 225
modifying system group attributes, 223
modifying system settings, 143
modifying Telnet setting for one or more device in batch mode, 277
modifying Telnet settings, 225
modifying the environment information for a card, 233
modifying the interface UP/DOWN alarm filter in batch mode, 281
modifying the link rule of a link rule ACL template, 692
modifying the login type for network devices in batch mode, 280
modifying trap definition severity settings, 551
modifying trap to alarm rule, 540
modifying trap to alarm strategy, 539
modifying unknown trap filters, 532
modifying unmanaged devices trap filter, 533
modifying user-defined rule set of an existing ACL resource, 725
modifying user-defined rules in a user-defined ACL template, 694
modifying user-defined Syslog template, 559
modifying user-defined Syslog to alarm rule, 564
modifying user-defined template, 678
modifying user-defined trap definitions, 548
modifying user-defined trap filter rule, 536
monitoring the performance indexes in real time, 275
navigating to the configuration backup history, 409
navigating to the deployment task list, 445
navigating to the device list from a custom view, 300, 309
navigating to the device list from the device view, 299, 307
navigating to the device list from the IP view, 300, 308
network segment based advanced auto discovery, 166
opening a web manager session to the selected device, 217
optimizing rules in a rule set, 751
performing a basic device search, 62, 210
performing a basic network asset query, 347
performing a basic query on the asset audit list, 356
performing a basic user search, 63
performing a manual backup, 478
performing a server query, 362
performing a Traceroute from the IMC server to the selected device, 218
performing an advanced device search, 63, 210
performing an advanced interface search, 64
performing an advanced network asset query, 348
performing an advanced query on the asset audit list, 356
performing an advanced user search, 64
performing attack alarm advanced query, 805
performing attack alarm basic query, 804
print report to PDF, 165
printing a real-time report, 856
printing real-time report to PD, 852
printing real-time report to PDF, 856
printing the auto-discovery report to PDF, 159
printing the report to PDF, 171
querying a compliance policy, 493
querying a trap, 544
querying a vendor name, 374
querying a VLAN device, 830
querying ACL devices list, 755
querying alarms using advanced query, 570
querying alarms using basic query, 570
querying asset OID, 350
querying check task history, 513
querying for devices in the Configuration Center, 405
querying history access logs, 329
querying migration recommendations, 368
querying migration reports, 370
querying operation logs, 149
querying port group lists, 205
querying Syslog entries using advanced query, 555
querying Syslog entries using basic query, 554
querying the backup history report, 479
querying the configuration backup report, 482
querying the configuration baseline report, 484
querying the configuration template list, 420
querying the list of performance views, 622
querying the software baseline report, 488
querying the software update report, 486
querying the unauthorized access list, 323
querying traps by advanced query, 528
querying traps by basic query, 527
querying unauthorized access logs, 324
rebooting devices from the device list, 314
rebooting using batch operations feature, 306
recovering alarms from the all alarms page, 582
recovering alarms from the real-time alarms page, 573
recovering alarms from the root alarms view, 578
re-executing a failed backup, 481
re-executing a partially successful backup, 481
refreshing a network asset detail, 354
refreshing a widget manually on the home page, 33
refreshing data for monitor instances, 229
refreshing devices from the current view, 303, 311
refreshing history access logs, 330
refreshing IMC views with current data, 216
refreshing IP/MAC binding lists, 342
refreshing real-time attack alarm list, 808
refreshing switch access binding list, 338
refreshing the attack alarm list, 806
refreshing the selected interface from the interface details page, 269
refreshing the server details page, 364
refreshing the terminal access binding list, 335
refreshing the unauthorized access list, 327
refreshing the unauthorized access log list, 327
refreshing the virtual network view, 363
removing a compiled MIB from IMC, 139
removing a device from a device group, 129
removing a network asset, 354
removing ACLs from devices, 796
removing ACLs from devices, 788
removing blocking from an operator account, 125
removing devices from custom views, 204
removing devices from the current custom view, 310
removing devices from the current view, 301
removing files from network device memory, 415
removing interfaces with unchanged 802.1X statuses, 245
removing multiple devices from a device group, 129
removing performance view from the left navigation tree, 627
removing the single device transfer mode option from one or more devices, 141
renaming a configuration template, 430
renaming a software library entry, 437
renaming a space tab on the home page, 31
renaming an ACL, 698
reordering rules in an ACL rule set, 751
re-running failed deployment tasks, 449
re-running suspended deployment tasks, 449
resetting a device, 232
resetting My Report, 850
resetting routers, 232
resetting switches, 232
resetting the environment information for a card, 233
