Abstract
This document contains setup, installation, and configuration information for HPE Virtual Connect. This document is for the person who installs, administers, and troubleshoots servers and storage systems. Hewlett Packard Enterprise assumes you are qualified in the servicing of computer equipment and trained in recognizing hazards in products with hazardous energy levels.
Contents

Documentation resources .........................................................................................................................6
  Virtual Connect documentation ..................................................................................................................6

Planning the installation ..............................................................................................................................8
  Virtual Connect overview ..........................................................................................................................8
  VC module supported firmware ..................................................................................................................9
  Pre-deployment planning ...........................................................................................................................9
  Hardware setup overview ..........................................................................................................................10
  Default module configuration ....................................................................................................................11
  Virtual Connect Manager setup overview ...............................................................................................12

Installation ...............................................................................................................................................13
  Installation requirements ............................................................................................................................13
    Supported configurations ..........................................................................................................................14
    Bay configuration requirements ..............................................................................................................16
    HPE Virtual Connect Flex-10 Module requirements ..............................................................................18
    HPE Virtual Connect Flex-10/10D Module requirements .....................................................................18
    HPE Virtual Connect FlexFabric 10Gb/24-port Module requirements ..................................................19
    HPE Virtual Connect FlexFabric-20/40 F8 Module requirements .........................................................19
    HPE Virtual Connect 16Gb 24-port Fibre Channel Module requirements .............................................20
    Virtual Connect and EBIPA .....................................................................................................................21
  Stacking links ...........................................................................................................................................21
    Stacking link guidelines ..........................................................................................................................21
    Recommended stacking connections .......................................................................................................22
    Partially stacked domains ..........................................................................................................................25
    Configure partially stacked domains .......................................................................................................26
    Network loop protection ............................................................................................................................26
  Connecting multiple enclosures ................................................................................................................27
    Using multiple enclosures .........................................................................................................................29
    Multiple enclosure requirements ............................................................................................................29
    FC and FlexFabric bay configuration using multiple enclosures ............................................................30
  Directly connecting VC domains .............................................................................................................32
  Virtual Connect FIPS mode of operation ...............................................................................................32
    FIPS mode information and guidelines .................................................................................................33
    FIPS mode protocol and feature restrictions .........................................................................................33
    Enabling FIPS mode ...............................................................................................................................34
    FIPS mode indicators (domain) ..............................................................................................................35
    FIPS mode indicators (VC Ethernet modules) .......................................................................................35
  Installing a VC-Enet module .....................................................................................................................35
  Installing a VC FlexFabric module ...........................................................................................................37
  Installing a VC-FC module ..........................................................................................................................40
  Installing DAC/AOC cables and transceivers ...........................................................................................41
    Installing a cable .......................................................................................................................................41
    Installing a transceiver ..............................................................................................................................42
  Removing QSFP+, SFP+ or SFP transceivers ..............................................................................................44
  Factory default settings ...............................................................................................................................44
  Connecting Virtual Connect Ethernet module uplinks ..........................................................................45
    Configuration example using a Cisco Core switch ..................................................................................48
  Failover and check-pointing .......................................................................................................................50
  Interconnect module upgrades ...................................................................................................................50
    Virtual Connect modules ..........................................................................................................................50
    Upgrading to an HPE Virtual Connect 16Gb 24-Port FC Module ............................................................51
    Upgrading to an HPE Virtual Connect 8Gb 24-Port FC Module ..............................................................52
    Upgrading to an HPE Virtual Connect 8Gb 20-Port FC Module ..............................................................52
Upgrading or removing an HPE Virtual Connect Flex-10, HPE Virtual Connect FlexFabric, or HPE Virtual Connect Flex-10/10D module ................................................................. 53
Upgrading to an HPE Virtual Connect FlexFabric module from a VC-FC module ........................................ 55
Onboard Administrator modules .................................................................................................................. 55

**HPE Virtual Connect Manager** .................................................................................................................. 57
Browser requirements and configuration ........................................................................................................... 57
Virtual Connect and Insight Control Server Deployment ................................................................................... 58
Accessing HPE Virtual Connect Manager ........................................................................................................ 58
Command Line Interface overview .................................................................................................................... 59
Logging on to the HPE Virtual Connect Manager GUI .................................................................................... 60
About HPE Virtual Connect Manager ................................................................................................................ 61
Reset Virtual Connect Manager ....................................................................................................................... 61
Recovering remote enclosures ............................................................................................................................ 61

Running the setup wizards ................................................................................................................................. 61
Virtual Connect Domain Setup Wizard .............................................................................................................. 61
Virtual Connect Network Setup Wizard ........................................................................................................... 77
HPE Virtual Connect Fibre Channel Setup Wizard ............................................................................................ 86
Virtual Connect Manager Server Profile Setup Wizard .................................................................................... 92

Verifying data center connections .................................................................................................................... 99
Verify link and speed .......................................................................................................................................... 99
Verify network status using VC Manager ........................................................................................................ 100

**Component identification** .......................................................................................................................... 101
HPE Virtual Connect Flex-10 10Gb Ethernet Module components and LEDs ................................................. 101
HPE Virtual Connect Flex-10 10Gb Ethernet Module components ...................................................................... 101
HPE Virtual Connect Flex-10 10Gb Ethernet Module LEDs ................................................................................ 102
HPE Virtual Connect Flex-10 10Gb Ethernet Module system maintenance switch .......................................... 104
HPE Virtual Connect Flex-10/10D Module components and LEDs ................................................................. 104
HPE Virtual Connect Flex10/10D Module components ..................................................................................... 104
HPE Virtual Connect Flex10/10D Module LEDs ................................................................................................ 105
HPE Virtual Connect Flex10/10D Module system maintenance switch ........................................................... 106
HPE Virtual Connect FlexFabric 10Gb/24-port Module components and LEDs .............................................. 107
HPE Virtual Connect FlexFabric 10Gb/24-port Module components .................................................................. 107
HPE Virtual Connect FlexFabric 10Gb/24-port Module LEDs ......................................................................... 108
HPE Virtual Connect FlexFabric 10Gb/24-port Module system maintenance switch ....................................... 110
HPE Virtual Connect FlexFabric-20/40 F8 Module components and LEDs .................................................. 111
HPE Virtual Connect FlexFabric-20/40 F8 Module components ...................................................................... 111
HPE Virtual Connect FlexFabric-20/40 F8 Module LEDs ............................................................................... 112
HPE Virtual Connect FlexFabric-20/40 F8 Module system maintenance switch ............................................. 114
HPE Virtual Connect 8Gb 24-Port Fibre Channel Module components and LEDs ......................................... 115
HPE VC 8Gb 24-Port FC Module components .................................................................................................. 115
HPE VC 8Gb 24-Port FC Module LEDs ............................................................................................................ 116
HPE VC 8Gb 24-Port FC Module system maintenance switch .......................................................................... 117
HPE Virtual Connect 8Gb 20-Port Fibre Channel Module components and LEDs .......................................... 118
HPE VC 8Gb 20-Port FC Module components .................................................................................................. 118
HPE VC 8Gb 20-Port FC Module LEDs ............................................................................................................ 119
HPE VC 8Gb 20-Port FC Module system maintenance switch ......................................................................... 120
HPE Virtual Connect 16Gb 24-Port FC Module components and LEDs ......................................................... 120
HPE VC 16Gb 24-Port FC Module components ............................................................................................... 120
HPE VC 16Gb 24-Port FC Module LEDs ........................................................................................................ 121
HPE VC 16Gb 24-Port FC Module system maintenance switch ..................................................................... 121

Resetting the Administrator password and DNS settings ............................................................................. 121

**Warranty and regulatory information** .......................................................................................................... 123
Warranty information ...................................................................................................................................... 123
Regulatory information .................................................................................................................................... 123
Safety and regulatory compliance ...................................................................................................................... 123
Belarus Kazakhstan Russia marking ................................................................................................................ 123
Turkey RoHS material content declaration ..................................................................................................... 124
Ukraine RoHS material content declaration .................................................................................................... 124
Electrostatic discharge .......................................................................................................................... 125
  Preventing electrostatic discharge ........................................................................................................ 125
  Grounding methods to prevent electrostatic discharge ........................................................................ 125
Support and other resources ................................................................................................................ 126
  Accessing Hewlett Packard Enterprise Support .................................................................................... 126
  Information to collect .............................................................................................................................. 126
  Accessing updates .................................................................................................................................. 126
  Websites .................................................................................................................................................. 126
  Customer Self Repair .............................................................................................................................. 127
  Remote support ....................................................................................................................................... 134
Acronyms and abbreviations ................................................................................................................ 135
Documentation feedback ....................................................................................................................... 138
Index ...................................................................................................................................................... 139
Virtual Connect documentation

The following Virtual Connect documentation is available on the Hewlett Packard Enterprise website (http://www.hpe.com/info/vc/manuals):

- **HPE Virtual Connect for c-Class BladeSystem User Guide**
  This guide provides details for the Virtual Connect GUI, including descriptions of screen contents and steps to set up domains, profiles, networks, and storage.

- **HPE Virtual Connect for c-Class BladeSystem Setup and Installation Guide**
  This guide provides hardware installation and configuration information for initial setup of a Virtual Connect solution. The guide also provides Virtual Connect module component and LED descriptions and guidelines for module installation and upgrades.

- **HPE Virtual Connect Manager Command Line Interface for c-Class BladeSystem User Guide**
  This guide provides information for using the Virtual Connect Command Line Interface, including use scenarios and complete descriptions of all subcommands and managed elements.

- **HPE Virtual Connect Ethernet Cookbook: Single and Multiple Domain (Stacked) Scenarios**
  This guide helps new Virtual Connect users understand the concepts of and implement steps for integrating Virtual Connect into a network. The scenarios in this guide vary from simplistic to more complex while covering a range of typical building blocks to use when designing Virtual Connect solutions.

- **HPE Virtual Connect Fibre Channel Networking Scenarios Cookbook**
  This guide details the concepts and implementation steps for integrating HPE BladeSystem Virtual Connect Fibre Channel components into an existing SAN fabric. The scenarios in this guide are simplistic while covering a range of typical building blocks to use when designing a solution.

- **HPE Virtual Connect with iSCSI Cookbook**
  This guide describes how to configure HPE Virtual Connect for an iSCSI environment. It provides tips and troubleshooting information for iSCSI boot and installation.

- **HPE Virtual Connect FlexFabric Cookbook**
  This guide provides users with an understanding of the concepts and steps required when integrating HPE BladeSystem and Virtual Connect Flex-10 or FlexFabric components into an existing network.

- **FCoE Cookbook for HPE Virtual Connect**
  This guide provides concept, implementation details, troubleshooting and use case scenarios of Fibre Channel over Ethernet through FIP Snooping using FC-BB-5 with HPE Virtual Connect.

- **HPE BladeSystem c-Class Virtual Connect Support Utility User Guide**
  This guide provides instructions for using the Virtual Connect Support Utility, which enables administrators to upgrade VC-Enet and VC-FC firmware and to perform other maintenance tasks remotely on both HPE BladeSystem c7000 and c3000 enclosures using a standalone, Windows-based, HP-UX, or Linux command line utility.

- **Release Notes**
  Release notes document new features, resolved issues, known issues, and important notes for each release of the Virtual Connect product and support utility.
The *HPE Virtual Connection Migration Guide* technical white paper on the Hewlett Packard Enterprise website ([http://www.hpe.com/info/VC-Migration](http://www.hpe.com/info/VC-Migration)) provides you with procedures to migrate from HPE VC 1/10 Ethernet modules to HPE Virtual Connect Flex-10/10D modules and retain VC-administered MAC and WW identifiers unchanged throughout the migration.
Planning the installation

Virtual Connect overview

HPE Virtual Connect is a set of interconnect modules and embedded software for HPE BladeSystem c-Class enclosures. VC implements server-edge virtualization between the server and the data center infrastructure so that networks can communicate with individual servers or pools of HPE BladeSystem server blades. You can upgrade, replace, or move server blades within the enclosures without visible changes to the external LAN and SAN environments. The external networks connect to a shared resource server pool rather than to individual servers. VC cleanly separates server enclosure administration from LAN and SAN administration.

VC simplifies the setup and administration of server connections and includes the following components:

- HPE Virtual Connect Manager
- VC Ethernet modules:
  - HPE VC Flex-10 10Gb Ethernet Module
  - HPE VC FlexFabric 10Gb/24-Port Module
  - HPE VC Flex-10/10D Module
  - HPE VC FlexFabric-20/40 F8 Module
- VC Fibre Channel modules:
  - HPE VC 8Gb 20-Port Fibre Channel Module
  - HPE VC 8Gb 24-Port Fibre Channel Module
  - HPE VC 16Gb 24-Port Fibre Channel Module

VC modules support HPE BladeSystem Enclosures and all server blades and networks contained within the enclosure:

- VC-Enet and FlexFabric modules enable connectivity to Ethernet switches, printers, laptops, rack servers, and network storage devices.
- VC-FC and FlexFabric modules enable connectivity to data center FC switches.
  Every FC fabric is limited in the number of switches it can support, but VC-FC and FlexFabric modules do not appear as switches to the FC fabric and do not count against FC fabric limits.

For information on module support of enclosures and configurations, see the product QuickSpecs on the Hewlett Packard Enterprise website (http://www.hpe.com/info/qs).

VCM is embedded on VC-Enet and FlexFabric modules, and is accessed through a web-based GUI or CLI. These interfaces are also accessible from Onboard Administrator.

A basic VC domain includes a single HPE c-Class BladeSystem c7000 Enclosure for a total of 16 servers (or up to 32 servers if the double-dense option is enabled), or a single HPE c-Class BladeSystem c3000 Enclosure for a total of 8 servers (or up to 16 servers if the double-dense option is enabled).

Within the domain, any server blade with the requisite LAN or SAN devices can access any LAN or SAN connected to a VC module, and a server blade of a given processor type (Integrity or X86) can be used as a spare for any server blade of the same processor type within the same enclosure, as long as the server has the requisite number and type of connections. Using the network access groups feature, the network administrator can clearly define a separation of networks based on their allowed functionality and prevent the server administrator from assigning specific network combinations in the same server profile.
By stacking (cabling) the VC-Enet modules together within the domain and connecting the VC-FC or FlexFabric module FC uplinks on the same bay of all enclosures to the same FC switch, every server blade in the domain can be configured to access any external network or fabric connection. With this configuration, you can use VCM to deploy and migrate a server blade profile to any server in the Virtual Connect domain without changing external LAN or SAN configurations.

**VC module supported firmware**

The following table lists all Virtual Connect modules and the highest firmware supported on that module.

<table>
<thead>
<tr>
<th>Module</th>
<th>Highest VC firmware supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>HPE Virtual Connect 16Gb 24-Port Fibre Channel Module</td>
<td>4.50</td>
</tr>
<tr>
<td>HPE Virtual Connect FlexFabric-20/40 F8 Module</td>
<td>4.50</td>
</tr>
<tr>
<td>HPE Virtual Connect Flex-10/10D Module</td>
<td>4.50</td>
</tr>
<tr>
<td>HPE Virtual Connect FlexFabric 10Gb/24-port Module</td>
<td>4.50</td>
</tr>
<tr>
<td>HPE Virtual Connect Flex-10 10Gb Ethernet Module</td>
<td>4.50</td>
</tr>
<tr>
<td>HPE Virtual Connect 8Gb 24-Port Fibre Channel Module</td>
<td>4.50</td>
</tr>
<tr>
<td>HPE Virtual Connect 8Gb 20-Port Fibre Channel Module</td>
<td>4.50</td>
</tr>
<tr>
<td>HPE Virtual Connect 4Gb Fibre Channel Module</td>
<td>4.45</td>
</tr>
<tr>
<td>HPE 4Gb Virtual Connect Fibre Channel Module</td>
<td>4.01</td>
</tr>
<tr>
<td>HPE 1/10Gb-F Virtual Connect Ethernet Module</td>
<td>3.62</td>
</tr>
<tr>
<td>HPE 1/10Gb Virtual Connect Ethernet Module</td>
<td>3.62</td>
</tr>
</tbody>
</table>

**Pre-deployment planning**

During the planning phase, the LAN and server administrator must determine how each server blade will connect to the network and on which IP network and VLAN the server will reside. In a traditional network, these connections are established through physical cables. If a move from one network to another is required, the cables must also be moved. Virtual Connect provides a wire-once implementation when VC modules are connected to upstream or core switches and the VC networks and server profiles are defined. Assigning a server profile to a server blade completes the physical connection to the core network. If a server blade fails or moves, all of the configuration parameters can be transferred easily to the new server.

Before beginning installation, complete the following tasks:

- Be sure that the firmware revisions on all VC modules in the domain are at the same revision level. The active VCM does not allow incompatible modules to be managed as part of the same VC domain.
- Be sure that OA, iLO, server blade system ROM, Ethernet option ROM, and FC option ROM firmware are up-to-date.
- Determine which mezzanine cards, HBAs, and interconnect modules are going to be used and where they will be installed in the enclosure. For installation and information on mapping server ports to interconnect bays, see the appropriate HPE BladeSystem enclosure setup and installation guide on the Hewlett Packard Enterprise website (http://www.hpe.com/support/BladeSystem/docs).
- If your organization requires the use of secure protocols and standards, consider the security requirements and restrictions of enabling FIPS mode ("Virtual Connect FIPS mode of operation" on page 32).

For a current status on FIPS certification, see the Hewlett Packard Enterprise website (http://hpe.com/info/government-certifications).
• Determine the Ethernet stacking cable layout, and ensure that the proper cable and transceiver options are ordered. Stacking cables enable any Ethernet NIC from any server to be connected to any of the Ethernet networks defined for the enclosure using stacking links.
  o For information on stacking links, see "Stacking links (on page 21)."
  o For information on stacking cable configurations, see "Recommended stacking connections (on page 22)."
  o For information on supported cable and transceiver options, see the Virtual Connect module QuickSpecs on the Hewlett Packard Enterprise website (http://www.hpe.com/info/qspec).

• Determine which Ethernet networks will be connected to or contained within the enclosure.
  Most installations will have multiple Ethernet networks, each typically mapped to a specific IP subnet. Virtual Connect Ethernet networks can be contained completely within the enclosure for server-to-server communication, or connected to external networks through rear panel ports (uplinks). For each network, the administrator must use the VCM to identify the network by name and to define any external port connections.

• Determine which Fibre Channel fabrics will be connected to the enclosure.
  Each uplink has a capability of aggregating up to 16 server HBA N-port links into an N-port uplink through the use of NPIV.

• Coordinate with data center personnel to ensure Ethernet network cable connections and Fibre Channel cable connections to the enclosure are installed or scheduled to be installed.

• Determine the Ethernet MAC address range to be used for the servers within the enclosure.
  Server and networking administrators should fully understand the selection and use of MAC address ranges before configuring the enclosure. For more information, see "MAC address settings (on page 72)."

• Determine the FC World Wide Name (WWN) range to be used for servers within the enclosure.
  Server and storage administrators should fully understand the selection and use of WWN ranges before configuring the enclosure. For more information, see "WWN settings (on page 86)."

• Identify the administrators for the Virtual Connect environment, and identify what roles and administrative privileges they will require. The VCM classifies each operation as requiring server, network, domain, or storage privileges. A single user may have any combination of these privileges. For more information, see the information on local users in the HPE Virtual Connect for c-Class BladeSystem User Guide on the Hewlett Packard Enterprise website (http://www.hpe.com/info/vc/manuals).

  IMPORTANT: If you plan on using VC-assigned MAC addresses and WWNs and are also working with server software that will be licensed by MAC addresses or WWNs, assign server profiles before deploying an image through RDP or attaching a license.

Hardware setup overview

The following steps provide an overview of setting up the interconnect modules:

1. Install and set up the enclosure. See the appropriate HPE BladeSystem enclosure quick install instructions on the Hewlett Packard Enterprise website (http://www.hpe.com/support/BladeSystem/docs).

2. Install the interconnect modules ("Installation" on page 13).
   To enable FIPS mode for the domain, be sure to configure the Virtual Connect Ethernet modules ("Virtual Connect FIPS mode of operation" on page 32).
   Plan your installation carefully. After the VC domain has been created, the position and type of the primary and backup VC modules cannot be changed without deleting and recreating the domain.

3. Install stacking links ("Recommended stacking connections" on page 22).
4. Connect the VC-Enet module uplinks to data center networks. The network administrator should have already installed the network cables into the rack with the proper labels. See "Connecting Virtual Connect Ethernet module uplinks (on page 45)."