resetting wireless devices, 232
restarting a paused ACL deployment task, 785
restoring a device configuration, 444
restoring an existing IP segment, 319
restoring default settings for port path cost, 266
restoring IP address allocations, 321
resuming a deployment task, 450
resuming scheduled reports, 864
retrieving data on the history access log, 329
retrieving history access log list immediately, 329
running a report using the quick custom report template, 866
running an ad hoc report using real-time report template, 852
saving a device ACL as a template, 765
saving a device ACL as an ACL rule set, 763
saving a space on the home page, 31
saving configurations on managed devices, 305
saving device configuration, 232
saving device configurations in batch mode, 283
saving monitors to an existing performance view, 626
saving router configuration, 232
saving switch configuration, 232
saving the configuration of devices from the device list, 314
saving wireless device configuration, 232
searching a deployment task list, 446
searching for a software library entry, 435
searching for IP/MAC bindings, 340
searching for monitors in the device list, 614
searching for monitors in the instance list, 615
searching for switch access bindings, 337
searching for terminal access bindings, 333
searching global index settings, 607
searching VLAN deployment tasks, 842
selecting device label configuration, 145
selecting export settings, 147
selecting interface Down alarm, 145
selecting interface Up alarm, 145
setting basic system settings, 143
setting device registration configuration, 145
setting display options, 642
setting message options, 70
setting monitor options, 642
setting the alarm generation mode, 141
setting the max backup configuration files, 142
setting the MG VLAN ID, 237
setting the refresh interval on the home page, 33
setting the transfer mode option for one or more devices, 141
setting web manager configuration, 144
sorting favorites, 66
sorting rules in an ACL rule set, 751
specifying default primary configuration file for a device, 231
specifying default secondary configuration file for a device, 231
specifying default startup software for a device, 231
stopping a deployment task, 785
suspending a deployment task, 450
suspending scheduled reports, 864
switching between spaces on the home page, 31
switching monitor list, 614
switching the active MPUs for a device, 233
switching the standby MPUs for a device, 233
switching to the port mode, 241
synchronizing ACL devices list, 755
synchronizing devices from the current view, 302, 311
synchronizing IMC views with current data, 216
synchronizing the selected interface from the interface details page, 269
taking actions from the root alarms page, 575
taking actions in the alarm details page, 581
taking actions on the alarm details page, 577
taking actions on the all alarms page, 580
testing the loopback interface for the selected device, 272
triggering automatic deployment on devices, 469
unbinding multiple IP/MAC addresses, 342
unfolding a monitor graph, 642
unfreezing a space tab on the home page, 30
unmanaging an interface, 270
unmanaging devices from the current view, 302, 311
unmanaging IMC views with current data, 216
using a SSH template to configure SSH settings for a device, 164
using a Telnet template to configure Telnet settings for a device, 163
using an SNMP template to configure SNMP settings for a device, 163
using batch mode to configure devices, 292
using batch mode to configure interfaces, 295
using batch mode to configure LACP, 291
using batch mode to configure management status on interfaces, 285
using batch mode to configure PoE settings, 286
using batch mode to configure spanning tree protocol on interfaces, 290
using batch mode to configure spanning tree protocol on switches, 288
using batch mode to configure trap destinations, 287
using batch mode to reboot devices, 284
using existing SNMP templates, 168, 224, 458, 463
using existing SOAP templates, 227
using existing SSH templates, 170, 226, 279, 459, 464
using existing Telnet template, 169
using existing Telnet templates, 225, 278, 459, 464
using Telnet/SSH proxy to access a device, 219
using Telnet/SSH proxy to manage a device, 219
verifying SSH settings for network devices using batch mode, 282
verifying Telnet settings for network devices using batch mode, 282
viewing a device list for a particular device group, 126
viewing a network address group in ACL Assistant, 650
viewing a performance view report, 629
viewing a quick custom report, 869
viewing a real-time report, 855
viewing a rule set for an ACL resource, 699
viewing a rule set list for an ACL resource, 699
viewing a single attack using the attack path map, 810
viewing access ports, 835
viewing ACL Assistant services, 646
viewing ACL configuration history, 773
viewing ACL configuration history entry, 774
viewing ACL device configuration page, 757
viewing ACL device list, 754
viewing ACL resource list, 696
viewing alarm details, 568
viewing alarm details from the all alarms page, 581
viewing alarm details from the root alarms page, 577
viewing alarm statistics charts, 584
viewing all attacks using the attack topology map, 809
viewing all scheduled reports, 859
viewing an ACL template, 659
viewing an alarm relation report, 581
viewing applied ACLs, 762
viewing asset OID list, 349
viewing attack alarm details, 803
viewing audit history for network asset details, 346
viewing automatic deployment device information, 454
viewing automatic deployment execution results, 469
viewing backup history, 477
viewing backup history detailed information, 480
viewing BGP information for a selected router, 261
viewing compliance policy check results, 517
viewing compliance policy list, 489
viewing configuration check report, 519
viewing configuration management summary, 408
viewing configuration retrieval report, 520
viewing current access information for a terminal, 329
viewing current data for performance monitor instances, 229
viewing current report data sources, 857
viewing deployment task detailed information, 783
viewing deployment task list, 781
viewing deployment tasks, 841
viewing detailed information about a compliance policy, 490
viewing detailed information about a rule, 491
viewing detailed information of an initial configuration file, 474
viewing details of a software library entry, 434
viewing details of ACL Assistant services, 646
viewing details of an individual time range, 653
viewing device ACL time range list, 771
viewing device groups, 125
viewing device Syslog detailed information, 556
viewing device violating results, 518
viewing existing IP address allocations, 317
viewing flow template applications, 779
viewing flow template details, 777
viewing flow templates, 776
viewing hardware information for the selected device, 240
viewing historical data for performance monitor instances, 229
viewing historical data for the performance monitors, 215
viewing hybrid ports, 839
viewing imported software, 433
viewing information for a rule set for an ACL, 700
viewing information for the selected interface, 274
viewing invalid event list details, 256
viewing invalid RMON alarm details, 253
viewing IPv6 information for the selected router, 241
viewing IPv6 information for the selected switch, 241
viewing IPv6 information for the selected wireless device, 241
viewing MAC address binding for selected device, 238
viewing migration reports of the virtual machine, 369
viewing monitored services, 213
viewing net address group in ACL Assistant, 649
viewing network asset list, 344
viewing operation logs, 148
viewing operators currently online, 123
viewing OSPF information for a selected router, 261
viewing physical servers managed by a specific vManager, 200
viewing PoE switch information, 244
viewing port aggregation information, 242
viewing real-time alarm details, 572
viewing RIP information for a selected router, 261
viewing RMON alarm group details, 251
viewing RMON event group details, 255
viewing RMON extension alarm group details, 257
viewing RMON history group details, 249
viewing RMON log details, 260
viewing RMON statistics group details, 248
viewing rule information for a rule for an ACL resource, 701
viewing SMS and managed devices in the topology, 824
viewing SSC reports, 821
viewing Syslog filtering rules, 556
viewing Syslog to alarm rules, 561
viewing system information for selected device, 234
viewing task execution results, 515
viewing the ACL definition list, 758
viewing the ACL use list, 766
viewing the asset audit list, 355
viewing the check task details, 508
viewing the check task history, 512
viewing the check task list, 507
viewing the device category list, 98
viewing the device model list, 96
viewing the device series list, 93
viewing the device vendor list, 91
viewing the environment information for a card, 233
viewing the execution result page, 447
viewing the execution result report, 814
viewing the filter list, 100
viewing the global VLAN list, 826
viewing the history access log list, 328
viewing the interfaces list of a port group, 206
viewing the IP/MAC binding list, 339
viewing the latest running configuration, 407
viewing the latest startup configuration, 406
viewing the list of ACL templates, 658
viewing the login control template list, 110
viewing the operator group list, 103
viewing the operator list, 114
viewing the PowerShell template list, 86
viewing the real-time monitor window, 635
viewing the resource list for a server, 359
viewing the security control policy list, 815
viewing the SNMP template list, 73
viewing the SOAP template list, 82
viewing the software baseline report, 487
viewing the software update history, 414
viewing the software update report, 486
viewing the SSH template list, 79
viewing the switch access binding list, 336
viewing the Telnet template list, 77
viewing the terminal access binding list, 332
viewing the time range list in the ACL Assistant, 652
viewing the topology of a device, 219
viewing the unauthorized access log list, 323
viewing the ungrouped devices list, 129
viewing the user group list, 131
viewing the View ACL page, 762
viewing the virtual network, 358, 364
viewing the virtual network topology, 362
viewing the virtual network with VNM topology maps, 199
viewing the VLAN device list, 829
viewing the WMI template list, 89
viewing time range information for a rule for an ACL resource, 704
viewing traffic with traffic topology, 198
viewing trap definitions, 543
viewing trap details, 527
viewing trap filter rules, 528
viewing trap to alarm rules, 537
viewing trunk ports, 837
viewing unauthorized access list, 322
viewing virtual interfaces for a specific switch, 833
viewing virtual machine recommendations, 367
viewing VLAN topo maps, 843
viewing VLANs for specific device, 831