5. Connect data center FC fabric links (if applicable).

6. Note the default DNS name, user name, and password settings for the primary VC module, available on the module Default Network Settings label.
   - The primary VC module is the first VC-Enet module in an odd-numbered interconnect bay.


8. Apply power to the enclosures. See "Default module configuration (on page 11).” Also see the appropriate HPE BladeSystem enclosure quick install instructions on the Hewlett Packard Enterprise website (http://www.hpe.com/support/BladeSystem/docs).


10. Be sure that all Virtual Connect interconnect module management interfaces and server blade iLO interfaces have valid IP and gateway addresses using one of the following methods:
    - Run DHCP on the management network connected to the Onboard Administrator.
    - Configure the Onboard Administrator to set enclosure bay IP addresses. See "Virtual Connect and EBIPA (on page 21)."

11. Be sure that OA, iLO, server blade system ROM, Ethernet option ROM, and FC option ROM firmware are current.

12. Access VCM using one of the following methods:
    - Use a web link from within the Onboard Administrator GUI or use the dynamic DNS name from the Default Network Settings label. See "Accessing HPE Virtual Connect Manager (on page 58)."
    - Access the VCM CLI remotely through an SSH session. See the HPE Virtual Connect Manager Command Line Interface User Guide on the Hewlett Packard Enterprise website (http://www.hpe.com/info/vc/manuals).

**IMPORTANT:** For proper management of enclosure devices there must be an Ethernet connection from the Onboard Administrator module to the external management network. For information on Onboard Administrator module cabling, see the HPE BladeSystem Onboard Administrator User Guide.

---

**Default module configuration**

When VC modules are inserted into an enclosure that is not yet part of a Virtual Connect domain, the modules are configured to provide basic connectivity. After a Virtual Connect domain is defined for an enclosure, server blades within that enclosure are isolated from all external network and fabric connections until configured explicitly within VCM.

When not part of a Virtual Connect domain, each VC-Enet module is configured so that all server ports connected to that module are connected to a single network, which is then connected to a single uplink. To provide greater bandwidth, you can use LACP to aggregate additional ports on that module, as long as they are connected to the same external switch. For aggregation of links to an external switch, the external switch must support dynamic creation of link aggregation groups using the IEEE 802.3ad LACP. All stacking links are disabled. This default configuration enables connectivity testing between server NICs and devices outside the enclosure prior to Virtual Connect domain configuration.

When not part of a Virtual Connect domain, all of the VC-FC Module uplink ports are grouped into an uplink port group and dynamically distribute connectivity from all server blades across all available uplink ports.
Virtual Connect Manager setup overview

The following steps provide an overview of setting up VCM:

1. Log in and run the domain setup wizard ("Virtual Connect Domain Setup Wizard" on page 61).
   a. Import the enclosure.
   b. Name the Virtual Connect domain.
   c. Set up local user accounts and privileges.

   **TIP:** If you want to setup network access groups, uncheck the "Start the Network Setup Wizard" checkbox on the Finish screen of the Domain Setup Wizard.

2. Define network access groups. For more information about network access groups, see "Network Access Groups screen" in the user guide.
   a. Select **Network Access Group** from the Define pull-down menu.
   b. Set up network access groups. For more information about creating network access groups, see "Define Network Access Group screen" in the user guide.

3. Run the network setup wizard ("Virtual Connect Network Setup Wizard" on page 71).
   a. Assign the MAC addresses used by server blade Ethernet network adapters within the Virtual Connect domain ("MAC Address Settings" on page 72).
   b. Configure server VLAN tagging support.
   c. Set up the networks.

4. Run the Fibre Channel setup wizard.
   a. Select a WWN range to be used by server blade FC HBAs ("WWN settings" on page 86).
   b. Define the SAN fabrics.

5. If you created associated networks using the network setup wizard, all networks are assigned to the Default network access group. You must be sure that all networks are in the proper network access group before running the server profile setup wizard. For more information about editing network access groups, see "Edit Network Access Group screen" in the user guide.

6. Run the server profile setup wizard ("Virtual Connect Manager Server Profile Setup Wizard" on page 92).
   a. Assign serial numbers to server blades within the domain.
   b. Create a server profile definition.
   c. Assign server profiles.
   d. Name server profiles.
   e. Create server profiles.

After an enclosure is imported into a Virtual Connect domain, server blades that have not been assigned a server profile are isolated from all networks to ensure that only properly configured server blades are attached to data center networks.

A server profile can be assigned and defined for each device bay so that the server blade can be powered on and connected to a deployment network. These profiles can then later be modified or replaced by another server profile.

A server profile can also be assigned to an empty bay to enable deployment at a later date.
Installation

Installation requirements

⚠️ CAUTION: Always use blanks to fill empty spaces in enclosures. This arrangement ensures proper airflow. Using an enclosure without the proper blanks results in improper cooling that can lead to thermal damage.

Observe the following requirements:

- In all Virtual Connect configurations, a VC-Enet or FlexFabric module must be installed in the enclosure. The embedded VCM operates on this module.
- VC-Enet modules are used typically in pairs to provide access to all Ethernet controllers on the server blade.
- The specific interconnect bays with Ethernet connectivity depend on mezzanine card locations within the server blade.
- For c3000 enclosures, when two Fibre Channel mezzanine cards are installed in slots 2 and 3 of a full-height server blade, the VC Manager only creates Fibre Channel connections and assigns WWNs to the ports associated with the Fibre Channel mezzanine card in slot 2. This restriction does not apply for c7000 enclosures.
- For each Ethernet mezzanine port you want to manage with VCM, install a VC-Enet, HPE VC FlexFabric-20/40 F8 Module, or HPE VC FlexFabric 10Gb/24-port Module in the interconnect bay connected to that port. For more information, see the appropriate HPE BladeSystem enclosure setup and installation guide.
- For Ethernet connections, Virtual Connect can be configured to assign or migrate MAC addresses for device bay ports connected to VC-Enet or FlexFabric modules.
- For Fibre Channel connections, FlexFabric module SFP ports can be connected only to Fibre Channel switch ports that support N_port_ID virtualization. To verify that NPIV support is provided, see the firmware documentation that ships with the Fibre Channel switch.
- When using optional transceiver modules, or when using stacking cables to connect multiple VC-Enet modules or multiple FlexFabric modules, order the cables and transceiver modules separately. For more information, see the HPE Virtual Connect QuickSpecs on the Hewlett Packard Enterprise website (http://www.hpe.com/info/vc/manuals).
- All modules in the enclosure require a valid and unique IP address, and all modules must be on the same subnet. Use a DHCP server or the Onboard Administrator EBIPA feature to assign each module an IP address.
- For server or I/O interconnect hardware changes that involve adding or removing Flex-10 functionality, the profile assigned to a server or server bay must be removed, all hardware changes performed, and the profile reassigned. Otherwise, indeterminate network operation might occur. For more information, see "Upgrading or removing an HPE Virtual Connect Flex-10, HPE Virtual Connect FlexFabric, or HPE Virtual Connect Flex-10/10D module (on page 53)."

Additional information

- For the most up-to-date support information, see the Hewlett Packard Enterprise website (http://www.hpe.com/storage/spock). Simple registration is required.
- For more information on the association between the server blade mezzanine connectors and the interconnect bays, see the HPE BladeSystem enclosure setup and installation guide that ships with
the enclosure. During server blade installation, the location of the mezzanine card determines the installation location of the interconnect modules.

- For specific interconnect module port connection information for each server blade, see the HPE BladeSystem enclosure setup and installation guide that ships with the enclosure. Connections differ by server blade type.
- For more information on BladeSystem port mapping, see the HPE BladeSystem enclosure setup and installation guide that ships with the enclosure.
- For the most current product information, see the release notes on the Hewlett Packard Enterprise website (http://www.hpe.com/info/vc/manuals).

**Supported configurations**

The following table outlines the Ethernet, Fibre Channel, and enclosure support for each version of Virtual Connect.

<table>
<thead>
<tr>
<th>VC firmware version</th>
<th>Enclosure</th>
<th>FlexFabric support per domain</th>
<th>Ethernet support per domain</th>
<th>FC support per domain</th>
<th>Enclosures per single VC domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.10</td>
<td>c3000</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>1.10</td>
<td>c7000</td>
<td>—</td>
<td>Up to 8 modules</td>
<td>Up to 4 modules</td>
<td>1</td>
</tr>
<tr>
<td>1.20</td>
<td>c3000</td>
<td>—</td>
<td>Up to 4 modules</td>
<td>Up to 2 modules</td>
<td>1</td>
</tr>
<tr>
<td>2.10/3.00/3.10</td>
<td>c7000</td>
<td>—</td>
<td>Up to 16 modules</td>
<td>Up to 16 modules</td>
<td>Up to 4</td>
</tr>
<tr>
<td>2.10/3.00/3.10</td>
<td>c3000</td>
<td>—</td>
<td>Up to 4 modules</td>
<td>Up to 2 modules</td>
<td>1</td>
</tr>
<tr>
<td>3.15/3.17/3.30/3.51/3.6x 3.70/3.75/4.01/4.10</td>
<td>c7000</td>
<td>Up to 16 modules*</td>
<td>Up to 16 modules</td>
<td>Up to 16 modules</td>
<td>Up to 4</td>
</tr>
<tr>
<td>3.15/3.17/3.30/3.51/3.6x 3.70/3.75/4.01/4.10 4.20/4.30/4.40/4.41/4.45 4.50</td>
<td>c3000</td>
<td>—</td>
<td>Up to 4 modules</td>
<td>Up to 2 modules</td>
<td>1</td>
</tr>
<tr>
<td>4.20/4.30/4.40/4.41/4.45 4.50</td>
<td>c7000</td>
<td>Up to 16 modules*</td>
<td>Up to 16 modules</td>
<td>Up to 16 modules</td>
<td>Up to 4</td>
</tr>
</tbody>
</table>

*A FlexFabric module counts as one Ethernet and one VC-FC module. Combinations of FlexFabric, VC-Enet, and VC-FC modules are allowed as long as the 16-module limit for each module type (Ethernet and FC) is not exceeded in the domain.

**HPE BladeSystem c3000 Enclosure supported configurations**

The following tables show commonly supported configurations for an HPE BladeSystem c3000 Enclosure.

**Bay 1**
- VC Ethernet

**Bay 2**
- VC Ethernet

**Bay 3**
- Other/empty

**Bay 4**
- Other/empty*

**Bay 1**
- VC Ethernet

**Bay 2**
- VC Ethernet

**Bay 3**
- VC Ethernet

**Bay 4**
- VC Ethernet

**Bay 1**
- VC Ethernet

**Bay 2**
- VC Ethernet

**Bay 3**
- VC-FC

**Bay 4**
- VC-FC

**Bay 1**
- Other/empty

**Bay 2**
- Other/empty

**Bay 3**
- VC Ethernet

**Bay 4**
- VC Ethernet
Installing a VC Ethernet module in Bay 1 and a Fibre Channel module in bay 2 is not supported. The HPE Virtual Connect Flex 10/10D Module is supported as an Ethernet only module. The following VC modules are not supported in HPE BladeSystem c3000 Enclosures:
- HPE Virtual Connect FlexFabric-20/40 F8 Module
- HPE Virtual Connect 16Gb 24-Port Fibre Channel
- HPE Virtual Connect FlexFabric 10Gb 24-Port Module

**HPE BladeSystem c7000 Enclosure supported configurations**

The following tables show commonly supported configurations for an HPE BladeSystem c7000 Enclosure.

<table>
<thead>
<tr>
<th>Bay 1</th>
<th>Bay 2</th>
<th>Bay 3</th>
<th>Bay 4</th>
<th>Bay 5</th>
<th>Bay 6</th>
<th>Bay 7</th>
<th>Bay 8</th>
</tr>
</thead>
<tbody>
<tr>
<td>VC Ethernet</td>
<td>Empty</td>
<td>Other/empty</td>
<td>Other/empty</td>
<td>Other/empty</td>
<td>Other/empty</td>
<td>Other/empty</td>
<td>Other/empty</td>
</tr>
<tr>
<td>Other/empty</td>
<td></td>
<td>Other/empty</td>
<td>Other/empty</td>
<td>Other/empty</td>
<td>Other/empty</td>
<td>Other/empty</td>
<td>Other/empty</td>
</tr>
<tr>
<td>Other/empty</td>
<td></td>
<td>Other/empty</td>
<td>Other/empty</td>
<td>Other/empty</td>
<td>Other/empty</td>
<td>Other/empty</td>
<td>Other/empty</td>
</tr>
<tr>
<td>Other/empty</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Other** indicates any VC interconnect module for c-Class BladeSystem.

<table>
<thead>
<tr>
<th>Bay 1</th>
<th>Bay 2</th>
<th>Bay 3</th>
<th>Bay 4</th>
<th>Bay 5</th>
<th>Bay 6</th>
<th>Bay 7</th>
<th>Bay 8</th>
</tr>
</thead>
<tbody>
<tr>
<td>VC Ethernet</td>
<td>VC Ethernet</td>
<td>Other/empty</td>
<td>Other/empty</td>
<td>Other/empty</td>
<td>Other/empty</td>
<td>Other/empty</td>
<td>Other/empty</td>
</tr>
<tr>
<td>Other/empty</td>
<td>Other/empty</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other/empty</td>
<td>Other/empty</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other/empty</td>
<td>Other/empty</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Requires minimum VC v3.10 firmware

<table>
<thead>
<tr>
<th>Bay 1</th>
<th>Bay 2</th>
<th>Bay 3</th>
<th>Bay 4</th>
<th>Bay 5</th>
<th>Bay 6</th>
<th>Bay 7</th>
<th>Bay 8</th>
</tr>
</thead>
<tbody>
<tr>
<td>VC Ethernet</td>
<td>VC Ethernet</td>
<td>VC Ethernet</td>
<td>Other/empty</td>
<td>Other/empty</td>
<td>Other/empty</td>
<td>Other/empty</td>
<td>Other/empty</td>
</tr>
<tr>
<td>VC Ethernet</td>
<td>VC Ethernet</td>
<td>VC Ethernet</td>
<td>Other/empty</td>
<td>Other/empty</td>
<td>Other/empty</td>
<td>Other/empty</td>
<td>Other/empty</td>
</tr>
<tr>
<td>VC Ethernet</td>
<td>VC Ethernet</td>
<td>VC Ethernet</td>
<td>Other/empty</td>
<td>Other/empty</td>
<td>Other/empty</td>
<td>Other/empty</td>
<td>Other/empty</td>
</tr>
<tr>
<td>Other/empty</td>
<td>Other/empty</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Bay 1</th>
<th>Bay 2</th>
<th>Bay 3</th>
<th>Bay 4</th>
<th>Bay 5</th>
<th>Bay 6</th>
<th>Bay 7</th>
<th>Bay 8</th>
</tr>
</thead>
<tbody>
<tr>
<td>VC Ethernet</td>
<td>Empty</td>
<td>VC-FC</td>
<td>Empty</td>
<td>Other/empty</td>
<td>Other/empty</td>
<td>Other/empty</td>
<td>Other/empty</td>
</tr>
<tr>
<td>VC Ethernet</td>
<td>Empty</td>
<td>VC-FC</td>
<td>Empty</td>
<td>Other/empty</td>
<td>Other/empty</td>
<td>Other/empty</td>
<td>Other/empty</td>
</tr>
<tr>
<td>VC-FC</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Bay 1</th>
<th>Bay 2</th>
<th>Bay 3</th>
<th>Bay 4</th>
<th>Bay 5</th>
<th>Bay 6</th>
<th>Bay 7</th>
<th>Bay 8</th>
</tr>
</thead>
<tbody>
<tr>
<td>VC Ethernet</td>
<td>VC Ethernet</td>
<td>VC Ethernet</td>
<td>VC Ethernet</td>
<td>Other/empty</td>
<td>Other/empty</td>
<td>Other/empty</td>
<td>Other/empty</td>
</tr>
<tr>
<td>VC-FC</td>
<td></td>
<td>VC-FC</td>
<td></td>
<td>Other/empty</td>
<td>Other/empty</td>
<td>Other/empty</td>
<td>Other/empty</td>
</tr>
<tr>
<td>VC-FC</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Bay configuration requirements

Primary and backup VC modules

Observe the following requirements when installing primary and backup interconnect modules:

- Plan your installation carefully. After the VC domain has been created, the position and type of the primary and backup VC modules cannot be changed without deleting and recreating the domain.

  **IMPORTANT:** The primary bay pair cannot be changed after the domain is created, including through a restore configuration file operation.

- To support failover configurations, install two VC-Enet modules or two FlexFabric modules in horizontally adjacent bays.

- To support high availability of the Virtual Connect environment, Hewlett Packard Enterprise recommends that VC-Enet modules are installed in horizontally adjacent interconnect bays. The embedded VCM operates in an active/standby configuration. For more information, see "Failover and check-pointing (on page 50)."

- To set up and configure VC, an odd-numbered interconnect bay must be populated with a VC-Enet module or FlexFabric module. The lowest odd-numbered interconnect bay populated with a VC-Enet module or FlexFabric module becomes the primary VC module.
Horizontally adjacent interconnect bays

Observe the following requirements when installing interconnect modules in horizontally adjacent bays:

- When the following modules are installed in an interconnect bay, only an identical module can reside in the horizontally adjacent bay:
  - VC-Enet Modules
  - HPE Virtual Connect Flex-10 10Gb Ethernet Modules
  - HPE Virtual Connect Flex-10/10D Modules
  - HPE Virtual Connect FlexFabric-20/40 F8 Modules
  - HPE Virtual Connect FlexFabric 10Gb/24-port Modules
  - HPE Virtual Connect 8Gb 20-Port Fibre Channel Modules
  - HPE Virtual Connect 8Gb 24-Port Fibre Channel Modules
  - HPE Virtual Connect 16Gb 24-Port Fibre Channel Modules

- Do not install Fibre Channel modules in interconnect bays 1 or 2.

- Do not mix HPE VC 8Gb or 16Gb 24-Port FC Modules with HPE VC 4Gb or 8Gb 20-Port FC Modules in interconnect bays connected to the same server blade mezzanine card.

- To avoid electronic keying errors, do not install VC-Enet modules and VC-FC modules in interconnect bays connected to the same server blade mezzanine card.

- Do not install Virtual Connect and non-Virtual Connect modules in interconnect bays connected to the same server blade mezzanine card.

<table>
<thead>
<tr>
<th>Odd numbered bay</th>
<th>Horizontally adjacent bay</th>
<th>Good configuration?</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>VC FlexFabric 10Gb/24-port</td>
<td>VC FlexFabric 10Gb/24-port</td>
<td>Yes</td>
<td>—</td>
</tr>
<tr>
<td>VC FlexFabric 10Gb/24-port</td>
<td>Flex-10 Enet</td>
<td>No</td>
<td>Install only HPE VC FlexFabric 10Gb/24-port Modules into bays horizontally adjacent to bays containing HPE VC FlexFabric 10Gb/24-port Modules.</td>
</tr>
<tr>
<td>VC FlexFabric-20/40 F8</td>
<td>VC FlexFabric-20/40 F8</td>
<td>Yes</td>
<td>—</td>
</tr>
<tr>
<td>VC FlexFabric-20/40 F8</td>
<td>Flex-10 Enet</td>
<td>No</td>
<td>Install only HPE VC FlexFabric-20/40 F8 Modules into bays horizontally adjacent to bays containing HPE VC FlexFabric-20/40 F8 Modules.</td>
</tr>
<tr>
<td>Flex-10 Enet</td>
<td>Flex-10 Enet</td>
<td>Yes</td>
<td>—</td>
</tr>
<tr>
<td>Flex-10 Enet</td>
<td>Flex-10/10D</td>
<td>No</td>
<td>Install only HPE Flex-10 10Gb VC-Enet Modules into bays horizontally adjacent to bays containing HPE Flex-10 10Gb VC-Enet Modules.</td>
</tr>
<tr>
<td>Flex-10 Enet</td>
<td>4Gb FC with enhanced NPIV</td>
<td>No</td>
<td>Do not mix Ethernet and FC modules in horizontally adjacent bays.</td>
</tr>
<tr>
<td>Flex-10/10D</td>
<td>Flex-10/10D</td>
<td>Yes</td>
<td>—</td>
</tr>
<tr>
<td>Flex-10/10D</td>
<td>Flex-10 Enet</td>
<td>No</td>
<td>Install only HPE VC Flex-10/10D Modules into bays horizontally adjacent to bays containing HPE VC Flex-10/10D Modules.</td>
</tr>
<tr>
<td>4Gb FC</td>
<td>4Gb FC</td>
<td>Yes for 4.01 No for 4.10</td>
<td>Beginning with VC 4.10, the HPE 4Gb VC-FC Module is no longer supported.</td>
</tr>
<tr>
<td>4Gb FC</td>
<td>4Gb FC with enhanced NPIV</td>
<td>Yes for 4.01 No for 4.10</td>
<td>Beginning with VC 4.10, the HPE 4Gb VC-FC Module is no longer supported.</td>
</tr>
<tr>
<td>4Gb FC with enhanced NPIV</td>
<td>8Gb 20-Port FC</td>
<td>Yes</td>
<td>You can mix HPE VC 4Gb FC Modules (with enhanced NPIV) and HPE 8Gb 20-Port FC Modules in horizontally adjacent bays.</td>
</tr>
</tbody>
</table>
## HPE Virtual Connect Flex-10 Module requirements

The following requirements apply to the installation or replacement of HPE Virtual Connect Flex-10 10Gb Ethernet Modules:

- Only install HPE Virtual Connect Flex-10 Modules into bays horizontally adjacent to bays containing another HPE Virtual Connect Flex-10 Module.
  