protocol management
BGP browsing for routers, 261
clearing MSTP statistics entries, 266
forcing port migration to MSTP mode, 265
IGMP snooping, 266
modifying MSTI settings, 263
modifying port MSTI settings, 264
MSTP options for routers and switches, 262
OSPF browsing for routers, 261
restoring default settings for path cost, 266
RIP browsing for routers, 261
QoS. See Quality of Service Manager
query Syslog entries
advanced alarm query, 555
basic alarm query, 554
querying alarms in IMC
advanced alarm query, 570
basic alarm query, 570
querying network assets
advanced query, 348
basic query, 347
querying the asset audit list
advanced query, 356
basic query, 356
querying the attack alarm list
advanced query, 805
basic query, 804
querying the attack alarm list
advanced query, 805
basic query, 804
quick custom report templates
accessing the quick custom report template list, 865
adding a quick custom report template, 867
deleting a quick custom report template, 868
exporting a report, 866
modifying a quick custom report template, 868
running a report via the quick custom report template, 866
quick custom reports
managing quick custom reports, 868
quick custom report templates, 865
real time location
querying IP address location, 331
querying MAC address location, 331
real time report templates
accessing the real time report template list, 851
adding a real time report template, 853
modifying a real time report template, 853
running a real time report template, 852
real time reports
adding company name to reports, 859
adding logos to reports, 859
managing real time report data sources, 857
managing real time reports, 854
real time report options, 859
real time report templates, 851
reporting
customizing my real time report page, 850
my real time reports, 848
quick custom reports, 848, 865
real time reports, 851
real-time reports, 848
scheduling real time reports, 859
resource management
adding devices in IMC, 153
configuring vendor and device information, 91
device access templates, 73
device access templates, PowerShell templates, 86
device access templates, SNMP templates, 73
device access templates, SOAP templates, 82
device access templates, SSH templates, 82
device access templates, Telnet templates, 76
device access templates, WMI templates, 89
filter interfaces, managing filters to, 100
managing filters to filter interfaces, 100
managing multiple devices from the device list, 298
managing multiple devices using batch operations, 275
managing one device via device details, 211
network asset manager, 344
searching for devices, 209
terminal access, 316
vendor and device information, configuring, 91
view device interface with port groups, 205
viewing devices, 175
virtual network manager, 357, 358
RMON
adding RMON alarm group entries, 252
adding RMON event group entries, 255
adding RMON extension alarm group entries, 259
adding RMON history group entries, 250
adding RMON statistics group entries, 249
deleting RMON alarm group entries, 253
 deleting RMON event group entries, 253
 deleting RMON extension alarm group entries, 260
 deleting RMON history group entries, 251
 deleting RMON statistics group entries, 249
managing RMON alarm group, 251
managing RMON event group, 255
managing RMON extension alarm group, 257
managing RMON history group details, 249
managing RMON log, 260
viewing invalid RMON alarm details, 253
viewing RMON alarm group details, 251
viewing RMON event group details, 255
viewing RMON extension alarm group details, 257
viewing RMON history group details, 249
viewing RMON log details, 260
viewing RMON statistics group details, 248
rule examples
aggregate link, 506
configuration segment, 506
device, 503
interface, 504
links, 505
running a real time report template
exporting a real time report, 853
printing a real time report to PDF, 852
scheduling real time reports
adding scheduled reports, 860
assessing scheduled report histories, 863
deleting scheduled report histories, 864
deleting scheduled reports, 865
filtering the scheduled report list, 860
modifying scheduled reports, 862
resuming scheduled reports, 864
suspending scheduled reports, 864
viewing all scheduled reports, 859
searching for devices
advanced search, 210
basic search, 210
searching for monitors
searching in the device list, 614
searching in the instance list, 615
securing access via authentication
LDAP authentication, modifying, 109
LDAP authentication, using, 108
securing access via authentication services
modifying LDAP authentication, 109
modifying RADIUS authentication, 108
RADIUS authentication, modifying, 108
RADIUS authentication, using, 107
using LDAP authentication, 108