  If any other type of module is installed, the second one discovered is set to UNKNOWN, and no connections are made to the server NICs attached to the interconnect bay. The module is set to UNKNOWN because it is removed automatically from the VC domain when removed physically from the interconnect bay.

- If an HPE Virtual Connect Flex-10 Module is connected to a Flex-10 NIC that corresponds to an Ethernet connection in a server profile, then replacing the module with any other type of Virtual Connect Ethernet module requires that all network uplinks be removed from the module before replacement. For more information on module removal, see "Interconnect module removal and replacement."
  
  If the replacement module is not removed from the GUI, the module is marked as INCOMPATIBLE, and no connections are made to the server NICs attached to the interconnect bay.

- An empty interconnect bay horizontally adjacent to a bay containing an HPE Virtual Connect Flex-10 Module is treated as if it has a Flex-10-compatible Ethernet module for server configuration. If the corresponding server NIC is Flex-10, it is partitioned according to the connections in the server profile. Adding a module that does not support Flex-10 when the corresponding server is configured for Flex-10 results in the module being set to INCOMPATIBLE.

## HPE Virtual Connect Flex-10/10D Module requirements

The following requirements apply to the installation or replacement of HPE Virtual Connect Flex-10/10D Modules:

- Only install HPE Virtual Connect Flex-10/10D Modules into bays horizontally adjacent to bays containing another HPE Virtual Connect Flex-10/10D Module.
  
  If any other type of module is installed, the second one discovered is set to UNKNOWN, and no connections are made to the server NICs attached to the interconnect bay. The module is set to UNKNOWN because it is removed automatically from the VC domain when removed physically from the interconnect bay.

- If an HPE Virtual Connect Flex-10/10D Module is connected to a Flex-10 NIC that corresponds to an Ethernet connection in a server profile, then replacing the module with any other type of Virtual Connect Ethernet module requires that all network uplinks be removed from the module before replacement. For more information on module removal, see "Interconnect module removal and replacement."

### Odd numbered bay
<table>
<thead>
<tr>
<th>Horizontally adjacent bay</th>
<th>Good configuration?</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>8Gb 24-Port FC</td>
<td>8Gb 20-Port FC</td>
<td>No</td>
</tr>
<tr>
<td>16Gb 24-Port FC</td>
<td>8Gb 20-Port FC</td>
<td>No</td>
</tr>
<tr>
<td>VC FlexFabric 10Gb/24-port</td>
<td>8Gb 20-Port FC</td>
<td>No</td>
</tr>
<tr>
<td>VC-Enet or VC-FC</td>
<td>non-VC Other</td>
<td>No</td>
</tr>
</tbody>
</table>
If the replacement module is not removed from the GUI, the module is marked as INCOMPATIBLE, and no connections are made to the server NICs attached to the interconnect bay.

- An empty interconnect bay horizontally adjacent to a bay containing an HPE Virtual Connect Flex-10/10D Module is treated as if it has a Flex-10-compatible Ethernet module for server configuration. If the corresponding server NIC is Flex-10, it is partitioned according to the connections in the server profile. Adding a module that does not support Flex-10 when the corresponding server is configured for Flex-10 results in the module being set to INCOMPATIBLE.
- An HPE Virtual Connect Flex-10/10D Module can only be used in a domain running VC firmware v3.70 or higher, otherwise the module is marked as UNKNOWN.
- When the HPE Virtual Connect Flex-10/10D Module has ports configured to carry FCoE traffic, those ports do not support stacking.

HPE Virtual Connect FlexFabric 10Gb/24-port Module requirements

The following requirements apply to the installation or replacement of HPE Virtual Connect FlexFabric 10Gb/24-port Modules:

- For full storage network compatibility, each server blade attached to the HPE VC FlexFabric 10Gb/24-port Module must have either an embedded or mezzanine-based FlexFabric converged network adapter.
- Only install an HPE VC FlexFabric 10Gb/24-port Module in an interconnect bay horizontally adjacent to a bay that contains an HPE VC FlexFabric 10Gb/24-port Module.
- The HPE VC FlexFabric 10Gb/24-port Module only supports external stacking for Ethernet traffic. When the HPE VC FlexFabric 10Gb/24-port Module has ports configured to carry Fibre Channel or FCoE traffic, those ports do not support stacking.
- An HPE VC FlexFabric 10Gb/24-port Module can only be used in a domain running VC firmware v3.15 or higher, otherwise the module is marked as UNKNOWN.

HPE Virtual Connect FlexFabric-20/40 F8 Module requirements

The following requirements apply to the installation or replacement of HPE Virtual Connect FlexFabric-20/40 F8 Modules:

- The HPE VC FlexFabric-20/40 F8 Module is supported only on the following c7000 SKUs:
  - 5XXXXX-B21
  - 6XXXXX-B21
  - 7XXXXX-B21
  For information on updated SKUs, see the QuickSpecs on the Hewlett Packard Enterprise website (http://www.hpe.com/info/qs).
- If more than two HPE VC FlexFabric-20/40 F8 Modules are installed in a c7000 enclosure, the ambient operating temperature cannot exceed 30°C (86°F).
- Do not install more than six HPE VC FlexFabric-20/40 F8 Modules in a c7000 enclosure.
- Hewlett Packard Enterprise recommends a c7000 enclosure with a 10-fan configuration when HPE Virtual Connect FlexFabric-20/40 F8 Modules are installed.
- For full storage network compatibility, each server blade attached to the HPE VC FlexFabric-20/40 F8 Module must have either an embedded or mezzanine-based FlexFabric converged network adapter.
• Only install an HPE VC FlexFabric-20/40 F8 Module in an interconnect bay horizontally adjacent to a bay that contains an HPE VC FlexFabric-20/40 F8 Module.

• The HPE VC FlexFabric-20/40 F8 Module only supports external stacking for Ethernet traffic. When the HPE VC FlexFabric-20/40 F8 Module has ports configured to carry Fibre Channel or FCoE traffic, those ports do not support stacking.

• An HPE VC FlexFabric-20/40 F8 Module can only be used in a domain running VC firmware v4.20 or higher, otherwise the module is marked as UNKNOWN.

• VC uses the Link Aggregation Control Protocol to aggregate uplink ports into Link Aggregation Groups. A QSFP+ to SFP+ splitter cable must be used when aggregating from a QSFP+ port. Use the following table when configuring LAGs with the HPE VC FlexFabric-20/40 F8 Module.

<table>
<thead>
<tr>
<th>Port QX.1</th>
<th>Port QX.2</th>
<th>Port QX.3</th>
<th>Port QX.4</th>
<th>Port X1</th>
<th>Port X2</th>
<th>Port X3</th>
<th>Port X4</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

HPE Virtual Connect 16Gb 24-port Fibre Channel Module requirements

• The HPE Virtual Connect 16Gb 24-port Fibre Channel Module is compatible with first, second, and third generation HPE BladeSystem c7000 Enclosures:
  - First and second generation HPE BladeSystem c7000 Enclosures limit the speed between the server and the Fibre Channel Module to 8Gb.
  - Third generation (Platinum) HPE BladeSystem c7000 Enclosures (SKU 6XXXXX-B21 and 7XXXXX-B21) support 16Gb connectivity between the server and the Fibre Channel Module.

• The HPE Virtual Connect 16Gb 24-port Fibre Channel Module is not compatible with HPE BladeSystem c3000 Enclosures.

• Double-dense servers are not supported with the HPE Virtual Connect 16Gb 24-port Fibre Channel Module.

• Do not install an HPE Virtual Connect 16Gb 24-port Fibre Channel Module in interconnect bays 1 or 2. The HPE Virtual Connect 16Gb 24-port Fibre Channel Module can only be installed in interconnect bays 3–8.

• To configure the HPE Virtual Connect 16Gb 24-port Fibre Channel Module using Virtual Connect Manager, be sure to populate interconnect bays 1 or 2 with a Virtual Connect Ethernet module or FlexFabric module.

• Each server blade attached to the HPE Virtual Connect 16Gb 24-port Fibre Channel Module must have a Fibre Channel Host Bus Adapter which supports 8Gb or 16Gb speeds.

• To support a failover configuration for Virtual Connect Manager, install two HPE Virtual Connect 16Gb 24-port Fibre Channel Modules in horizontally adjacent bays.

• To avoid connectivity loss, do not install Virtual Connect and non-Virtual Connect modules in interconnect bays connected to the same server blade mezzanine card.

• To avoid electronic keying errors, do not install Virtual Connect Ethernet modules and Virtual Connect Fibre Channel modules in interconnect bays connected to the same server blade mezzanine card.
• N_port trunking is supported when connected to a Brocade FC switch.

• HPE Virtual Connect 16Gb 24-port Fibre Channel Module SFP+ ports can only be connected to Fibre Channel switch ports that support N_port_ID virtualization.

To verify that NPIV is supported, see the firmware documentation that ships with the Fibre Channel switch.

• All Virtual Connect modules in the enclosure require IP addresses and must all be on the same subnet. Use a DHCP server or the Onboard Administrator EBIPA feature to assign each module an IP address.

• If the HPE Virtual Connect 16Gb 24-port Fibre Channel Module is installed in a FIPS enabled domain, VCM permanently enables FIPS mode on the module. FIPS mode cannot be disabled for the module once it has been enabled.

• For information, see the latest Virtual Connect for c-Class BladeSystem User Guide in the VC Information Library (http://www.hpe.com/info/vc/manuals).

Virtual Connect and EBIPA

Enclosure Bay IP Addressing is used to specify IP addresses for the interconnect modules, which are then provided to the modules by the Onboard Administrator.

For information on using IPv6 with Virtual Connect, see the HPE Virtual Connect for c-Class BladeSystem User Guide on the Hewlett Packard Enterprise website (http://www.hpe.com/info/vc/manuals).

Because Virtual Connect communicates with other components through the Onboard Administrator, special considerations are required when using EBIPA with Virtual Connect Ethernet modules:

• The Onboard Administrator must be on the same IP subnet as all Virtual Connect modules.

• The Onboard Administrator IP address must be set properly before changing the IP addresses of the Virtual Connect modules.

Stacking links

Stacking links are used to add VC-Enet modules to a VC domain. This feature enables any server NIC physically connected to a VC module to be connected to any Ethernet network. By using stacking links, a single pair of uplinks can function as the data center network connections for the entire Virtual Connect domain.

Stacking link guidelines

Observe the following guidelines:

• Use uplink ports to connect modules to data center switches or stack VC-Enet modules and enclosures.

• Virtual Connect does not support stacking for FC modules. Each VC-FC module or FlexFabric module configured to carry Fibre Channel or FCoE traffic requires uplink connections to the external FC SAN environment.

• The following modules support only external stacking for Ethernet traffic:
  o HPE VC FlexFabric 10Gb/24-port
  o HPE VC FlexFabric-20/40 F8
  o HPE VC Flex-10/10D

When these modules have ports configured to carry Fibre Channel or FCoE traffic, those ports do not support stacking.
• Observe the following information when Ethernet modules are horizontally-adjacent:
  o HPE VC Flex-10 Enet modules
    Uplink ports X7 and X8 form internal stacking links between the modules when left unpopulated.
  o HPE VC FlexFabric 10Gb/24-Port modules
    Uplink ports X7 and X8 form internal stacking links between the modules when left unpopulated.
  o HPE VC Flex-10/10D Modules
    Ports X11, X12, X13, and X14 are dedicated 10Gb internal stacking links.
  o HPE VC FlexFabric-20/40 F8 Modules
    Ports X9 and X10 are dedicated 20Gb internal stacking links.

• Virtual Connect automatically detects when one VC-Enet module port is connected to another VC-Enet module port within the domain and changes the port ID indicator color to amber to indicate a stacking link.

• All VC-Enet modules within the Virtual Connect domain must be interconnected for fully-stacked configurations, and not for horizontal or primary-slice stacked configurations. Any combination of 1Gb and 10Gb cables can be used to interconnect the modules. If connecting HPE VC FlexFabric-20/40 F8 modules, 40Gb stacking cables can be used.

• ISL ports provide stacking links between horizontally adjacent modules.

• In partially stacked domains, the combination of a stacking link and horizontally-adjacent Enet modules is considered a logical interconnect. Logical interconnects are formed in horizontal and primary slice stacking modes.
  To configure a partially stacked domain, see "Partially stacked domains (on page 25)."

• Be sure to connect any stacking cables before running the network setup wizard.
  For recommended stacking cable configurations, see "Recommended stacking connections (on page 22)."

• To prevent VCM from using ports as stacking links, configure networks and ports before installing a cable.

Recommended stacking connections

Use the following table for recommended stacking connections.

<table>
<thead>
<tr>
<th>Single enclosure stacking</th>
<th>Modules (top to bottom)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stacking two modules</td>
<td></td>
</tr>
<tr>
<td>HPE Virtual Connect</td>
<td></td>
</tr>
<tr>
<td>FlexFabric 10Gb/24-port</td>
<td></td>
</tr>
<tr>
<td>Modules</td>
<td></td>
</tr>
<tr>
<td>HPE Virtual Connect</td>
<td></td>
</tr>
<tr>
<td>Flex-10 10Gb Ethernet</td>
<td></td>
</tr>
<tr>
<td>Modules</td>
<td></td>
</tr>
</tbody>
</table>

For recommended stacking cable configurations, see "Recommended stacking connections (on page 22)."
### Single enclosure stacking

<table>
<thead>
<tr>
<th>Modules (top to bottom)</th>
</tr>
</thead>
<tbody>
<tr>
<td>HPE Virtual Connect FlexFabric-20/40 F8 Modules</td>
</tr>
</tbody>
</table>

#### Stacking four modules
- HPE Virtual Connect FlexFabric 10Gb/24-port Modules
- HPE Virtual Connect FlexFabric 10Gb/24-port Modules
- HPE Virtual Connect Flex-10 10Gb Ethernet Modules
- HPE Virtual Connect FlexFabric-20/40 F8 Modules

#### Stacking six modules
- HPE Virtual Connect FlexFabric 10Gb/24-port Modules
- HPE Virtual Connect FlexFabric 10Gb/24-port Modules
- HPE Virtual Connect FlexFabric 10Gb/24-port Modules
## Single enclosure stacking

<table>
<thead>
<tr>
<th>Modules (top to bottom)</th>
</tr>
</thead>
<tbody>
<tr>
<td>- HPE Virtual Connect FlexFabric 10Gb/24-port Modules</td>
</tr>
<tr>
<td>- HPE Virtual Connect FlexFabric 10Gb/24-port Modules</td>
</tr>
<tr>
<td>- HPE Virtual Connect FlexFabric 10Gb/24-port Modules</td>
</tr>
<tr>
<td>- HPE Virtual Connect Flex-10 10Gb Ethernet Modules</td>
</tr>
</tbody>
</table>

## Stacking eight modules

<table>
<thead>
<tr>
<th>Modules (top to bottom)</th>
</tr>
</thead>
<tbody>
<tr>
<td>- HPE Virtual Connect FlexFabric 10Gb/24-port Modules</td>
</tr>
<tr>
<td>- HPE Virtual Connect FlexFabric 10Gb/24-port Modules</td>
</tr>
<tr>
<td>- HPE Virtual Connect FlexFabric 10Gb/24-port Modules</td>
</tr>
<tr>
<td>- HPE Virtual Connect FlexFabric-20/40 F8 Modules</td>
</tr>
</tbody>
</table>

### Diagrams

- Single enclosure stacking diagram
- Stacking eight modules diagram
### Single enclosure stacking

<table>
<thead>
<tr>
<th>Modules (top to bottom)</th>
</tr>
</thead>
<tbody>
<tr>
<td>• HPE Virtual Connect FlexFabric 10Gb/24-port Modules</td>
</tr>
<tr>
<td>• HPE Virtual Connect FlexFabric 10Gb/24-port Modules</td>
</tr>
<tr>
<td>• HPE Virtual Connect Flex-10 10Gb Ethernet Modules</td>
</tr>
<tr>
<td>• HPE Virtual Connect Flex-10 10Gb Ethernet Modules</td>
</tr>
</tbody>
</table>

The 1000BASE-T links can be used as stacking links of up to 100 m (328 ft). Ports with different connector types can be aggregated if the link speed is the same. For example, CX4 and SFP+ ports both running at 10G can be aggregated to provide enhanced throughput for the stacking link.

**NOTE:** The CX4 interface uses the same physical connector as InfiniBand, but InfiniBand cables are tuned differently and will not perform as well in CX4 applications. Hewlett Packard Enterprise recommends purchasing CX4 cable assemblies that meet the IEEE CX4 specifications and support 10-Gigabit communication at distances from 3 m to 15 m (9.84 ft to 49.20 ft).

For information on supported cables, see the module QuickSpecs on the Hewlett Packard Enterprise website ([http://www.hpe.com/info/vc/manuals](http://www.hpe.com/info/vc/manuals)).

Hewlett Packard Enterprise strongly recommends full redundancy of VC-Enet modules. The recommended stacking configurations have redundant connections. If a stacking cable is disconnected or fails, the Ethernet packets within the Virtual Connect domain are automatically re-routed to the uplink through the redundant path. This configuration helps preserve network connectivity if an Ethernet interconnect module fails or is removed.

### Partially stacked domains

A partially stacked domain uses logical interconnects to create stacking configurations in a VC domain. A logical interconnect is the combination of horizontally adjacent Enet modules and the internal stacking link that connects them.

The following stacking modes are available:
- **Full Stacking** is the default stacking mode for the VC domain. In Full Stacking, all Ethernet modules within the domain are connected by horizontal cross connects or by stacking cables.

- **Horizontal Stacking** disables all vertical stacking links. In horizontal stacking mode, each horizontal bay pair is a separate logical interconnect. For example, if bay 1 and bay 2 are populated, they form a logical interconnect.

- **Primary Slice Stacking** disables all stacking links outside of the primary slice. The primary slice is the primary and standby interconnect modules for the enclosure. In primary slice stacking, the primary slice is a logical interconnect.

When configuring horizontal or primary slice stacking, observe the following:

- A brief network outage occurs when you change the domain stacking mode.
- The following connections must reside within their configured logical interconnect for proper functionality. These connections must not span outside of their logical interconnect:
  - Network uplink ports
  - Shared uplink sets
  - Monitored ports
  - sFlow ports

  When configuring networks, uplink ports are filtered to ensure that all ports belong to the same logical interconnect.

- If there are connections not configured as stacking links between modules, the ports are linked and function as normal uplink ports.

- Server to server communications between logical interconnects requires a connection between the logical interconnects.

- Multiple enclosure configurations are supported and require that the primary slices of the enclosures be connected with stacking cables.

- Profile migrations are not supported in multi-enclosure domains.

- Double-dense mode is not supported.

- HPE BladeSystem c3000 Enclosures are not supported.

- Hewlett Packard Enterprise recommends enabling Smart Link.

**Configure partially stacked domains**

To configure the domain stacking mode, see the latest version of the following documents in the Virtual Connect Information Library (http://www.hpe.com/info/vc/manuals):

- **HPE Virtual Connect for c-Class BladeSystem User Guide**
- **HPE Virtual Connect Manager Command Line Interface for c-Class BladeSystem User Guide**

**Network loop protection**

To avoid network loops, Virtual Connect first verifies that only one active uplink exists per network from the Virtual Connect domain to the external Ethernet switching environment. Second, Virtual Connect makes sure that no network loops are created by the stacking links between Virtual Connect modules.

- One active link—A VC uplink set can include multiple uplink ports. To prevent a loop with broadcast traffic coming in one uplink and going out another, only one uplink or uplink LAG is active at a time. The uplink or LAG with the greatest bandwidth should be selected as the active uplink. If the active uplink loses the link, then the next best uplink is made active.
No loops through stacking links—If multiple VC-Enet modules are used, they are interconnected using stacking links, which might appear as an opportunity for loops within the VC environment. For each individual network in the Virtual Connect environment, VC blocks certain stacking links to ensure that each network has a loop-free topology.

Enhanced network loop protection detects loops on downlink ports, which can be a Flex-10 logical port or physical port. The feature applies to Flex-10 logical function if the Flex-10 port is operating under the control of DCC protocol. If DCC is not available, the feature applies to a physical downlink port.

Enhanced network loop protection uses two methods to detect loops:

- It periodically injects a special probe frame into the VC domain and monitors downlink ports for the looped back probe frame. If this special probe frame is detected on downlink ports, the port is considered to cause the loop condition.

  For tunneled networks, the probe frame transmission is extended over a longer period of time proportional to the number of tunneled networks. The probe frames are sent on a subset of tunnels every second until all tunnels are serviced.

- It monitors and intercepts common loop detection frames used in other switches. In network environments where the upstream switches send loop detection frames, the VC Enet modules must ensure that any downlink loops do not cause these frames to be sent back to the uplink ports. Even though VC probe frames ensure loops are detected, there is a small time window depending on the probe frame transmission interval in which the loop detection frames from the external switch might loop through down link ports and reach uplink ports. By intercepting the external loop detection frames on downlinks, the possibility of triggering loop protection on the upstream switch is eliminated. When network loop protection is enabled, VC-Enet modules intercept the following types of loop detection frames:
  - PVST+ BPDUs
  - Procurve Loop Protect frames

When the network loop protection feature is enabled, any probe frame or other supported loop detection frame received on a downlink port is considered to be causing the network loop, and the port is disabled immediately until an administrative action is taken. The administrative action involves resolving the loop condition and clearing the loop protection error condition. The "loop detected" status on a port can be cleared by one of the following administrative actions:

- Restart loop detection by issuing "reset" loop protection from the CLI or GUI
- Unassign all networks from the port in "loop detected" state

The SNMP agent supports trap generation when a loop condition is detected or cleared.

Virtual Connect provides the ability to enable or disable network loop protection. The feature is enabled by default and applies to all VC-Enet modules in the domain. Network loops are detected and server ports can be disabled even prior to any enclosure being imported.

A loop-protect reset command resets and restarts loop detection for all server ports in a "loop-detected" error condition.

For each individual network in the Virtual Connect environment, VC blocks certain stacking links to ensure that each network has a loop-free topology. VCM determines which stacking links are used to forward traffic by determining the shortest route from the module with the active uplink to the remaining stacked VC-Enet modules. For optimal stacking strategies, see HPE Virtual Connect for the Cisco Network Administrator in the HPE BladeSystem Information Library (http://www.hpe.com/support/BladeSystem/docs).

**Connecting multiple enclosures**

Virtual Connect supports the connection of up to four c7000 enclosures, which can reduce the number of network connections per rack and also enables a single VC Manager to control multiple enclosures. A single set of cables can be used to carry all external Ethernet traffic from a single rack.
Multiple enclosure support enables up to four c7000 enclosures to be managed within a single Virtual Connect domain.

Stacking multiple enclosures enables the management of up to four enclosures from a single control point. VC Manager operates in the primary enclosure, and it enables up to three additional remote enclosures of the same type to be added as part of a single VC domain. The locally managed primary enclosure must be imported into the domain before importing additional (remote) enclosures. If a failure occurs, the standby module in the primary enclosure takes over.

The VC Manager in the primary enclosure accesses all remote modules and OAs over the management network. The OAs for each enclosure to be managed as part of a VC domain must be on the same management subnet along with all of the VC-Enet and VC-FC modules that are in each enclosure. All enclosure OAs and VC modules within the same VC domain must be on the same lightly loaded subnet. Hewlett Packard Enterprise recommends that the OA IP addresses used are configured to be static. The VC-Enet modules use stacking cables between enclosures to route network traffic from any server port to any uplink port within the VC domain.

The VC-FC modules and FlexFabric FC-configured ports do not support stacking. Connecting multiple enclosures requires identical FC and FlexFabric module bay configuration in each enclosure. For more information, see "FC and FlexFabric bay configuration using multiple enclosures (on page 30)."

Multi-enclosure double dense domains require similar and compatible FC modules in bays 5, 6, 7, and 8 in all enclosures. If a multi-enclosure double dense configuration contains incompatible FC modules in bays 5, 6, 7, or 8 in either the local or remote enclosures, some or all of the compatible FC modules in the remote enclosures might be designated INCOMPATIBLE after import.
To add additional enclosures to a domain, see the HPE Virtual Connect for c-Class BladeSystem User Guide on the Hewlett Packard Enterprise website (http://www.hpe.com/info/vc/manuals).

Using multiple enclosures

Multiple enclosure support enables up to four c7000 enclosures to be managed within a single Virtual Connect domain. A VC-Enet or FlexFabric module connects each c7000 enclosure so that network traffic can be routed from any server Ethernet port to any uplink within the VC domain. When connecting multiple enclosures, observe the following information:

- c3000 enclosures are not supported in multiple enclosure domains.
- Use stacking cables to connect multiple enclosures.
- There are 16 half-height or 8 full-height server bays in a c7000 enclosure. A combination of full-height and half-height servers can be used in the same enclosure. If double-dense mode is enabled in the Domain Setup Wizard, each enclosure can support a total of 128 servers.
- A total of 16 Ethernet and 16 VC-FC type modules can be installed in a multi-enclosure domain. Each FlexFabric module counts as one Ethernet and one VC-FC module. Combinations of FlexFabric, VC-Enet and VC-FC modules are allowed as long as the 16-module limit for each module type (Ethernet and FC) is not exceeded in the domain.

For bay and module requirements, see "Installation requirements (on page 13)."

Multiple enclosure requirements

Observe the following requirements when connecting multiple enclosures:

- Each enclosure must have at least one supported VC Enet or FlexFabric module installed.
- If the domain stacking mode is configured to full stacking, all VC-Enet modules must be interconnected and redundantly stacked.
- If the domain stacking mode is configured to horizontal or primary slice stacking, the primary slice of each enclosure must be connected with stacking cables. The primary slice is the primary and standby interconnect modules for the enclosure.
- All enclosures must have the same FC and FlexFabric module configuration. For example, if bays 1 and 2 of the Primary Enclosure contain FlexFabric-20/40 F8 modules, then bays 1 and 2 of Remote Enclosures 1, 2, and 3 must also contain FlexFabric-20/40 F8 modules.
- All enclosures must have the same HPE VC Flex-10/10D module configuration. For example, if bays 1 and 2 of the Primary Enclosure contain HPE VC Flex-10/10D modules, then bays 1 and 2 of Remote Enclosures 1, 2, and 3 must also contain HPE VC Flex-10/10D modules.
- VC Fibre Channel or FlexFabric modules must be connected to the same FC switch to enable profile mobility.
- All Onboard Administrators and VC modules must be on the same lightly loaded and highly reliable management Ethernet network and IP subnet. If the management network is overloaded, configuration attempts may be disabled until the connectivity is re-established and synchronized with the domain.
- The VC-FC and FlexFabric FC-configured uplink port configuration must be identical across all enclosures.
- When FC connectivity is required in multi-enclosure double-dense domains, similar and compatible VC-FC modules are required in bays 5, 6, 7, and 8 in all enclosures.
If a multi-enclosure double-dense configuration contains incompatible VC-FC modules in bays 5, 6, 7, or 8 in any of the enclosures, some or all of the compatible VC-FC modules in the remote enclosures might be designated INCOMPATIBLE after import.

- The Onboard Administrator firmware must be version 3.11 or higher. Hewlett Packard Enterprise recommends using the latest version available.

- All Onboard Administrators must use the same user credentials. VCSU uses the primary credentials for the remote enclosure.

- When both Primary and Standby modules in the base enclosure are taken down for maintenance or lose power and are no longer present in the domain, the management capabilities in the VC domain are lost. Both the Primary and Standby modules in the base enclosure must be recovered to regain management access to the VC domain.

If network and fabric uplinks are defined on the remaining enclosures, the servers continue to have network and storage access.

**FC and FlexFabric bay configuration using multiple enclosures**

The VC-FC modules and FlexFabric FCoE or FC-configured uplinks do not support stacking. To ensure server profile mobility, the VC-FC and FlexFabric bay configurations must be identical for all enclosures in the domain.

For example, in a multi-enclosure domain with a total of four enclosures, if bays 3 and 4 of the Primary Enclosure contain VC-FC modules, then bays 3 and 4 of Remote Enclosures 1, 2, and 3 must also contain VC-FC modules. If bays 1 and 2 of the Primary Enclosure contain FlexFabric modules, then bays 1 and 2 of Remote Enclosures 1, 2, and 3 must also contain FlexFabric modules. The following illustration shows a valid VC-FC and FlexFabric bay configuration.
Sample valid VC-FC and FlexFabric bay configuration

The following illustration shows an invalid VC-FC and FlexFabric bay configuration. For VC-FC bay compatibility, Bay 4 in Remote Enclosure 1 is empty, and Bay 3 of Remote Enclosure 2 has an Ethernet module present. For FlexFabric bay compatibility, Bay 2 in Remote Enclosure 1 is empty, and Bay 1 of Remote Enclosure 2 has an Ethernet module present.
Sample invalid VC-FC and FlexFabric bay configuration

Directly connecting VC domains

In a multi-enclosure domain with properly installed stacking cables, each network defined in the domain is available to all server profiles in the domain without requiring any additional uplink ports. This configuration enables you to establish an open communication path between two or more enclosures.

You can also directly associate the uplinks from two enclosures from different domains so that servers in the two domains attached to the networks configured for those uplinks can communicate with one another. This configuration establishes a private communication path between the two enclosures. However, the communication path is public for all of those servers and applications associated with it. Traffic would not flow from an upstream switch over that direct connection.

The two enclosures can communicate with each other by a dedicated uplink port or a shared uplink port defined on each enclosure. These uplinks on the two enclosures can be “teamed” using LACP because both domains run LACP active. The link between the two enclosures cannot have any additional active links connected to other targets. Only networks defined for that link can be shared between the two enclosures.

Virtual Connect FIPS mode of operation

Beginning with version 4.30, Virtual Connect supports FIPS 140-2 Level 1 security requirements. Enabling FIPS mode requires the use of secure protocols, standards, and procedures within the VC
domain. The Virtual Connect FIPS certification is currently based on the standards described in Federal Information Processing Standards Publication 140-2 (http://csrc.nist.gov/publications/PubsFIPS.html).

The term FIPS mode is used throughout this document to describe the feature, not the validation status. For information about current FIPS status of this or any other firmware version, see the following documents:

- FIPS 140-1 and FIPS 140-2 Vendor List (http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401vend.htm)

FIPS mode information and guidelines

Before enabling FIPS mode, observe the following information:

- The OA should be enabled with FIPS mode before VCM. If FIPS mode cannot be set on the OA, perform the following procedures before enabling FIPS mode on VCM:
  - If it exists, delete the VC domain.
  - Clear the VC mode from the OA.
  - A partial VC domain state is created when VCM discovers the local OA in VC mode. Be sure to clear the partial VC domain state by powering off and then powering on the primary VC Enet module.
- When entering or exiting FIPS mode, the VC domain is deleted.
- The firmware must be updated to version 4.30 or higher before FIPS mode can be enabled.
- A rollback or downgrade of firmware is not supported once the domain is in FIPS mode.
- Incompatible Fibre Channel modules display a status of incompatible.
- The HPE VC 16Gb 24-Port FC Module is the only VC FC module compatible with FIPS mode. All other VC FC modules are incompatible.

**IMPORTANT:** Once FIPS mode is enabled for the domain and VCM configures the VC 16Gb 24-Port FC module, the module is permanently enabled with FIPS mode. The FC module will continue to operate in a non-FIPS domain after a FIPS configuration occurs, but SNMPv3 traps and informs with AUTHPRIV security levels will remain permanently configured on the module.

- Ethernet and FlexFabric modules must be physically enabled with FIPS mode.
- When the FIPS mode of a VC-Enet module does not match the FIPS mode of the domain, the module displays a status of incompatible.
- VC domain configuration files created in a FIPS-enabled domain cannot be used in a non-FIPS domain.
- VC domain configuration files created in a non-FIPS domain cannot be used in a FIPS-enabled domain.
- VC domain configuration files from previous versions cannot be restored to current, active versions.
- VC domain configuration files are deleted when FIPS mode is enabled or disabled.

FIPS mode protocol and feature restrictions

When FIPS mode is enabled, security is increased across the domain. The following protocols and features are restricted:
• FTP and TFTP
• TACACS+ authentication
• RADIUS authentication
• Automated deployment
• Configurable user roles
• Administrator password recovery
• USB firmware updates
• SNMPv1 and SNMPv2
• MD5 authentication and DES encryption for SNMPv3
• Remote logging, except when using stunnel for encryption
• Short passwords
• Weak passwords

Observe the following requirements:
• By default, the password strength is set to strong.
• The minimum password length must be 8 or more characters.
  VCM uses SCP and SFTP protocols instead of FTP and TFTP.
• SSH sessions require the SHA-256 algorithm for key exchanges.
• TLS 1.2 is the default communication security protocol for a FIPS enabled domain. Verify the following components support TLS 1.2:
  o The OA version
    OA firmware versions prior to 4.10 do not support TLS 1.2.
  o The LDAP server
  o The terminal emulator you use for SSH
  o The browser you use to access the VCM web interface
If a component does not support TLS 1.2, configure VCM to support all TLS versions in the Web SSL Configuration screen.
To verify browser settings, see "Configuring browser support ("Browser requirements and configuration" on page 57)."

Enabling FIPS mode

Enable FIPS mode by configuring the DIP switches on the primary VC-Enet or FlexFabric module:

1. Verify the module firmware version ("FIPS mode information and guidelines" on page 33).
   Hewlett Packard Enterprise recommends upgrading to the latest firmware version.
   △ CAUTION: Before upgrading the firmware, be sure no plans exist to downgrade or rollback firmware. Once the domain is in FIPS mode, the firmware cannot be downgraded.

2. Remove the module from the interconnect bay.
3. Remove the access panel, and then locate the DIP switches ("Component identification" on page 101).
   DIP switches on the HPE VC FlexFabric-20/40 F8 module are accessible without removing the access panel.
4. Locate DIP switch 3, and then set to the ON position. Be sure that all other switches remain in the OFF position.

OFF OFF ON OFF

5. Install the access panel.

6. Install the module.

Allow the module to power up and reach an operational state (approximately 1 minute).

7. Log in to VC Manager and then verify the domain and the module indicate FIPS mode is enabled ("FIPS mode indicators (domain)" on page 35).

FIPS mode indicators (domain)

VCM indicates if the domain is in FIPS mode by displaying the following icon in the banner.

The VCM CLI prompt indicates if the domain is in FIPS mode by displaying the following prompt:

FIPS->

FIPS mode indicators (VC Ethernet modules)

If a module is not enabled with FIPS mode, it is displayed as incompatible. To identify an incompatible module, use the Interconnect Bays screen.

Installing a VC-Enet module

VC-Enet modules can be installed in a c7000 or c3000 enclosure. The following procedure shows a VC-Enet module being installed in a c7000 enclosure.
To install the component:

1. Remove the interconnect blank.

**NOTE:** HPE Virtual Connect works optimally in enclosures configured with HPE Virtual Connect interconnect modules only.

2. Prepare the VC-Enet module. An HPE VC Flex-10 10Gb Ethernet Module is shown.
3. Install the module into the interconnect bay.

4. Install stacking cables, if required.
   For more information, see "Stacking links (on page 21)."

5. Use any available port to connect to the data center network.
   This step can also be performed after configuring Virtual Connect Manager. For more information, see "Default module configuration (on page 11)."
   Be sure to use supported SFP+ transceiver modules.

6. Remove the perforated portion of the Default Network Setting label that extends beyond the faceplate of the primary module, or record the information from the label.
   The Default Network Settings label contains the DNS name, user name, and password of the primary interconnect module. This information is required to access VCM.

7. Connect a workstation to the data center network hosting the HPE BladeSystem Onboard Administrator for the enclosure.

8. Start and log on to the workstation.

9. Open a web browser.

10. Log on to the HPE BladeSystem Onboard Administrator.
    If prompted, follow the steps in the OA First Time Setup Wizard. For specific instructions, see the HPE BladeSystem Onboard Administrator User Guide on the Hewlett Packard Enterprise website (http://www.hpe.com/info/oa).

11. Before accessing VCM, verify that the HPE BladeSystem Onboard Administrator firmware is at the recommended firmware version. For specific instructions, see the Hewlett Packard Enterprise website (http://www.hpe.com/info/oa).

12. Review the Onboard Administrator bay summary screens to verify that each server blade iLO and interconnect module has been assigned an IP address. Each IP address must be valid and unique, and all iLOs and VC modules must be on the same subnet.
    For more information, see the HPE BladeSystem Onboard Administrator User Guide on the Hewlett Packard Enterprise website (http://www.hpe.com/info/oa).

   IMPORTANT: For proper Virtual Connect operation, always assign an IP address to each server blade iLO and interconnect module.
13. From the enclosure overview screen, click the **Virtual Connect Manager** link. The VCM logon screen appears.

14. Enter the user name and password from the Default Network Settings label, and then click **Sign In**. The HPE Virtual Connect Manager Setup Wizard screen appears ("Virtual Connect Domain Setup Wizard" on page 61).

15. Use VCM to administer the module.

After an enclosure is imported into a Virtual Connect domain, server blades that have not been assigned a server profile are isolated from all networks to ensure that only properly configured servers are attached to data center networks.

A pre-deployment server profile can be defined within VCM for each device bay so that the server blade can be powered on and connected to a deployment network. These profiles can then be modified at a later time or replaced by another server profile.

To configure server profiles, see the *HPE Virtual Connect for c-Class BladeSystem User Guide* on the Hewlett Packard Enterprise website ([http://www.hpe.com/info/vc/manuals](http://www.hpe.com/info/vc/manuals)).

### Installing a VC FlexFabric module

For individual FlexFabric module installation requirements, see "Installation requirements (on page 13)."

To install the component:

1. Remove the interconnect blank.

**NOTE:** HPE Virtual Connect works optimally in enclosures configured with HPE Virtual Connect interconnect modules only.
2. Prepare the FlexFabric module. An HPE Virtual Connect FlexFabric 10/24-port Module is shown.

3. Install the FlexFabric module into the interconnect bay.

4. Install stacking cables, if required.
   The FlexFabric module supports stacking links for Ethernet traffic only. For more information, see "Stacking links (on page 21)."

5. Use any available port to connect to the data center network.
   o If the FlexFabric module is being configured for Ethernet traffic, connect an Ethernet port to the data center network. Be sure the transceiver module is supported and compatible with the data center port type.
   o If the FlexFabric module is being configured for Fibre Channel traffic, connect the data center SAN switch ports to ports X1 through X4 of the module, or ports X1 through X8 on HPE Virtual Connect FlexFabric-20/40 F8 Modules.

   ☑️ IMPORTANT: For proper thermal operation, always install dust covers in QSFP+, SFP+, or SFP ports without transceivers installed.
6. Remove the perforated portion of the Default Network Settings label that extends beyond the faceplate of one of the VC-Enet module or FlexFabric module installed in the enclosure. The Default Network Settings label contains the DNS name, user name, and password of the interconnect module. This information is required to access VCM.

7. Connect a workstation to the data center network hosting the HPE BladeSystem Onboard Administrator for the enclosure.

8. Start and log on to the workstation.

9. Open a web browser.

10. Log on to the HPE BladeSystem Onboard Administrator. If prompted, follow the steps in the OA First Time Setup Wizard. For specific instructions, see the [HPE BladeSystem Onboard Administrator User Guide](http://www.hpe.com/info/oa) on the Hewlett Packard Enterprise website.