using RADIUS authentication, 107
security control center
  integrating SSC with SMS, 823
  managing security attack alarms, 800
  managing security control policies, 814
  viewing SSC reports, 821
server details page
  network card, 361
  port group, 361
  server, 360
  storage, 362
  virtual machine, 361
  vSwitch, 361
service module
  EAD, 12
  MPLS VPN manager, 14
  NTA, 14
  QoSM, 13
  Service Health Manager, 15
  UAM, 11
  UBA, 13
  VSM, 11
  WSM, 10
settings
  adding trap definitions
    rules for processing trap object IDs, 545
simplifying ACL rule creation
  configuring subnet mask types, 656
  managing net address groups, 649
  managing services, 646
  managing time ranges, 652
SMS. See Security Management System
  adding alarm notification rule, 593
  copying alarm notification rule, 597
  deleting alarm notification rule, 598
  disabling alarm notification rule, 598
  enabling alarm notification rule, 598
  managed devices in the topology, 824
  managing alarm notifications, 593
  modifying alarm notification rule, 595
  plug-in installation, 823
  viewing management page in SCC, 824
SMSC settings
  configuring SMSC messaging, 135
SNMP
  access batch operation feature for configuring settings, 312
  access device list management settings, 303
  access device settings, 303
  device access templates resource management, 73
  editing settings manually, 276, 458, 463
  editing template automatic deployment plan settings, 458
  manually edit auto discovery settings, 162
  manually edit device settings, 154
  manually edit templates for segment-based discovery, 168
  modify settings for selected device, 224
  modifying settings, 224
  use existing auto discovery templates, 163
  use existing device templates, 155
  using batch mode to configure, 275
  using existing automatic deployment plan template, 458
  using existing template settings, 224
  using existing template to apply existing settings, 224
  using existing templates, 276, 279, 458, 463
  using existing templates for segment-based discovery, 168
SNMP templates
  adding v1 or v2 template, 74
  adding v3 template, 75
  modifying an SNMP template, 76
  SNMP template, deleting, 76
  SNMP template, modifying, 76
  v1 or v2 template, adding, 74
  v3 template, adding, 75
  viewing the SNMP template list, 73
SOAP
  device access templates resource management, 82
  modify settings for selected device, 226
  modifying settings for selected device, 226
  using existing templates, 227
  using existing templates to configure settings for device, 227
SOAP templates
  adding a SOAP template, 83
  adding devices by advanced query, 84
  adding devices by view, 84
  by advanced query, adding devices, 84
  by view, adding devices, 84
  deleting a SOAP template, 86
  modifying a SOAP template, 86
  SOAP template list, viewing, 82
  SOAP template, adding, 83
  SOAP template, deleting, 86
  SOAP template, modifying, 85
  viewing the SOAP template list, 82
software baseline report
  querying the software baseline report, 488
restoring a software file from the software baseline report page, 488
viewing the software baseline report, 487
software update report
querying the software update report, 486
restoring a software file from the software update report page, 487
viewing the software update report, 486
SSH, 226
accedd device settings, 304
access batch operation feature for configuring settings, 313
access device list management settings, 304
check device list management settings, 304
check settings on managed devices, 304, 313
device access templates resource management, 79
editing automatic deployment plan template settings, 459
editing settings manually, 279, 459, 464
launch session to selected device, 221
manually edit auto discovery settings, 164
manually edit device settings, 156
manually editing templates for segment-based discovery, 169
modify settings for selected device, 225
use existing device templates, 156
using batch mode to check, 282
using batch mode to configure, 278
using existing auto discovery templates, 164
using existing automatic deployment plan template, 459
using existing templates, 226, 279, 459, 464
using existing templates for segment-based discovery, 170
SSH templates
adding a SSH template list, 80
deleting a SSH template, 82
modifying a SSH template list, 81
SSH template list, viewing, 79
SSH template, adding, 80
SSH template, deleting, 82
SSH template, modifying, 81
viewing the SSH template list, 79
support and resources
contacting HP, 871
subscription service, 871
Syslog
advanced alarm query, 555
alarm recovery, 564
basic alarm query, 554
browsing entries, 553