11. Before accessing VCM, verify that the HPE BladeSystem Onboard Administrator firmware is at the recommended firmware version. For specific instructions, see the Hewlett Packard Enterprise website ([http://www.hpe.com/info/oa](http://www.hpe.com/info/oa)).

12. Verify that each server blade iLO and interconnect module has been assigned an IP address by reviewing the bay summary screens in the Onboard Administrator. Each IP address must be valid and unique, and all iLOs and Virtual Connect modules must be on the same subnet. For more information, see the [HPE BladeSystem Onboard Administrator User Guide](http://www.hpe.com/info/oa) on the Hewlett Packard Enterprise website.

   **IMPORTANT:** For proper Virtual Connect operation, always assign an IP address to each server blade iLO and interconnect module.

13. From the enclosure overview screen, click the Virtual Connect Manager link. The VCM logon screen appears.

14. In the Username field, enter Administrator.

15. Enter the password from the Default Network Settings label into the Password field.

The HPE Virtual Connect Manager Setup Wizard screen appears.

16. Use VCM to administer the Virtual Connect Ethernet module for the enclosure. For more information, see the [HPE Virtual Connect for c-Class BladeSystem User Guide](http://www.hpe.com/info/vc/manuals) on the Hewlett Packard Enterprise website.
Installing a VC-FC module

1. Remove the interconnect blank, if needed.

2. Prepare the module for installation.

3. Install the module.

4. Install transceivers, and then connect the module to the SAN switch.
IMPORTANT: For proper thermal operation, always install SFP dust covers in SFP ports without SFP transceivers installed.

5. Log in to VCM, and then review the bay summary screen to verify that the module is available to configure.

6. Configure the module:
   - If VC-Enet or FlexFabric modules are installed in the same enclosure, use VCM to administer VC-FC modules.
   - If VC-Enet or FlexFabric modules are not installed in the same enclosure, the VC-FC module operates in the default configuration only.

Installing DAC/AOC cables and transceivers

To install a DAC/AOC cable or a QSFP+, SFP+, or SFP transceiver, use the following procedures:

- Installing a cable (on page 41)
- Installing a transceiver (on page 42)

Installing a cable

1. If needed, remove the packaging and protective caps.
2. Verify the cable is the correct type by checking the label on the transceiver.
3. Remove the dust plug from the correct port.
4. Align the transceiver in front of the port with the label facing up.
5. Install the cable. (QSFP+ DAC cable shown)

Installing a transceiver

⚠️ WARNING: To avoid serious injury, never look directly into an open transceiver port.
**CAUTION:** Disconnect all cables before removing or installing any transceivers or transceiver adapters. Leaving the cable connected while handling the transceiver may damage the cable, the cable connector, or the optical interfaces in the transceiver. Do not remove and install transceivers more often than is necessary. Doing so can shorten the useful life of the transceiver.

**CAUTION:** Do not remove the dust plugs from the transceiver or the connector until you are ready to connect the cable. The plugs protect the ports and connectors from contamination and ambient light.

**NOTE:** Transceivers may have a bail clasp or a pull tab. If installing a transceiver with a bail clasp, then be sure the clasp is closed before connecting the cable. If installing a transceiver with a pull tab, note that the pull tab may be located above or below the cable and vary in size or shape.

To install a transceiver or transceiver adapter:

**IMPORTANT:** Use only Hewlett Packard Enterprise approved transceivers.

1. Verify the transceiver type by checking the label on the transceiver.
2. Remove the dust plug from the correct port of the device or module.
3. Align the transceiver in front of the port with the label facing up.
4. Install the transceiver:
   - Transceiver with a bail clasp
Removing QSFP+, SFP+ or SFP transceivers

⚠️ **WARNING:** To avoid serious injury, never look directly into an open transceiver port.

⚠️ **CAUTION:** Disconnect all cables before removing or installing a QSFP+, SFP+ or SFP transceiver, because of the potential damage to the cables, the cable connector, or the optical interfaces in the transceiver. Do not remove and install transceivers more often than is necessary. Doing so can shorten the useful life of the transceiver.

1. Disconnect all cables.
2. Open the latch.
3. Remove the transceiver. (SFP transceiver shown).

4. Install dust plugs on the fiber-optic transceiver and rubber plugs on the fiber-optic cable.

⚠️ **CAUTION:** Be sure to install the dust plugs on the fiber-optic transceiver and the rubber plugs on the fiber-optic cable. The plugs and caps protect the transceiver ports and cables from contamination and ambient light.

### Factory default settings

The Virtual Connect Delete Domain operation returns all VC-FC modules to the factory default settings. VC-FC modules that are physically removed from a VC domain can be returned to the factory default settings when placed into a new enclosure by applying power, and then pressing and holding the reset button on the front panel for at least 10 seconds. When moved from a VC domain and placed into an enclosure not part of a VC domain, VC-FC modules retain assigned mappings until reset to the factory default.

### Connecting Virtual Connect Ethernet module uplinks

Each interconnect module has several numbered Ethernet connectors. All of these connectors can be used to connect to data center switches (uplink ports), or they can be used to stack Virtual Connect modules as part of a single Virtual Connect domain (stacking ports). See "Recommended stacking connections (on page 22)."

Networks must be defined within VCM so that specific named networks can be associated with specific external data center connections. These named networks can then be used to specify networking connectivity for individual servers. The network connection can be between one or many networks to one or many uplink ports:

- One network to one port (unshared network)
- One network to multiple uplink ports (unshared network)
- Multiple networks to one port (shared uplink set)
- Multiple networks to multiple ports (shared uplink set)

In addition, multiple networks can be connected to server downlink ports using server VLAN IDs. For more information, see "Managing server profiles" in the user guide.
The following sections provide an overview of the types of external connections and their behaviors.

**Mapping individual networks to individual external uplink ports**

The simplest approach to connecting the defined networks to the data center is to map each network to a specific external uplink port. This uplink port is defined by the following:

- Enclosure name
- Interconnect bay containing the VC-Enet module
- Selected port on that module

Port status indicators can be used to locate a specific port or to provide additional status.

The following table shows an example of simple network mapping, where the Virtual Connect enclosure is named Enclosure1 and VC-Enet modules are in interconnect module bays 1 and 2.

<table>
<thead>
<tr>
<th>Network</th>
<th>Uplink port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Production_Network</td>
<td>Enclosure1:Bay1:PortX2</td>
</tr>
<tr>
<td>Dev_Network</td>
<td>Enclosure1:Bay1:Port4</td>
</tr>
<tr>
<td>Backup_Network</td>
<td>Enclosure1:Bay2:Port3</td>
</tr>
<tr>
<td>iSCSI_Storage_Network</td>
<td>Enclosure1:Bay2:PortX2</td>
</tr>
</tbody>
</table>

In this case, the Ethernet packets are passed unchanged between the server blades and the external networks. Any VLAN tags added by the server or external switch are ignored and pass through the VC-Enet modules.

The previous figure also shows a local connection between Server Blade 2 and Server Blade 16, which might be used in a cluster or as a network heartbeat.

**Mapping a single network to multiple uplinks (uplink port set)**

A single network can be mapped to more than one external uplink port to provide improved throughput and availability, referred to as an uplink port set. Review the following guidelines before mapping a single network to an uplink port set:

- External uplink ports within an uplink port set can be on the same VC-Enet module or on multiple VC-Enet modules within the Virtual Connect domain.
- Cables can be connected to one or more data center Ethernet switches.
- When multiple external uplink ports are used for the same network, the VC-Enet modules provide automatic loop prevention by enabling for a single active link or link set at any one time.
• VC automatically chooses the uplink port that optimizes throughput and availability. Where possible, links within the uplink port set automatically form a link aggregation group with LACP. This action requires multiple uplink ports on a single VC-Enet module to be connected to an external switch that is capable and configured to form link aggregation groups with LACP.

In the following example, a single network is mapped to four external uplink ports.

<table>
<thead>
<tr>
<th>Network</th>
<th>Uplink port set</th>
</tr>
</thead>
<tbody>
<tr>
<td>Production_Network</td>
<td>{ Enclosure1:Bay1:Port1, Enclosure1:Bay1:Port2, Enclosure1:Bay2:Port1, Enclosure1:Bay2:Port2 }</td>
</tr>
</tbody>
</table>

In this example, the ports from Bay 1 could be connected to one external switch, and the ports on Bay 2 could be connected to a second switch. If the external switches support link aggregation, then this configuration would provide an active 2-Gb link to one switch and a standby 2-Gb link to the other.

To make VCM aware of individual network connections, see "Define Ethernet Network screen" in the user guide.

**Mapping multiple networks to a single port in a shared uplink set**

The network administrator can choose to reduce the number of cables between the Virtual Connect enclosure and the data center switches by mapping multiple networks to a single, shared uplink port. In this case, a network is not just mapped to an uplink port, but to a VLAN on that port. This configuration requires VLAN tags to be added to each packet as it leaves the Virtual Connect domain and that packets entering the Virtual Connect domain be tagged. The VLAN tag is stripped from packets entering the Virtual Connect domain before they are routed to the appropriate server.

In the following example, an uplink port is defined as a shared uplink port so that it can then be used as the external connection for multiple networks.

**Shared_Uplink_Port_A = Enclosure1:Bay1:PortX2**

<table>
<thead>
<tr>
<th>Network</th>
<th>Shared uplink port and VLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Production_Network</td>
<td>Shared_Uplink_Port_A:VLAN_15</td>
</tr>
<tr>
<td>Dev_Network</td>
<td>Shared_Uplink_Port_A:VLAN_21</td>
</tr>
<tr>
<td>Backup_Network</td>
<td>Shared_Uplink_Port_A:VLAN_32</td>
</tr>
<tr>
<td>iSCSI_Storage_Network</td>
<td>Shared_Uplink_Port_A:VLAN_76</td>
</tr>
</tbody>
</table>
Because appropriate VLAN tags are added as the packets leave the enclosure, this type of uplink should not be used in cases where VLAN tags are already added on the server itself. The system drops any Ethernet packets with server-inserted VLAN tags that are received on networks connected to shared uplink ports.

To make VCM aware of shared network connections, see "Define Shared Uplink Set screen" in the user guide.

**Mapping multiple networks to a shared uplink set**

It is also possible to map multiple VLAN-tagged networks to a set of shared uplink ports. The resulting shared uplink set allows for the minimum number of cables while still providing for link aggregation and failover.

In the following example, a shared uplink set is first defined to provide aggregation and failover.

```plaintext
Shared_Uplink_Set_A = {Enclosure1:Bay1:PortX2, Enclosure1:Bay2:PortX2}
```

<table>
<thead>
<tr>
<th>Network</th>
<th>Shared uplink set and VLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Production_Network</td>
<td>Shared_Uplink_Set_A:VLAN_15</td>
</tr>
<tr>
<td>Dev_Network</td>
<td>Shared_Uplink_Set_A:VLAN_21</td>
</tr>
<tr>
<td>Backup_Network</td>
<td>Shared_Uplink_Set_A:VLAN_32</td>
</tr>
<tr>
<td>iSCSI_Storage_Network</td>
<td>Shared_Uplink_Set_A:VLAN_76</td>
</tr>
</tbody>
</table>

In this example, all of the defined networks share a single active uplink port (such as Enclosure1:Bay1:PortX2) using VLAN tagging, while the second link in the shared uplink set is available for failover. The shared uplink set can also be constructed from multiple 1-Gb external ports.

To make VCM aware of shared network connections, see "Define Shared Uplink Set screen" in the user guide.

**Mapping FCoE networks to a shared uplink set**

When mapping FCoE networks to a shared uplink set, the shared uplink set uplink port must be connected to a supported FCoE switch that is capable of splitting the converged Enet and FCoE traffic out into native FC or Enet, as it applies.

**Configuration example using a Cisco Core switch**

There are several ways to implement a redundant Virtual Connect configuration. This example provides a reference for anyone unfamiliar with switch configurations. This example is just one of several ways to connect an HPE Virtual Connect to a Cisco Core switch. For more information, see *HPE Virtual Connect for the Cisco Network Administrator* on the Functionality & Value tab of the Hewlett Packard Enterprise BladeSystem Technical Resources website ([http://www.hpe.com/info/bladesystem/docs](http://www.hpe.com/info/bladesystem/docs)).

**Connecting Virtual Connect to a Cisco Core/distribution switch using a shared uplink set and VLAN tagging done at the VC/data center boundary**
In the following example, LACP is used on the Cisco Switch to connect to a shared uplink set using three uplink ports. VLANs 10, 20, 30, and 40 from the network are tagged on the three shared uplink ports.

**IMPORTANT:** Change Channel Mode to LACP on the Cisco switch.

By default, all ports on a Catalyst 4500/4000 switch and a Catalyst 6500/6000 switch use channel protocol PAgP and are not running LACP. For all ports concerned, you must change the channel mode to LACP.

On switches running CatOS, you can only change channel mode per module. In the following example, change the channel mode for slots 1 and 2 by using the following command:

```
set channelprotocol lacp module_number
```

Verify the changes by using the following command:

```
show channelprotocol.
```

```
CatOSSwitch (enable) set channelprotocol lacp 1
Mod 1 is set to LACP protocol.
CatOSSwitch (enable) set channelprotocol lacp 2
Mod 2 is set to LACP protocol.
CatOSSwitch (enable) show channelprotocol
  Channel
  Module  Protocol
    ------  --------
    1       LACP
    2       LACP
    3       PAGP
    5       PAGP
```

On switches running Cisco IOS Software, specify which interfaces should be using LACP by entering the following interface configuration command:

```
channel-protocol lacp:
```

```
CiscoIOSSwitch(config-if)#channel-protocol lacp
```

Example switch configuration of a Cat 6500 switch using IOS. Ports 7/46, 7/47, and 7/48 on the Cat 6500 switch are used to uplink to the Virtual Connect module:

```
interface Port-channel10
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 10,20,30,40
```
switchport mode trunk
no ip address

interface GigabitEthernet7/46
description test-VC
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 10,20,30,40
switchport mode trunk
no ip address
speed 1000
channel-protocol lacp
channel-group 10 mode active
!

interface GigabitEthernet7/47
description test-VC
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 10,20,30,40
switchport mode trunk
no ip address
speed 1000
channel-protocol lacp
channel-group 10 mode active
!

interface GigabitEthernet7/48
description test-VC
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 10,20,30,40
switchport mode trunk
no ip address
speed 1000
channel-protocol lacp
channel-group 10 mode active

Failover and check-pointing

VCM runs as a high-availability pair when VC-Enet modules are installed in horizontally adjacent interconnect bays. The active VCM is usually on the lowest odd numbered bay when the enclosure is powered up.

Each time a configuration is changed, it is written to local flash memory and then check-pointed to the standby module. Configurations can also be backed up to a workstation using the GUI or Virtual Connect Support Utility.

NOTE: Hewlett Packard Enterprise recommends saving a configuration after each session and before updating firmware.

Interconnect module upgrades

Virtual Connect modules

It is not necessary to remove the module from the domain if the module is not in use. The module is removed automatically from the domain without user intervention.
Replacing a primary or backup VC module with a different VC module type is not allowed without first deleting the domain.

If a module is in use and configured by the domain at the time it is physically removed from an enclosure, then the module is marked as MISSING, and can only be replaced by a module of the same model and type. If an in-use module is replaced by a module of a different type, then it is marked as INCOMPATIBLE by the domain.

If a module being physically removed is the primary module of a primary bay pair, then it is marked as MISSING and can only be replaced by a module of the same type.

A VC-Enet module is in use if any of the following conditions exist:

- The module physically exists in an interconnect bay using VC release prior to 3.00.
- The uplink and downlink ports of the module are being used by one or more networks, uplink sets, or profiles.
- Port monitoring is enabled for the interconnect module.

A VC-FC capable module is in use if any of the following conditions exist:

- The module physically exists in an interconnect bay using VC release prior to 3.00.
- The uplink ports of the module are being used by a fabric that is being used by a profile.
- The module is part of a FC bay group in a multi-enclosure configuration where other FC modules exist in the bay group.

If a VC-FC module is replaced with a spare VC-FC module without powering down the servers, and if the server has profiles assigned to it with FC connections, servers are allowed to log in for a brief period through an uplink of the new module, provided that the uplink is connected to the fabric. Approximately 8 seconds after discovering the new VC-FC module, VCM configures it with the correct information, mapping downlinks to the correct uplinks. To work around this problem, power down the servers in the enclosure before replacing or swapping FC modules. Alternatively, do not connect the VC-FC uplinks to the fabric until VCM recognizes and configures the VC-FC module.

When adding VC interconnect modules to a VC managed enclosure, wait until the modules have been fully integrated into the current domain before attempting to make configuration changes to the VC domain. These changes include adding or editing networks, fabrics, profiles, and shared uplink sets. Verify that the domain status is clear for the newly added interconnect module before making any changes to the configuration. Modifying the configuration before the integration is complete can cause unexpected behavior such as incorrect/invalid connections in a profile.

### Upgrading to an HPE Virtual Connect 16Gb 24-Port FC Module

This procedure replaces the following modules with an HPE VC 16Gb 24-Port FC Module:

- HPE 4Gb VC-FC Module
- HPE VC 4Gb FC Module
- HPE 8Gb 20-Port FC Module
- HPE 8Gb 24-Port FC Module

To upgrade to an HPE VC 16Gb 24-Port FC Module:

1. Upgrade the VC domain firmware to the latest supported version. See "VC module supported firmware (on page 9)."
2. Verify that the replacement will result in a good configuration. See "Multiple enclosure requirements (on page 29)."
3. Verify that the user has server and storage role permissions.
4. Remove any FC profile connections that are connected to the interconnect bays being upgraded. To remove the profile connections, un-assign the profile, and then delete the connections from the profile.

5. If any FC SAN fabrics were created using uplinks from the interconnect bays that are being upgraded, delete these FC SAN fabrics from the Virtual Connect domain.

6. Physically remove the existing modules from BOTH horizontally adjacent bays for each enclosure in the domain. In a double-dense domain, remove the modules from Bay 7 and Bay 8 when removing modules in Bay 5 and Bay 6.

7. Ensure that the VC-FC modules are no longer shown in the domain.

8. Install the HPE VC 16Gb 24-Port FC Modules.

9. Re-create the previously deleted FC SAN fabrics.

10. Re-assign the server profiles, and then add the FC connections to the profiles.

### Upgrading to an HPE Virtual Connect 8Gb 24-Port FC Module

This procedure replaces the following modules with an HPE VC 8Gb 24-Port FC Module:

- HPE 4Gb VC-FC Module
- HPE VC 4Gb FC Module
- HPE 8Gb 20-Port FC Module
- HPE VC 16Gb 24-Port FC Module

To upgrade to an HPE VC 8Gb 24-Port FC Module:

1. Upgrade the VC domain firmware to the latest supported version. See "VC module supported firmware (on page 9)."

2. Verify that the replacement will result in a good configuration. See "Multiple enclosure requirements (on page 29)."

3. Verify that the user has server and storage role permissions.

4. Remove any FC profile connections that are connected to the interconnect bays being upgraded. To remove the profile connections, un-assign the profile, and then delete the connections from the profile.

5. If any FC SAN fabrics were created using uplinks from the interconnect bays that are being upgraded, delete these FC SAN fabrics from the Virtual Connect domain.

6. Physically remove the existing modules from BOTH horizontally adjacent bays for each enclosure in the domain. In a double-dense domain, remove the modules from Bay 7 and Bay 8 when removing modules in Bay 5 and Bay 6.