browsing Syslog template, 557
copying Syslog template, 560
copying template, 560
copying to system alarm rule, 566
copying to user-defined alarm rule, 566
creating user-defined alarm rule, 562
creating user-defined Syslog template, 558
creating user-defined template, 558
deleting template, 560
deleting user-defined Syslog template, 560
deleting user-defined to alarm rule, 567
disabling filtering rules, 557
disabling to alarm rules, 567
enabling filtering rules, 557
enabling to alarm rules, 567
modifying user-defined alarm rule, 564
modifying user-defined Syslog template, 559
modifying user-defined template, 559
modifying user-defined templates, 559
using templates, 557
using to alarm rules, 561
viewing detailed information, 556
viewing filtering rules, 556
Syslog details
viewing device Syslog detailed information, 556
Syslog management
configuring alarms for Syslog messages, 557
filtering Syslog entries, 556
querying Syslog entries, 554
Syslog description, 553
Syslog details, 555
using Syslog to alarm rules, 561
view Syslog entries, 553
system settings
basic system settings, 143
device label configuration, 145
device registration configuration, 145
DismanPing configuration, 146
DNS server setting, 146
external tool settings, 146
interface up/down alarm, 145
internet connection configuration, 145
modifying system settings, 143
NNMi configuration, 144
ping configuration, 144
web manager configuration, 144
system settings and maintenance functions
configuring default monitor indices, 150
configuring network asset audit options, 151
data analysis management, 149
data export, 146
log files, 148
My Favorites, 150
system settings, 143
system-wide help
searching, 61
task execution and configuration retrieval report
view compliance policy check results, 517
view configuration check report, 519
view configuration retrieval report, 520
view device violating results, 518
view task execution results, 515
task management
accessing task management, 69
message history, 70
message options, 70
Telnet
access batch operation feature for configuring settings, 312
access device settings, 303
check device list management settings, 304
check settings on managed devices, 304, 312
device access templates resource management, 76
editing automatic deployment plan template settings, 458
editing settings manually, 277, 458, 463
launch Telnet session to selected device, 217
manually edit auto discovery settings, 163
manually edit device settings, 155
manually editing template settings for segment-based discovery, 169
modify settings for selected device, 225
modifying template settings, 225
use existing auto discovery templates, 163
use existing device templates, 155
using batch mode to check settings, 282
using batch mode to configure, 277
using existing automatic deployment plan template, 459
using existing template to configure settings for device, 225
using existing templates, 225
using existing templates, 278
using existing templates, 278
using existing templates, 459
using existing templates, 464
using existing templates for segment-based discovery, 169
Telnet templates
adding a Telnet template, 77
deleting a Telnet template, 79
modifying a Telnet template, 78
Telnet template list, viewing, 77
Telnet template, adding, 77
Telnet template, deleting, 79
Telnet template, modifying, 78
viewing the telnet template list, 77
Telnet/SSH proxy
access and manage a device, 219
terminal access
access configuration, 332
allocating IP addresses, 317
history access log, 328
IP to MAC address binding, 339
real-time location, 331
unauthorized access, 322
unauthorized access processing policy, 343
third part device support
extending an existing function, 374
third party device support
extending a customized function, 385
TopN
accessing the view, 586
browsing alarms, 585
topology groupings
access service, 180
custom, 180
data center, 180
IP, 180
MPLS VPN, 180
VNM, 180
WSM service, 180
topology monitoring and management
left mouse-click monitoring, 182
right mouse-click link management, 186
right mouse-click monitoring, 183
translating requirements
access, device, 27
adding devices, 27
compiling information, 26
configuration, system, 27
device access, 27
devices, adding, 27
event management, 26
groups and views, 27
IMC access, 28
management, event and performance, 26
network infrastructure, 26
performance management, 26
system configuration, 27
trap definition settings
adding trap definitions, 544
importing trap definitions from a MIB file, 552
modifying trap definition severity settings, 551
modifying user-defined trap definitions, 548
querying for a trap, 544
viewing trap definitions, 543