7. Ensure that the VC-FC modules are no longer shown in the domain.

8. Install the HPE VC 8Gb 24-Port FC Modules.

9. Re-create previously deleted FC SAN fabrics.

10. Re-assign the server profiles, and then add the FC connections to the profiles.

### Upgrading to an HPE Virtual Connect 8Gb 20-Port FC Module

To replace an HPE 4Gb VC-FC Module or HPE VC 4Gb FC Module with an HPE VC 8Gb 20-Port FC Module:

1. Upgrade the VC domain firmware to the latest supported version. See "VC module supported firmware (on page 9)."

2. Physically remove the existing module.

3. Install the HPE VC 8Gb 20-port FC Module.
The installation is complete.

To replace an HPE 8Gb or 16Gb 24-Port FC Module with an HPE VC 8Gb 20-Port FC Module:

1. Upgrade the VC domain firmware to the latest supported version. See "VC module supported firmware (on page 9)."
2. Verify that the replacement will result in a good configuration. See "Multiple enclosure requirements (on page 29)."
3. Verify that the user has server and storage role permissions.
4. Remove any FC profile connections that are connected to the interconnect bays being upgraded. To remove a profile connection, un-assign the profile, and then delete the connections from the profile.
5. If any FC SAN fabrics were created using uplinks from the interconnect bays that are being upgraded, delete these FC SAN fabrics from the Virtual Connect domain.
6. Physically remove the existing modules from BOTH horizontally adjacent bays for each enclosure in the domain. In a double-dense domain, remove the modules from Bay 7 and Bay 8 when removing modules in Bay 5 and Bay 6.
7. Ensure that the VC-FC modules are no longer shown in the domain.
8. Install the HPE VC 8Gb 20-port FC Modules.
9. Re-create previously deleted FC SAN fabrics.
10. Re-assign the server profiles, and then add the FC connections to the profiles.

The installation is complete.

If the module displays an UNKNOWN or INCOMPATIBLE state, physically remove the module, and then insert the correct module type.

If the server is not connecting properly to the network, restart the server.

Upgrading or removing an HPE Virtual Connect Flex-10, HPE Virtual Connect FlexFabric, or HPE Virtual Connect Flex-10/10D module

Upgrading an enclosure to Flex-10 or FlexFabric support or removing Flex-10 support requires several steps, depending on the starting configuration.

- For more information on individual module requirements, see "Installation requirements (on page 13)."
- For detailed migration information, see the HPE Virtual Connection Migration Guide technical white paper on the Hewlett Packard Enterprise website (http://www.hpe.com/info/VC-Migration).

Replacing a Virtual Connect Ethernet module with an HPE Virtual Connect Flex-10, HPE FlexFabric, or HPE Flex-10/10D module in a horizontally adjacent bay pair hosting VC Manager (the horizontal bays housing primary and/or backup modules)

⚠️ CAUTION: Replacing the primary/backup bay pair modules with modules of a different type requires the creation of a new VC domain, creating the probability that VC managed identifiers (MAC, WWN, and serial numbers) could be assigned to different server ports or slots from the original VC domain. The HPE Virtual Connection Migration Guide technical white paper on the Hewlett Packard Enterprise website (http://www.hpe.com/info/VC-Migration) details a procedure for upgrading to newer Virtual Connect modules while maintaining the same VC-managed identifiers.

1. Upgrade the VC domain firmware to the latest supported version. See "VC module supported firmware (on page 9)."
2. Delete the domain.
3. Remove all network uplinks from the modules to be removed.
4. Remove the existing modules from both horizontally adjacent bays.
5. Install the HPE Virtual Connect Flex-10, FlexFabric, or Flex-10/10D modules.
6. Import one or more enclosures and create a new VC domain. If available, a user-created CLI script file can accelerate VC domain recreation. However, be sure to verify the settings because VC-managed identifiers, such as MAC, WWN, and serial numbers, might not match the original VC domain settings.

Replacing a Virtual Connect Ethernet module with an HPE Virtual Connect Flex-10, HPE FlexFabric, or HPE Flex-10/10D module in a horizontally adjacent bay pair not hosting VC Manager

1. Upgrade the VC domain firmware to the latest supported version. See "VC module supported firmware (on page 9)".
2. Save the configuration.
3. If any Flex-10 NICs with profile connections are connected to the interconnect bays being upgraded, the profile connections must be removed. To remove a profile connection, unassign the profile (recommended) or delete the connection from the profile.
4. Remove all network uplinks from the modules to be removed.
5. Remove the existing modules from both horizontally adjacent bays.
6. Ensure that the modules are removed from the Virtual Connect GUI. If the modules still appear on the GUI, there are still profiles with connections to the modules or networks with uplinks on the modules. Do not proceed until the modules are removed.
7. Install the HPE Virtual Connect Flex-10, FlexFabric, or Flex-10/10D modules.
8. Reassign the server profiles or add the connections to the profiles, depending on what was done in step 3.

Replacing an HPE Virtual Connect Flex-10, HPE FlexFabric, or HPE Flex-10/10D module with a Virtual Connect Ethernet module in a horizontally adjacent bay pair hosting VC Manager (the horizontal bays housing primary and/or backup modules)

⚠️ CAUTION: Replacing the primary/backup bay pair modules with modules of a different type requires the creation of a new VC domain, creating the probability that VC managed identifiers (MAC, WWN, and serial numbers) could be assigned to different server ports or slots from the original VC domain.

The HPE Virtual Connection Migration Guide technical white paper on the Hewlett Packard Enterprise website (http://www.hpe.com/info/VC-Migration) details a procedure for upgrading to newer Virtual Connect modules while maintaining the same VC-managed identifiers.

1. Delete the domain.
2. Remove all network uplinks from the modules to be removed.
3. Remove the existing Flex-10, FlexFabric, or Flex-10/10D modules from both horizontally adjacent bays.
4. Install the Virtual Connect Ethernet modules.
5. Import one or more enclosures and create a new VC domain. If available, a user-created CLI script file may accelerate VC domain recreation. However, be sure to verify the settings because VC-managed identifiers, such as MAC, WWN, and Serial Numbers, might not match the original VC domain settings.

Replacing an HPE Virtual Connect Flex-10, HPE FlexFabric, or HPE Flex-10/10D module with a Virtual Connect Ethernet module in a horizontally adjacent bay pair not hosting VC Manager

1. If any Flex-10 NICs with profile connections are connected to the interconnect bays being upgraded, then the profile connections must be removed. To remove a profile connection, unassign the profile (recommended) or delete the connection from the profile.
2. Remove all network uplinks from the modules to be removed.
3. Remove the existing Flex-10, FlexFabric, or Flex-10/10D modules from both horizontally adjacent bays.
4. Ensure that the modules are removed from the Virtual Connect GUI. If the modules still appear on the GUI, there are still profiles with connections to the modules or networks with uplinks on the modules. Do not proceed until the modules are removed.
5. Install the Virtual Connect Ethernet modules.
6. Reassign the server profiles or add the connections to the profiles, depending on what was done in step 1.

Possible errors
If the previous steps are not followed exactly, the newly inserted module might be set to the UNKNOWN or INCOMPATIBLE state, depending on how the error state was reached. To correct this error:
1. Physically remove the module.
2. Insert the original module.
3. Ensure that all profiles have been unassigned.
4. Remove the module.
5. Verify that the module is removed from the GUI.
6. Insert the correct module type.

If the previous steps have been followed and the server is not connecting properly to the network, power down the server, and then power it back up.

Upgrading to an HPE Virtual Connect FlexFabric module from a VC-FC module

Replacing any VC-FC module with an HPE VC FlexFabric module:
1. Upgrade the VC domain firmware to the latest supported version. See "VC module supported firmware (on page 9)."
2. Verify that the replacement will result in a good configuration. See "Multiple enclosure requirements (on page 29)."
3. Verify that the user has server and storage role permissions.
4. Remove any FC profile connections that are connected to the interconnect bays being upgraded by deleting the connections from the profile.
5. If any FC SAN fabrics were created using uplinks from the interconnect bays being upgraded, delete these FC SAN fabrics from the Virtual Connect domain.
6. Physically remove the existing modules from both horizontally adjacent bays.
7. Ensure that the VC-FC modules are no longer shown in the domain.
8. Replace the server blade FC HBA mezzanine cards with FlexFabric Adapter mezzanine cards.
9. Install the HPE VC FlexFabric Modules with the appropriate FC SFP+ transceivers.
10. Recreate the previously deleted FC SAN fabrics.
11. Add FCoE connections to the profiles.
12. Power up the server and install the appropriate drivers for the FlexFabric Adapter mezzanine card.

Onboard Administrator modules
Replacing the OA in an enclosure containing only one OA causes the OA to leave VC mode. This mode change requires VC Manager to re-establish credentials with the OA. During this process, VC Manager rewrites all server settings and sets the state of the servers to “profile recovered.” There should not be any
disruption to the servers, but the administrator should be sure that all servers have the correct MAC addresses and WWNs. Powering off the server clears the "profile recovered" state. If any servers are rebooted or power-cycled while the credential recovery occurs, the MAC addresses and WWNs might be returned to the factory default settings.
Browser requirements and configuration

Access to the VCM GUI is provided through HTTPS (HTTP exchanged over an SSL-encrypted session) and requires HTTPS (port 443) to be enabled on the management network.

The minimum supported screen resolution is 1024 x 768 with 256 colors. For optimal viewing, Hewlett Packard Enterprise recommends setting the screen resolution to 1280 x 1024.

Requirements

The VCM web interface requires an XSLT-enabled browser with support for JavaScript 1.3 or the equivalent.

The following browsers are supported:

- Microsoft Internet Explorer 10.x and 11.x
- Mozilla Firefox 39.0.3 and 42

Browsers that provide the required functionality but do not appear in the previous list are not prevented from running the application, but no support is offered for unlisted browsers.

If you receive a notice that your browser does not have the required functionality, examine your browser settings to ensure they meet the following requirements or contact your administrator:

- The use of third-party browser download managers is not supported or recommended when using Virtual Connect. Using third-party download managers might cause some VC file download functionality to work incorrectly, for example, when saving the domain configuration, downloading a support information file, and so on.

- The following browser settings must be enabled before running the application:
  - **JavaScript**
    Client-side JavaScript is used extensively by this application. Check the browser settings to make sure JavaScript is enabled before running the application.
  - **ActiveX**
    When using Microsoft Internet Explorer with this application, ActiveX must be enabled. Check the browser settings to make sure ActiveX is enabled before running the application.
  - **Adobe Flash Player**
    Virtual Connect Manager requires Adobe Flash Player 11.1 or higher before you can log in. Hewlett Packard Enterprise recommends updating to Adobe Flash Player 13 or higher for Windows and 11.2 for Linux systems.
    To allow Adobe Flash Player to function properly in Windows Server 2012, be sure to enable the "Desktop Experience" feature in the Add Roles and Features Wizard.

Pop-up windows

Pop-up windows must be enabled for certain features to function correctly. Check the browser settings to make sure pop-up blockers are not enabled before running the application.
Cookies
Cookies must be enabled for certain features to function correctly. Check your browser settings to make sure cookies are enabled before running the application.

TLS 1.2
When managing Virtual Connect domains in FIPS mode, TLS 1.2 must be enabled in the browser.
The following browser versions support TLS 1.2 natively:
- Internet Explorer 11 and above
- Mozilla Firefox 27 and above

Virtual Connect and Insight Control Server Deployment
If you plan on using VC-assigned MAC addresses and WWNs and are also working with server software that will be licensed by MAC addresses or WWNs, assign server profiles before deploying an image through HPE Insight Control Server Deployment or attaching the license.

Always apply relevant licenses that are dependent on MAC addresses after the server profiles are assigned so that the licenses are not lost due to a change in MAC address.

IMPORTANT: If you plan to use Insight Control Server Deployment for RedHat Linux installation and also plan to use User- or Hewlett Packard Enterprise-defined MAC addresses, you must import the enclosure and assign profiles before running Insight Control Server-Deployment.

"Rip and replace" is not supported in a Virtual Connect environment.

For more information on HPE Insight Control Server Deployment, see the Hewlett Packard Enterprise website (http://www.hpe.com/servers/rdp).

Accessing HPE Virtual Connect Manager
Access to VCM occurs over the same Ethernet connection used to access the enclosure Onboard Administrator and server blade iLO connections.

Access VCM in one of the following ways:
- If the management network uses dynamic DNS, locate the Default Network Settings label on the primary VC-Enet module, and then type the DNS name into the address field of the web browser. If the management network does not use dynamic DNS, use the Onboard Administrator to access VCM.
Log on to the enclosure Onboard Administrator. From the rack overview screen, select the Virtual Connect Manager link from the left navigation tree.

Log on to the enclosure Onboard Administrator. To display the Interconnect Bays summary screen, select Interconnect Bays in the left navigation tree of the Onboard Administrator user interface. Select the Management URL link for the primary VC-Enet module. VCM typically operates on the primary VC-Enet module unless that module becomes unavailable, causing a failover to the backup VC-Enet module. If you cannot connect to the primary VC-Enet module, try connecting to the management URL for the backup VC-Enet module.

Access the VCM CLI remotely through an SSH session by connecting to the VC-Enet module management IP address. In a multi-enclosure VC domain, VCM runs on the primary module in the primary enclosure. If both the primary and backup modules in the primary enclosure fail, are powered off, or are removed, VCM is not accessible.

Command Line Interface overview

The VCM Command Line Interface can be used as an alternative method for administering the VCM. Using the CLI can be useful in the following scenarios:

- You can develop tools that utilize VCM functions for data collection and for executing provisioning and configuration tasks.
- When no browser is available or you prefer to use a command line interface, you can access management data and perform configuration tasks.
- You can batch commands using script files. These script files can be run manually or scheduled to run automatically.

For more information, see the HPE Virtual Connect Manager Command Line Interface for c-Class BladeSystem User Guide on the Hewlett Packard Enterprise website (http://www.hpe.com/info/vc/manuals).
Logging on to the HPE Virtual Connect Manager

Log on using the user name (Administrator) and password.

You can optionally specify the authentication method or VCM role at log on:

- To specify the authentication method (local, ldap, radius, tacacs), enter the authentication method followed by a colon before the user name. For example, ldap:user1.
- To specify the VCM role (domain, network, server, storage), enter the role followed by a colon before the user name. For example, network:user1.

For more information on authentication methods and VCM roles, see the information about Virtual Connect users and roles in the HPE Virtual Connect for c-Class BladeSystem User Guide on the Hewlett Packard Enterprise website (http://www.hpe.com/info/vc/manuals).

If the default password for the Administrator user has been changed and needs to be restored, see "Resetting the Administrator password and DNS settings (on page 121)."

Logon problems might be caused by the following:

- You have recently upgraded the VCM firmware. You might have to clear the browser cache before attempting to log on again.
- The information is not being entered correctly. User names and passwords are case-sensitive.
- The account being entered is not an account for VCM.
- The account being entered has been deleted, disabled, or locked out.
- The password for the account needs to be changed.
- There is no connection to the primary VC-Enet module running VCM.
- VCM is undergoing a failover or recovery.
- The attempted IP sign-in address is not valid for the specified account.
- The attempted IP sign-in address is for a VC-Enet module not running the primary VCM.
- The browser settings are incorrect. See "Configuring browser support ("Browser requirements and configuration" on page 57)."
- You have entered an invalid role or authentication service name.
- Authentication service is disabled, is not correctly configured, or is not up in the server.

About HPE Virtual Connect Manager

To view detailed product information, select About HPE Virtual Connect Manager from the Help pull-down menu.

Reset Virtual Connect Manager

You must have domain privileges to reset VCM. In a multi-enclosure environment, the VC-Enet modules in bays 1 and 2 of the local enclosure host VCM. With VC 3.10 and higher, the primary modules can be in bays other than 1 and 2.

To reset VCM running on the primary VC-Enet module, select Reset Virtual Connect Manager from the Tools pull-down menu. The Reset Virtual Connect Manager screen appears.

- If the Force Failover checkbox is selected and a VC-Enet module is available in the alternate interconnect bay, the GUI is redirected to the alternate VC-Enet module for log on after the VCM has restarted. Reset times depend on the size and complexity of the VC domain configuration.
- If the Force Failover checkbox is not selected or a VC-Enet module is not available in the alternate interconnect bay, the VCM restarts on the current VC-Enet module, and you are presented the logon screen for the current VC-Enet module after VCM restarts. Reset times depend on the size and complexity of the VC domain configuration.

When resetting the VC-Enet module, VCM is temporarily unavailable. If failover is specified and a backup VC-Enet module is available, you are logged off and redirected to the backup VC-Enet module IP address.

Recovering remote enclosures

The credentials of the remote enclosure must be restored in the following situations:

- A previously saved configuration file is restored.
- The Onboard Administrator is reset to factory defaults.
- The Onboard Administrator associated with the remote enclosure is replaced.

If the IP address of the OA in the remote enclosure is lost, the remote enclosure is also marked as NO-COMM. If IP connectivity is lost, credential recovery is not required. The enclosure automatically recovers after connectivity is returned.

Running the setup wizards

Virtual Connect Domain Setup Wizard

A Virtual Connect domain consists of an enclosure and a set of associated modules and server blades that are managed together by a single instance of the VCM. The Virtual Connect domain contains specified networks, server profiles, and user accounts that simplify the setup and administration of server connections. Establishing a Virtual Connect domain enables you to upgrade, replace, or move servers within your enclosures without changes being visible to the external LAN/SAN environments.
Beginning with VC 4.10, an auto-deployment feature allows for the configuration of a VC domain from a centralized location using DHCP and TFTP to access the configuration script. Auto-deployment is supported only for single-enclosure domains. For more information on auto-deployment, see the HPE Virtual Connect for c-Class BladeSystem User Guide on the Hewlett Packard Enterprise website (http://www.hpe.com/info/vc/manuals).

Plan your interconnect module usage carefully before running the Virtual Connect Domain Setup Wizard. After an interconnect bay is configured for use with a VC module, it remains configured for that module type until the module is removed or the overall VC domain is deleted. Virtual Connect reports failures for any VC module that is removed from the domain.

Before getting started, perform the following tasks:

- Verify that the HPE Onboard Administrator is running the latest firmware. Hewlett Packard Enterprise recommends using the latest version available. Using IPv6 requires OA 4.01 or higher.
- Note the following information from the Default Network Settings label attached to the primary module:
  - DNS name
  - User name
  - Password
- Connect any Ethernet module stacking cables ("Recommended stacking connections" on page 22).

After logging in for the first time, the Virtual Connect Domain Setup Wizard appears. This wizard walks you through the following tasks:

- Importing the enclosure (creating the domain)
- Naming the domain
- Administrating local users

If the wizard is canceled before an enclosure is imported, you are returned to the Virtual Connect login page. An enclosure must be imported to proceed.
Local Enclosure

To communicate with other VC modules and server blades, VCM requires the logon credentials for the local Onboard Administrator.

**IMPORTANT:** An Onboard Administrator user name and password with full administrative privileges for the selected enclosure is required.

Enter the user name and password for the enclosure Onboard Administrator. The local enclosure is detected and selected automatically. If an error appears, it indicates that an invalid Onboard Administrator user name and password, or one without sufficient privileges, might have been used.

After you import the remote enclosure, the OA IP address must not change. You must always assign a static IP address or configure it appropriately through your DHCP server.

VCM creates a local user named "vcmuser" on the OA module. Do not modify the credentials for this user. Do not change the "local users" authentication setting for the OA module.

Enclosure Import/Recovery

After VCM has successfully established contact th e Onboard Administrator, you can create a Virtual Connect domain by importing the enclosure or by restoring a previously created Virtual Connect domain from a saved configuration file.

If you plan to use double density server blades, select the "Enable double dense server support (Restricts single dense server support)" checkbox to display server device bays as double density slots.

This option should only be selected if double-dense servers will be in use. Single-dense servers do not have access to I/O bays 7 and 8 when this option is selected.
NOTE: This option cannot be modified. After the enclosure is imported, select the Display single dense device bays checkbox on the Domain Settings (Configuration) screen to display server device bays as single density slots again.

For more information, see "Using double-dense server blades (on page 66)."

Select the appropriate method for creating the Virtual Connect domain.

- To create the Virtual Connect domain by importing an enclosure, select the "Create a new Virtual Connect domain by importing this enclosure" radio button, and then click Next. This process can take several minutes as VCM establishes contact with each module in the enclosure and identifies its capabilities.

  CAUTION: Restoring a Virtual Connect domain configuration from a backup file that was created on another Virtual Connect domain is not supported and can cause serious faults within this and other Virtual Connect Domains within the environment. The restore selection and configuration files should only be used to restore the same previously existing domain.

- To restore a domain using an existing configuration file, select the "Restore a Virtual Connect domain using an externally-saved configuration file" radio button, and then click Next.
Enclosure Import

After making the selection to create a new Virtual Connect domain by importing the enclosure on the Enclosure Import/Recovery screen, the Import Status screen appears and provides information about whether the import was successful. If the import is not successful, error information is displayed.

Importing additional enclosures

To import additional enclosures using the Domain Setup Wizard after the initial enclosure has been imported:

1. Select **Tools > Domain Setup Wizard**.
2. On the Enclosure Import Recovery screen, click **Find Enclosure**.
3. Click **Find Enclosure** to find additional enclosures.
4. Enter the OA IP address, user name, and password.
5. Select the checkbox next to the enclosures to import.
6. Click **Next**. The Import status screen appears so that you can verify a successful import.