trap details
viewing trap details, 527

trap management
browsing traps, 525
duplicate trap filter, 528
filter traps with existing rules, 528
filter traps with user-defined rules, 533
generate alarms from traps, 537
intermittent trap filter, 528
trap definition settings, 543
trap details, 526
trap query, 527
unknown trap filter, 528
unmanaged devices' trap filter, 528

trap query
advanced, 528
basic, 527

trunk port tab
adding trunk ports, 838
deleting trunk ports, 839
modifying trunk ports, 838
viewing trunk ports, 837

UAM. See User Access Manager
UBA. See User Behavior Auditor

unauthorized access
canceling action, 326
configuring switch access binding, 326
configuring terminal access binding, 325
deleting unauthorized access entries, 326
querying unauthorized access list, 323
refreshing unauthorized access list, 324
viewing unauthorized access list, 322
viewing unauthorized access log list, 323, 327

unauthorized access processing policy
configure conflict processing policy, 343
configure undefined access processing policy, 343

user groups
adding a user group, 131
adding a user subgroup, 132
deleting a user group, 133
deleting a user subgroup, 134
modifying a user group, 132
modifying a user subgroup, 133
viewing the user group list, 131

using Syslog to alarm rules
browsing Syslog to alarm rules, 561
copying Syslog to alarm rules, 566
creating user-defined Syslog to alarm rules, 562
deleting user-defined Syslog to alarm rules, 567
disabling Syslog to alarm rules, 567
enabling Syslog to alarm rules, 567
modifying a user-defined Syslog to alarm rules, 564

using the ACL assistant
configuring subnet mask types, 656
managing net address groups, 649
managing services, 646
managing time ranges, 652

using the Configuration Center
accessing the Configuration Center, 404
device configuration options, 406
querying for devices, 405