To import additional enclosures using the Domain Settings screen:

1. Click the **Domain Settings** link on the Virtual Connect Home screen.
2. Click the **Domain Enclosures** tab.
3. Click **Add**.
4. Enter the appropriate OA information, and then click **OK**.
5. Select the checkbox next to the enclosure to import.
6. Click **Import**.
Using double-dense server blades

Virtual Connect Manager supports the use of double-dense server blades, enabling support for up to 32 device bays in a single c7000 enclosure. This support also provides 32 new device bays (1A-16A and 1B-16B) for profile assignment. On a c3000 enclosure, this feature supports 8 additional or 16 total device bays. (1A-8A and 1B-8B)

The two physical servers A and B in a double-dense server blade correspond to the left and the right sides of the device bay in c7000 enclosures, or the top and bottom of the device bay in c3000 enclosures. Servers A and B have independent iLO, power, presence, and status capabilities.

In c7000 enclosures, Bays 1A-16A are associated with the left sides of the double-dense server blades seated in the half-height bays 1-16. Bays 1B-16B are associated with the right sides of the double-dense server blades seated in the half-height bays 1-16. In c3000 enclosures, Bays 1A-8A are associated with the top of the double-dense server blades seated in the half-height bays 1-8. Bays 1B-8B are associated with the bottom of the double-dense server blades seated in the half-height bays 1-8.

Enclosure recovery

If restoring a Virtual Connect domain using an externally saved configuration file, click **Browse** and locate the saved configuration file.

⚠️ **CAUTION:** Restoring a Virtual Connect domain configuration from a backup file that was created on another Virtual Connect domain is not supported and can cause serious faults within this and other Virtual Connect Domains within the environment. The restore selection and configuration files should only be used to restore the same previously existing domain.

If the configuration file was originally created on an enclosure with a different serial number, the **Ignore enclosure serial number in restored configuration file** checkbox must be selected to allow it to be used in a new enclosure. Click **Next** to continue restoring the enclosure. At the end of the restoration, the browser returns to the login screen. After the domain is restored, one of the local user accounts from the original Virtual Connect domain must be used to login.
When restoring from the configuration file, remote enclosure credentials are lost. See "Recovering remote enclosures (on page 61)."

**General Settings**

The Virtual Connect domain name should be unique within the data center, and can be up to 31 characters without spaces or special characters.

The Domain Setup Wizard automatically assigns a domain name (enclosurename_vc_domain). This name can be changed when running the setup wizard, or at any time from the Domain Settings (Configuration) screen.
Local Users

The first time this screen appears, the Administrator account, which has all administrative user role
permissions, might be the only user listed. The Administrator account cannot be deleted or have domain
user role permissions removed. However, the Administrator password can be changed, and the network,
server, and storage user role permissions can be removed. The default Administrator password is
identified on the Default Network Settings label on the primary VC module.

To reset the Administrator password to the factory default, see "Resetting the Administrator password and
DNS settings (on page 121)." Resetting the Administrator password using the system maintenance switch
does not delete the VC domain, if configured. The password and DNS name of the module is reset to
match the information included on the Default Network Settings label on the module.

The following tasks can be performed on this screen:

- To create a new local user account, click Add. The Add Local User screen appears.
- To edit attributes of a defined local account, click the Edit link in the user row.
- To delete a user account, select the checkbox next to the user name, and then click Delete.

⚠️ TIP: You can also highlight a user, right-click, and then select Add, Delete, or Edit from the
pull-down menu.

- To enable strong passwords, select the Require Strong Passwords checkbox. Use the up and
down arrows to select a password length between 3 and 40 characters. The default password length
for a newly created domain is 8 characters. With strong passwords enabled, passwords must also
contain at least one character from three of the following four categories:
  - Upper-case character
  - Lower-case character
  - Numeric character
  - Non-alphanumeric character
Click Apply to save your changes.

- To set a session timeout period, enter a number between 10 and 1440 in the Session Timeout box.
To disable a session timeout period, enter 0. Click Apply to save your changes.
Any change in the timeout value affects all open sessions and is applied to new sessions.

- To edit the delete confirmation preference, select or clear **Auto Populate Name During Delete Confirmation**, and then click **Apply**. VCM displays confirmation dialog boxes when deleting objects such as server profiles, networks, and so on. These dialog boxes require you to enter the name of the item you want to delete and, in some cases, you must also enter the word "delete." If you enable the Auto Populate Name During Delete option, the confirmation dialog boxes appear with the required information automatically populated, enabling you to simply click **OK** to proceed with the deletion. This is a domain-wide setting.

- To enable local users, select the **Enable Local Users** checkbox. To disable local users, clear the **Enable Local Users** checkbox. Click **Apply** to save your changes. You cannot disable local users if you are logged in as a local user. Log in as an LDAP, TACACS, or RADIUS authenticated user with domain privileges to disable local users.

- To select the Primary Remote Authentication Method, select an option from the Primary Remote Authentication Method list. Click **Apply** to save your changes. The Primary Remote Authentication Method is the primary authentication mechanism that triggers the re-enablement of local user authentication (if it was disabled) if the remote authentication servers are found to be unavailable during login by a remote VC user. Valid values include NONE, LDAP, RADIUS, and TACACS. The default value is NONE.
User Settings

Observe the following user settings guidelines:

- Username is a required field.
- The Username field must contain an alpha-numeric value with 1 to 31 characters.
- The Password field must contain an alpha-numeric value with 3 to 40 characters. The default password length is 8 characters.
- If strong passwords are enabled, the password must contain the administrator-designated number of characters and at least one character from three of the following four categories:
  - Upper-case character
  - Lower-case character
  - Numeric character
  - Non-alphanumeric character
- The Full Name field can contain a value with a maximum value of 63 characters.
- The Contact field can contain a value with a maximum value of 127 characters.

Up to 32 local user accounts can be created. Each account can be set up to have a combination of up to four access roles: Domain, Network, Server, Storage. When a role is selected, the operations for that role are listed with a checkmark.

The operations assigned to each role can be edited on the Role Management (Role Operations) screen.
Finish domain wizard

Click **Finish** to complete this wizard, and then run the Network Setup Wizard ("Virtual Connect Network Setup Wizard" on page 71) to define the Ethernet networks that will be available within the Virtual Connect domain.

Deselect the Start the Network Setup Wizard checkbox, and then click **Finish** to go to the Home page without running additional setup wizards.

**Virtual Connect Network Setup Wizard**

This wizard establishes external Ethernet network connectivity for the HPE BladeSystem c-Class enclosure using HPE Virtual Connect. A user account with network privileges is required to perform these operations. Use this wizard to do the following:

- Identify the MAC addresses to be used on the servers deployed within this Virtual Connect domain.
- Choose the method of handling VLAN tagged packets from servers.
- Configure multiple networks link speed settings.
- Set up connections from the HPE c-Class enclosure to the external Ethernet networks. These connections can be uplinks dedicated to a specific Ethernet network or shared uplinks that carry multiple Ethernet networks with the use of VLAN tags.
- Define external network connections with shared uplinks that carry multiple Ethernet networks or FCoE networks

Be sure to connect any Ethernet module stacking cables before running the setup wizard.
IMPORTANT: For a Virtual Connect environment to operate properly, all HPE Virtual Connect Ethernet modules within the Virtual Connect domain must be interconnected with stacking links. Hewlett Packard Enterprise strongly recommends that redundancy be maintained in stacking links to ensure continued connectivity of servers to the external networks.

For more information, see "Supported configurations (on page 14)" and "Recommended stacking connections (on page 22)."

NOTE: Virtual Connect does not support stacking for FC modules, so each VC-FC module requires uplink connections to the external FC SAN environment.

To initiate this wizard, click the Network Setup Wizard link on the homepage, or select Network Setup Wizard from the Tools pull-down menu. You must have network role permissions to access the Network Setup Wizard.

MAC Address Settings

At this point in the wizard, you are asked to select the type of Ethernet MAC addresses to be used on the server blades within the enclosure. Choose either the server factory default Ethernet MAC address that came with the server or the Ethernet MAC addresses assigned by Virtual Connect. Be sure to fully understand the following information before making this selection.

IMPORTANT: Configuring Virtual Connect to assign server blade MAC addresses requires careful planning to ensure that the configured range of MAC addresses is used once within the environment. Duplicate MAC addresses on an Ethernet network can result in a server network outage.

Each server blade Ethernet NIC ships with a factory default MAC address. The MAC address is a 48-bit number that uniquely identifies the Ethernet interface to other devices on the network. While the hardware ships with default MAC addresses, Virtual Connect can assign MAC addresses that override the factory default MAC addresses while the server remains in that Virtual Connect enclosure.
Always establish control processes to ensure that a unique MAC address range is used in each Virtual Connect domain in the environment. Reusing address ranges could result in server network outages caused by multiple servers having the same MAC addresses.

If using Virtual Connect assigned MAC addresses, the following notes apply:

- Virtual Connect automatically assigns two MAC addresses to each VC-Enet connection in the server profile, a primary address for the Ethernet NIC, and an iSCSI MAC address for use by multifunction gigabit server adapters, such as the HPE NC373m PCI Express Dual Port Multifunction Gigabit Server Adapter. Only the primary MAC address is used by standard (not multifunction) Ethernet devices.

- If a server blade is moved from a Virtual Connect managed enclosure to a non-Virtual Connect enclosure, the local MAC addresses on that server blade are automatically returned to the original factory defaults.

- If a server blade is removed from a bay within a Virtual Connect domain and installed in another bay in the same Virtual Connect domain or in a bay in a different domain, it is assigned the new set of addresses appropriate for that server location.

When FlexFabric adapters are in use, Virtual Connect assigns a MAC address to each FCoE connection in the server profile.

**Assigned MAC addresses**

The MAC address range used by the Virtual Connect domain must be unique within the environment. Hewlett Packard Enterprise provides a set of pre-defined ranges that are for use by VCM and do not conflict with server factory default MAC addresses.

When using the Hewlett Packard Enterprise-defined MAC address ranges, be sure that each range is used only once within the environment.
Select the type and range of MAC address, and then click **Next**.

**Selecting VC-assigned MAC address ranges**

When using VC-assigned MAC addresses, you can choose between using a Hewlett Packard Enterprise pre-defined MAC address range or using a user-defined MAC address range.

- **Hewlett Packard Enterprise pre-defined MAC address range (recommended).** These pre-defined ranges are reserved and are not the factory default on any hardware. There are 64 ranges of 1024 unique addresses to choose from. Be sure to use each range only once within a data center. 1024 unique addresses might not be enough for a large configuration (multiple enclosures with many Flex-10 NICs). If you plan a domain of this type, determine the number of MAC addresses you are likely to use, and then select an option that provides the domain with sufficient MAC addresses.

- **User-defined MAC address range.** To avoid potential conflict with other hardware MAC addresses in the environment, consider using a subrange of MAC addresses reserved by the IEEE for locally-administered MAC addresses. Ensure that the range does not conflict with any Ethernet device already deployed within the enterprise.

**IMPORTANT:** If you plan to use Insight Control Server Deployment for RedHat Linux installation and also plan to use User- or Hewlett Packard Enterprise-defined MAC addresses, you must import the enclosure and assign profiles before running Insight Control Server-Deployment.
NOTE: After any server profiles are deployed using a selected MAC address range, that range cannot be changed until all server profiles are deleted.

Select the type and range of MAC address, and then click **Next**.

**Server VLAN Tag Settings**

![Server VLAN Tag Settings](image)

**VLAN tunneling support**

You can tunnel VLAN tags and map VLAN tags in the same domain. As of VC 3.30, tunneling and mapping is configured at the network level, not at the domain level. Server VLAN tunneling is supported only on networks with dedicated uplinks and cannot be used with shared uplink sets.

**Server VLAN tagging support**

When the 'Force server connections to use same VLAN mappings as shared uplink sets' check box is selected, server ports connected to multiple VC Ethernet networks are forced to use the same VLAN mappings as those used for the corresponding shared uplink sets. This action forces all server connections mapped to multiple networks to be linked to a shared uplink set. Server administrators cannot override this selection when creating or editing a profile. When this check box is selected, server network connections can only be selected from a single shared uplink set.

When the 'Force server connections to use same VLAN mappings as shared uplink sets' check box is not selected, server network connections can be selected from any VC Ethernet network and the external VLAN ID mappings can be manually edited. However, administrators must ensure that no server connection VLAN ID conflict exists.

The 'Force server connections to use the same VLAN mappings as shared uplink sets' check box can be selected if no server profile connections are assigned to multiple networks that are not linked to a shared uplink set.

**VLAN capacity**

When the domain is configured with the Expanded VLAN capacity mode, observe the following information:

- 8,192 VLANs can be defined per domain.
- 4,094 VLANs can be defined per shared uplink set.
- 1,000 networks can be active and in use at any time:
An Ethernet network remains in a Linked/Standby state and becomes active when it is assigned to a server profile or an sFlow configuration.

An FCoE network becomes active when it is associated with a shared uplink set.

- 162 VLANs can be defined per physical server port.
  - Duplicate VLANs cannot be configured on the same physical port.
  - Do not map more than 162 VLANs to one physical server port. If you exceed the 162 VLAN limit, the physical server port is disabled and the four server connections are marked as failed.
    For example, if you configure 150 VLAN mappings to FlexNIC-a, then only 12 VLANs can be configured for the remaining FlexNICs (FlexNIC-b, FlexNIC-c, and FlexNIC-d).

- VCEM enforces consistent in-use definitions across all domains in each domain group. If a domain is in maintenance mode and changes are made which would increase the number of in-use networks beyond 1000 for any domain in the domain group, the complete maintenance operation fails, and the domain stays in maintenance mode.

When the domain is configured with the Legacy VLAN Capacity mode, observe the following:

- The option to select Legacy VLAN Capacity mode is disabled when creating new domains with VC firmware 3.70 or higher. Reverting from Expanded VLAN Capacity mode back to Legacy VLAN Capacity mode is not allowed.
- To maintain compatibility for VC domains configured with Legacy VLAN Capacity mode and upgrading firmware from VC 3.30 to VC3.70 or higher, the VCM CLI maintains the functionality of the Legacy VLAN capacity setting. This allows the use of existing scripts that configure the VLAN capacity mode.

### Multiple Networks Link Speed Settings

When using mapped VLAN tags (multiple networks over a single link), these settings are used for the overall link speed control. Select the checkbox next to each item to set the value.

These settings affect only newly created profiles.

Versions of VC prior to v4.01 used the "preferred speed" to control bandwidth allocation. When existing profiles are upgraded to VC v4.01 or later, the "maximum speed" from the network is set automatically on the connection. If no maximum speed was configured prior to the upgrade, then the maximum speed is 20 Gb for Ethernet connections. The 20Gb maximum speed is dependent on 20Gb NICs and the HPE VC FlexFabric-20/40 F8 Module being present in the domain. The pre-4.01 behavior can be retained by setting "maximum speed" to the same value as "preferred speed". When the maximum speed and preferred speed for a network are set to the same bandwidth, then the profile connection bandwidth does not exceed the custom speed set on the connection.

**IMPORTANT:** Depending on the NIC firmware versions in use, you might need to upgrade the NIC firmware for these speed enforcement settings to work correctly.

To change these settings:

1. Click the selection box, and then select a setting (100Mb to 20Gb):
   - Set preferred connection speed. This value is the default speed for server profile connections mapped to this network. The server administrator can increase or decrease this setting on an individual profile connection. This setting is used for the minimum bandwidth.
   - Set maximum connection speed. This value is the maximum speed for server profile connections mapped to this network. This setting limits the maximum port speed from the server to the network connection associated with the multiple networks. Maximum bandwidth is determined by the maximum connection speed of the network. All multiple networks share the same maximum connection speed.

The availability of the 20Gb setting is dependent on 20Gb NICs and HPE VC FlexFabric-20/40 F8 Modules being present in the domain.

2. Click **Apply**.
Virtual Connect can control link speed for FlexNICs only when they are connected to an HPE Virtual Connect Enet Module. Virtual Connect cannot control the link speed of traditional NICs.

**IMPORTANT:** Each FlexNIC and FlexHBA is recognized by the server as a PCIe physical function device with adjustable speeds from 100 Mb to 10 Gb in 100 Mb increments when connected to an NC553i/m 10Gb 2-port FlexFabric FlexFabric Adapter or any Flex-10 NIC. For NC551i/m Dual Port FlexFabric 20 Gb FlexFabric Adapters, the range is limited to 1 Gb to 20 Gb in 100 Mb increments.

For more information on FlexNICs, see the *HPE Virtual Connect for c-Class BladeSystem User Guide* on the Hewlett Packard Enterprise website ([http://www.hpe.com/info/vc/manuals](http://www.hpe.com/info/vc/manuals)).

Select Network Connection Type

To begin, select one of the following external network connections:

- Connection with uplink(s) dedicated to a single network ("Define Single Network" on page 78)
  Select this option to define a network within the Virtual Connect environment and identify any module uplink ports used to connect to that network in the data center. Internal-only networks (without external uplinks) can also be defined.
  These single networks pass through any VLAN tags added by the server or added externally.

- Connection with uplink(s) carrying multiple Ethernet networks and/or FCoE networks (using VLAN tagging) ("Define Shared Uplink Set Connection" on page 81)
  Select this option to define multiple networks, FCoE networks, or both that all share a common set of module uplink ports within the Virtual Connect environment. Network traffic from each network within the Virtual Connect environment receives a VLAN tag as it exits on a shared uplink port. Virtual Connect uses the VLAN tag on incoming network traffic to place it on the appropriate internal network. Ethernet VLAN tags are added on egress and stripped on ingress.
  Avoid using this type of network connection when the server inserts VLAN tags.
  One network can be designated as a native VLAN, causing all untagged incoming Ethernet packets to be placed on this network. For more information, see "Shared uplink sets and VLAN tagging" in the user guide.

After each network is defined, you have the option to define additional networks or finish the wizard.
To determine the types of network connections to use, see "Connecting Virtual Connect Ethernet module uplinks (on page 45)."

Define Single Network
To define a network:
1. Enter a name for the network that will be easily understood and recognized by the server administrators defining and deploying server profiles. The network name can be up to 64 characters in length (no spaces).
2. To add a color to the network, select a color from the Color pull-down menu. The network color is used as a visual identifier for the network within VCM.
3. To add labels to the network, type a label in the Labels field, and then press Enter. Labels are used as text-based identifiers for the network within VCM. Each label can contain up to 24 characters, excluding spaces. Each network can have up to 16 labels.
4. To enable Smart Link, select the Smart Link checkbox. The checkbox is not available until an uplink is added to the network.
5. To designate as a private network, select the Private Network checkbox.
6. To enable VLAN tunneling, select the Enable VLAN Tunneling checkbox.
7. To set a custom value for the preferred link connection speed or maximum link connection speed, select the Advanced Network Settings checkbox. For more information, see "Advanced Network Settings (on page 79)."
8. Set the connection mode to Auto or Failover.
9. If the connection mode is set to Auto, set the length of the LACP Timer.
10. Select the specific VC-Enet module external uplink ports that will connect the network to the data center. The available external ports are listed in the multi-level Add Port selector. Each port is labeled as linked or not linked. This status refers to whether or not a current connection to an external switch exists.
   If the network will be local to the servers within the VC domain (enclosure), then no uplinks need to be selected.
   To delete a port, click the Delete link in the Action column of the row to be deleted.
11. In the Network Access Groups field, begin typing the name of a Network Access Group that should include this network. When the Network Access Group name appears, select the name.
12. Click Create Network.

For more information on defining networks, see the HPE Virtual Connect for c-Class BladeSystem User Guide on the Hewlett Packard Enterprise website (http://www.hpe.com/info/vc/manuals).

Advanced Network Settings
These settings affect only newly created profiles.

Versions of VC prior to v4.01 used the "preferred speed" to control bandwidth allocation. When existing profiles are upgraded to VC v4.01 or later, the "maximum speed" from the network is set automatically on the connection. If no maximum speed was configured prior to the upgrade, then the maximum speed is 20 Gb for Ethernet connections. The 20Gb maximum speed is dependent on 20Gb NICs and the HPE VC FlexFabric-20/40 F8 Module being present in the domain. The pre-4.01 behavior can be retained by setting "maximum speed" to the same value as "preferred speed". When the maximum speed and preferred speed for a network are set to the same bandwidth, then the profile connection bandwidth does not exceed the custom speed set on the connection.