VC. See Virtual Connect

view configuration check report
exporting a report, 519
printing a report, 520

view configuration retrieval report
exporting a report, 520
printing a report, 520

view network assets
accessing network assets, 345
device level network asset details, 345
network asset list, 344
querying network assets, 347

view Syslog entries
browsing Syslog entries, 553

viewing ACL templates
viewing a template, 659
viewing the template list, 658

viewing alarm details
viewing from all alarms page, 568
viewing from real-time alarms page, 568
viewing from root alarms page, 568

viewing alarm relation report
exporting alarm relation report data, 578, 582
printing to PDF, 578, 582

viewing detailed information about a rule
advanced, 492
basic, 492

viewing devices
custom views, 200
device view, 176
IP view, 178
network topology view, 180

viewing performance reports
accessing a performance view list, 621
managing performance views, 624
organizing performance views, 623
querying a performance view list, 622
viewing rule list for an ACL resource
  advanced, 700
  basic, 700
  link, 701
rule info page for advanced ACL, 702
rule info page for link ACL, 703
rule info page for user-defined ACL, 703
rule info page for basic ACL, 702
time range info, 701
user-defined, 701
viewing SSC reports
  execution results report, 822
  Top 10 attack alarms report, 821
  Top 10 attack destinations report, 822
  Top 10 attack sources report, 821
viewing the check task list
  compliance policy information, 509
device information, 509
task attribute, 508
virtual interface tab
  adding a virtual interface, 834
deleting a virtual interface, 835
viewing the virtual interface, 833
virtual network manager
  configuring servers in virtual network manager, 363
  configuring virtual machines in virtual network manager, 365
querying servers, 362
refreshing virtual network view, 363
server details page, 360
viewing server level details, 360
viewing the resource list for a server, 359
viewing the virtual network, 358
viewing virtual network topology, 362
VLAN deployment task
  deleting deployment task entries, 843
  searching deployment tasks, 842
  viewing deployment tasks, 841
VLAN device details
  creating a VLAN, 832
  deleting a VLAN, 833
  modifying a VLAN, 833
  viewing VLANs, 831
VLAN device management
  access port tab, 835
  hybrid port tab, 839
query device, 830
trunk port tab, 837
viewing the VLAN device list, 829
virtual interface tab, 833
VLAN device details, 831
VLAN management
  deploying VLANs using batch mode, 844
  global VLAN management, 826
  VLAN deployment task, 841
  VLAN device management, 829
  VLAN topology maps, 843
VLAN topology maps, 843
VNM
  accessing server details page, 360
  adding port groups, 364
  adding vSwitch, 363
  configuring auto migration, 366
  joining virtual machines, 365
  manually migrating a virtual machine, 365
  modifying a VM profile, 366
  modifying advanced properties of a port group, 371
  modifying advanced properties of a vSwitch, 371
  performing a server query, 362
  querying migration recommendations, 368
  querying migration reports, 370
  refreshing server details page, 364
  refreshing the view, 363
  viewing, 358
  viewing migration reports, 369
  viewing server-level details, 360
  viewing the resource list for a server, 359
  viewing topology, 362
  viewing virtual machine recommendations, 367
VSM. See Voice Service Manager
wizard center
  quick start, 67
  third party device support, 68
WMI
  device access templates resource management, 89
WMI templates
  adding a WMI template, 89
  deleting a WMI template, 91
  modifying a WMI template, 90
  viewing the WMI template list, 89
WSM. See Wireless Service Manager