**IMPORTANT:** Depending on the NIC firmware versions in use, you might need to upgrade the NIC firmware for these speed enforcement settings to work correctly.

To change these settings:
1. Click the selection box, and then select a setting (100Mb to 20Gb):
   o Set preferred connection speed. This value is the default speed for server profile connections mapped to this network. The server administrator can increase or decrease this setting on an individual profile connection. This setting is used for the minimum bandwidth.
Set maximum connection speed. This value is the maximum speed for server profile connections mapped to this network. This setting limits the maximum port speed from the server to the network connection associated with the multiple networks. Maximum bandwidth is determined by the maximum connection speed of the network. All multiple networks share the same maximum connection speed.

The availability of the 20Gb setting is dependent on 20Gb NICs and HPE VC FlexFabric-20/40 F8 Modules being present in the domain.

2. Click **Apply**.
Define Shared Uplink Set Connection

To define multiple networks that share a common set of external uplink ports:

1. Enter an overall name for the set of shared uplinks (up to 64 characters, no spaces).
2. Set the connection mode to **Auto** or **Failover**.
3. If the connection mode is set to Auto, set the length of the LACP Timer.
4. From the Add Port list, select the external uplink ports that will carry these networks.
   To delete a port, click the **Delete** link in the Action column of the row to delete.
5. Click **Add** to define an associated FCoE Network.
   When associating an FCoE network, the shared uplink set must contain uplink ports from a single VC module. In a multi-enclosure domain, the matching ports must be available in all enclosures in the domain. For VC 4.10, only one FCoE network can be associated with a given shared uplink set. In VC 4.20 and later, up to 32 FCoE networks can be associated with a given shared uplink set.
   a. Enter a network name.
   b. Enter a VLAN identifier.
   c. To add a color to the network, select a color from the Color pull-down menu. The network color is used as visual identifier for the network within VCM.
d. To add labels to the network, type a label in the Labels field, and then press Enter. Labels are used as text-based identifiers for the network within VCM. Each label can contain up to 24 characters, excluding spaces. Each network can have up to 16 labels.

e. To set a custom value for the preferred link connection speed or maximum link speed, click Advanced Network Settings. For more information, see "Advanced Network Settings (on page 79)."

f. Click Apply.

6. Click Add to define the name and VLAN identifier of each network to use these shared uplinks.

   a. You can add a single associated network or multiple associated networks. Selecting multiple associated networks enables you to enter a comma-separated list of individual VLANs and ranges of VLANs that share a common name.

      The name is composed of the prefix, VLAN ID, and suffix. An example name is provided after the VLAN IDs are specified.

   b. To add a color to the network, select a color from the Color pull-down menu. The network color is used as a visual identifier for the network within VCM.

   c. To add labels to the network, type a label in the Labels field, and then press Enter. Labels are used as text-based identifiers for the network within VCM. Each label can contain up to 24 characters, excluding spaces. Each network can have up to 16 labels.

   d. To use native VLAN, select the Native check box. Only one VLAN can be designated as the native VLAN.

   e. To use Smart Link, select the Smart Link check box. The check box is not available until an uplink is added to the shared uplink set.

   f. To designate the network as private, select the Private Network check box.

   g. To set a custom value for the preferred link connection speed or maximum link speed, click Advanced Network Settings. For more information, see "Advanced Network Settings (on page 79)."

   h. Click Apply.

7. To create the associated networks, click Create Shared Uplink Set.

   To delete associated networks, select the check box for one or more networks, and then click Delete.

   For more information on defining a new shared uplink set and VLAN tagging, see the HPE Virtual Connect for c-Class BladeSystem User Guide on the Hewlett Packard Enterprise website (http://www.hpe.com/info/vc/manuals).
Add an Associated FCoE Network.

Add a single Associated Network.
Add multiple Associated Networks.

Defined Network Connections

This summary screen displays the external connections for each defined network.
Finish network wizard

When the Network Setup Wizard completes, external Fibre Channel connectivity can be configured (if applicable) or server profiles can be defined and associated with server blades.

To establish external Fibre Channel connectivity:
1. Be sure the Start the Fibre Channel Wizard checkbox is selected.
2. Click Finish. The Fibre Channel Wizard Welcome screen is displayed.

To begin deploying server blades:
1. Be sure the Start Fibre Channel Wizard checkbox is not selected.
2. Click Finish.
3. Select Define Server Profile from the homepage.

Additional network connections can be defined at any time by using one of the following methods:

- Select the Define a Network link on the homepage.
- Select the Define a Shared Uplink Set link on the homepage.
Select **Ethernet Network** from the **Define** pull-down menu.

### HPE Virtual Connect Fibre Channel Setup Wizard

This wizard configures external Fibre Channel connectivity for the HPE BladeSystem c-Class enclosure using HPE Virtual Connect. A user account with storage privileges is required to perform these operations. Use this wizard to do the following:

- Identify WWNs to be used on the server blades deployed within this Virtual Connect domain.
- Define fabrics.

To initiate this wizard, click the Fibre Channel Wizard link on the homepage, or select **Fibre Channel Setup Wizard** from the Tools pull-down menu. You must have storage privileges to access the Fibre Channel Setup Wizard.

**WWN settings**

At this point in the wizard, you are asked to select the type of FC WWNs to be used on the server blades within the enclosure. You can choose to use the server factory default WWNs provided with the FC HBA.
mezzanine card or to use FC WWNs assigned by Virtual Connect. Be sure to fully understand the following information before making this selection.

Each server blade FC HBA mezzanine card ships with factory default port and node WWNs for each FC HBA port. Each WWN is a 64-bit number that uniquely identifies the FC HBA port/node to other devices on the network. While the hardware ships with default WWNs, Virtual Connect has the ability to assign WWNs that override the factory default WWNs while the server remains in that Virtual Connect enclosure. When configured to assign WWNs, Virtual Connect securely manages the WWNs by accessing the physical FC HBA through the enclosure Onboard Administrator and the iLO interfaces on the individual server blades.

When assigning WWNs to FC HBA ports, Virtual Connect assigns both a port WWN and a node WWN. Because the port WWN is typically used for configuring fabric zoning, it is the WWN displayed throughout the Virtual Connect user interface. The assigned node WWN is always the same as the port WWN incremented by one.

Virtual Connect assigns or migrates WWNs for server FC ports connected to HPE Virtual Connect modules. Virtual Connect also assigns WWNs to FC ports that are not connected to an I/O module because Virtual Connect modules can be added later. Server FC ports connected to non-Virtual Connect modules retain the server factory default WWNs.

Configuring Virtual Connect to assign WWNs in server blades maintains a consistent storage identity (WWN) even when the underlying server hardware is changed. This method allows server blades to be replaced without affecting the external Fibre Channel SAN administration.

⚠️ **CAUTION:** To avoid storage networking issues and potential loss of data associated with duplicate WWNs on a FC SAN fabric, plan carefully when allowing Virtual Connect to assign server blade WWNs so that the configured range of WWNs is used only once within the environment.
Assigned WWNs

The WWN range used by the Virtual Connect domain must be unique within the environment. Hewlett Packard Enterprise provides a set of pre-defined ranges that are reserved for use by Virtual Connect and do not conflict with server factory default WWNs.

When using the Hewlett Packard Enterprise-defined WWN ranges, be sure that each range is used only once within the environment.

Select the type and range of WWNs, and then click Next.
Define Fabric

To define a fabric, select the Define Fabric checkbox, and then click Next. If you do not want to define a fabric at this time, select I do not want to create a Fabric, and then click Next.

Define SAN Fabric

To define the SAN fabric:
1. Name the fabric. Do not use spaces.
2. Select the uplink ports to be used. Only uplinks on the same bay can be in the same SAN fabric.
3. If the uplink ports selected are FlexFabric module ports, select the fabric type. Supported fabric types are FabricAttach and DirectAttach:
   o Select FabricAttach if the FlexFabric module is connected using traditional SAN switches. For this fabric type, the advanced settings appear, allowing you to change the login re-distribution and set the preferred and maximum connection speed.
   o Select DirectAttach if the FlexFabric module is directly connected to a supported storage target. Login re-distribution is not applicable for a DirectAttach fabric; however, advanced settings are available for the preferred and maximum FCoE connection speed.

After a fabric is defined, its type cannot be changed. The default fabric type is FabricAttach.
4. If you are linking to an HPE VC FlexFabric module and the fabric type is FabricAttach, click Advanced to set the login re-distribution. For more information, see "Advanced SAN Fabric Settings (on page 90)."
5. Change the configuration speed, if preferred.
6. Click Apply.

In DirectAttach mode, connect the FC-capable uplink ports from the HPE VC FlexFabric module to the target ports on the 3PAR array controller node.

In FabricAttach mode, connect the uplink ports from the following modules to the NPIV-enabled Fibre Channel switch ports:
   • HPE VC 8Gb 24-Port FC Module
   • HPE VC 16Gb 24-Port FC Module
   • HPE VC 8Gb 20-Port FC Module
   • HPE VC FlexFabric-20/40 F8 Module
   • HPE VC FlexFabric 10Gb/24-port Module

If you are using a Brocade FC switch, verify that NPIV is enabled by using the portshow command.

For VC 8Gb or 16Gb 24-Port FC Modules, if uplink port 8 is present in the VC SAN fabric definition, the port is treated as the lowest-numbered port and receives server logins before any other uplink ports.

Advanced SAN Fabric Settings

Login Re-Distribution
When creating or editing a SAN fabric using HPE VC FlexFabric Modules in a FabricAttach fabric, select the Show Advanced Settings checkbox to select the login re-distribution:
   • Manual Login Re-Distribution—Default for all FC modules. You must initiate a Login Re-Distribution request through the VC GUI or CLI interfaces. You might re-distribute logins if an uplink that was previously down is now available, if you added an uplink to a fabric, or if the number of logins through each available uplink has become unbalanced for any reason.

   • Automatic Login Re-Distribution—When selected, the VC FlexFabric module initiates Login Re-Distribution automatically when the specified time interval expires. For more information about setting the time interval, see "Fibre Channel Settings (Misc.) screen" in the user guide.

The automatic option is only available on FlexFabric modules in a FabricAttach fabric and enables you to specify an interval, in seconds, for the length of time the previously offline links must be stable before the module can re-distribute logins. Login re-distribution is not supported for DirectAttach fabrics.

FCoE Connection Speed
To change these settings, click the selection box, and then select a setting (100Mb to 8Gb):
• Set a custom value for the Preferred FCoE Connection Speed. This value is the default speed for server profile connections mapped to this fabric. The server administrator can override this setting on an individual profile connection.

Set a custom value for the Maximum FCoE Connection Speed. This value is the maximum speed for server profile connections mapped to this fabric.

To see how logins are currently distributed on the VC-FC module, navigate to the Interconnect Bays Status and Summary screen and select the desired VC-FC module. A new Uplink Port column is added to the Server Ports section of the screen.

To see how logins are currently distributed on the VC FlexFabric module, navigate to the Interconnect Bays Status and Summary screen and select the desired VC FlexFabric module. A new SAN Uplink Port column is added to the Server Ports tab.

You can also see how logins are currently distributed on the VC-FC or FlexFabric modules by logging in to the upstream FC SAN fabric switch.

Fabric summary

This screen lists the summary of fabrics that are created.

Select **Create more fabrics** to define additional fabrics, or **Done** if you have defined all available fabrics.

<table>
<thead>
<tr>
<th>Fabric Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fabric created successfully!</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>All Fabric Connections</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
</tr>
<tr>
<td>--------</td>
</tr>
<tr>
<td>✔️</td>
</tr>
<tr>
<td>✔️</td>
</tr>
</tbody>
</table>

Review all existing fabric connections. Click 'Create more fabrics' to add additional fabric connections. Click 'Done' if you are done creating fabric connections.
Finish Fibre Channel wizard

When the Fibre Channel Setup Wizard completes, server profiles can be defined and associated with server blades.

To begin deploying server blades:
1. Be sure the Start the Server Profile Wizard check box is selected.
2. Click Finish. The Server Profile Wizard Welcome screen appears.

The FC SAN configuration can be changed at any time by using one of the following methods:
- Click WWN Settings under Fibre Channel Settings in the left navigation tree of the homepage.
- Select Fibre Channel Settings from the Configure pull-down menu.

Virtual Connect Manager Server Profile Setup Wizard

This wizard enables you to setup and configure network/SAN connections for the server blades within the enclosure.

Use the wizard to define a server profile template that identifies the server connectivity to use on server blades within the enclosure. Then use the template to create and apply server profiles to up to 16 server blades automatically. Once created, the individual server profiles can be edited independently.

Before beginning the server profile wizard, do the following:
- Complete the Network Setup Wizard.
- Complete the Fibre Channel Setup Wizard (if applicable).
- Be sure that any server blades to be configured using this wizard are powered off.

This wizard walks you through the following tasks:
Serial Number Settings

Use this screen to assign serial numbers to server blades within the domain. By configuring VCM to assign serial numbers, a profile can present a single serial number regardless of the physical server. With these configuration values added to server profiles, software that is licensed to a particular server, based on one or both of these values, can be migrated to new server hardware without re-licensing the software for the new server hardware. This feature prevents you from having to reinstall serial number sensitive software after a system recovery.

⚠️ CAUTION: The use of Serial Number Settings might prevent the proper operation of software designed to track servers by serial number or UUID. Do not enable this feature until you consider and understand the impact to the entire software environment in which the servers operate. This impact includes, but is not limited to, warranty service, asset tracking, server deployment, and software licensing.
Create Server Profile Definition

Use this screen to create a new server profile definition, which defines and configures Ethernet and Fibre Channel connectivity for the server.
Server profile troubleshooting

In some cases, server profiles can be assigned to server blades when certain mismatches exist between the server profile definition and the server blade. The following list summarizes Virtual Connect behavior under these circumstances:

- If the number of network connections in the profile is more than the number of physical Ethernet ports, the profile is assigned. When you view the profile, the connections display a status of "Not mapped."
- If a switch other than a Virtual Connect Ethernet switch is connected to any port in the profile, the profile is assigned, but the MAC address is not changed on the NIC. The connections display a status of "Not mapped" when you view the profile.
- If the number of Fibre Channel connections in the profile is more than the number of physical Fibre Channel HBA ports, the profile is assigned, but the connections display a status of "Not mapped" when you view the profile.
- If the number of iSCSI connections in the profile is more than the number of available iSCSI ports on the server, the profile assignment succeeds, but the connections display a status of "Not mapped" when you view the profile.

For more information on defining a server profile and advanced profile settings, see the HPE Virtual Connect for c-Class BladeSystem User Guide on the Hewlett Packard Enterprise website (http://www.hpe.com/info/vc/manuals).
• If the number of FCoE connections in the profile is more than the number of available FCoE ports on the server, the profile assignment succeeds, but the connections display a status of "Not mapped" when you view the profile.

VCM supports a maximum of 256 profiles within the domain.

**IMPORTANT:** Disabling a server port by entering the iLO Remote Console, rebooting the server, and then using the F9 key to enter RBSU causes a "Profile pending" status for a server profile when a VCM failover occurs.

**IMPORTANT:** Virtual Connect versions 4.30 and later no longer support first-generation HPE Integrity BL860c Server Blades and HPE Integrity BL870c Server Blades. HPE Integrity i2 and i4 model server blades are still supported.

Assign Server Profiles

Server profiles are created from the definition. When these server profiles are created, you can choose to automatically assign them to device bays or to leave the server profiles unassigned.

When defining server profiles in a multi-enclosure configuration, profiles can be assigned to server bays in any of the enclosures that have been added and imported into the domain.

When a profile is created and assigned to a multi-blade server, the profile is applied to all of the blades in the multi-blade server. Be sure that the profile contains enough Ethernet and Fibre Channel connection entries for all of the ports on all of the blades in the multi-blade server.

• Single enclosure domain
Name Server Profiles

The table displays the automatically generated names that will be assigned to the new server profiles. The server profile name can be up to 64 characters in length (no spaces). Because the server profile can be assigned to different locations, Hewlett Packard Enterprise recommends that the name reflect the server function. For each enclosure, a base name is provided. You can use this enclosure name to create names for the profiles assigned to the enclosure. The individual profile names can be edited as needed. Be sure that the names are unique and meaningful.

After reviewing the profiles to be created, click **Create Profiles**.
• Single enclosure domain

Create Server Profiles
This screen provides confirmation of each profile that was created and successfully assigned (if applicable).
Click **Start Over** to create additional profiles using the wizard. This option returns you to the appropriate step for creating more profiles.

Click **Finish** if you are finished creating profiles at this time. This option launches the Virtual Connect Home page.

If creation of a server profile failed, see “Server profile troubleshooting (on page 95).”

---

**Verifying data center connections**

After completing the cabling between the HPE BladeSystem c-Class enclosure and the data center networks, use the following techniques to verify that the network connections are operating properly:

- Verify that all external connections are linked and operating at the right speed.
- Review the Virtual Connect Manager Network status screens (“Verify network status using VC Manager” on page 100).
- Use port IDs to verify network connections.
- Configure a server and verify network connectivity.

**Verify link and speed**

To verify external ports are linked and operating at the appropriate speed:

1. Verify all hardware has power:
   a. The data center switches are powered on.
   b. VC Enet, FC, and FlexFabric modules are powered on.
2. Verify module LEDs are green:
a. Verify the health or status LEDs are green for all modules.
    If any health or status LEDs are not green, use the HPE Onboard Administrator to verify that the modules are powered on or to diagnose the problem.

b. Verify the link/speed LED for each external port.
    If ports are not linked, verify the cables are not defective and both ends of the link are configured for the same speed/duplex settings. Both sides of the configuration must match for the link to be established. For autonegotiation, both ports must be configured to autonegotiate. To use a forced speed, for example, 100Mb full-duplex, both ports must be configured to be the same speed. Mismatched configurations can result in ports not linking or functioning properly. VC-Enet and FlexFabric modules do not support half-duplex operations.

c. Verify that the port status LED (the port number) of each configured external port is green, assuming no port IDs are enabled.

3. Verify the VCM configuration:
   a. The network is configured properly.
   b. The network is connected to a server profile in VCM.
      When a VC network is defined and connected to one or more uplinks, those uplinks will remain in a Linked/Standby state until the network is associated with a server profile.

**Verify network status using VC Manager**

VCM provides many status and summary screens that can be used to verify that the networks were defined properly and mapped to the appropriate network.

One useful summary screen is the Ethernet Networks (Summary) screen. To access this screen, click the Ethernet Networks link in the left navigation tree.

The following actions are available from this screen:

- Identify the external ports associated with each Ethernet network.
- View the current port status (link, speed) of each external port.
- View the current active/standby state of each external port.
- Access information about attached switches (if the external switch supports LLDP).
- Highlight the port IDs for all external ports associated with a specific network.
## Component identification

### HPE Virtual Connect Flex-10 10Gb Ethernet Module components and LEDs

### HPE Virtual Connect Flex-10 10Gb Ethernet Module components

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Port X1 (10GBASE-CX4), multiplexed with item 4</td>
</tr>
<tr>
<td>2</td>
<td>USB 2.0 mini AB port (covered)</td>
</tr>
<tr>
<td>3</td>
<td>Next button</td>
</tr>
<tr>
<td>4</td>
<td>Port X1 SFP+ port*, multiplexed with item 1</td>
</tr>
<tr>
<td>5</td>
<td>Port X2 SFP+ port*</td>
</tr>
<tr>
<td>6</td>
<td>Port X3 SFP+ port*</td>
</tr>
<tr>
<td>7</td>
<td>Port X4 SFP+ port*</td>
</tr>
<tr>
<td>8</td>
<td>Port X5 SFP+ port*</td>
</tr>
<tr>
<td>9</td>
<td>Port X6 SFP+ port*</td>
</tr>
<tr>
<td>10</td>
<td>Port X7 SFP+ port*, multiplexed with internal 10Gb interface cross-link</td>
</tr>
<tr>
<td>11</td>
<td>Port X8 SFP+ port*, multiplexed with internal 10Gb interface cross-link</td>
</tr>
<tr>
<td>12</td>
<td>Reset button (recessed)</td>
</tr>
</tbody>
</table>

*Supports 1000BASE-T-SFP, 1000BASE-SX-SFP, 10GBASE-LR SFP+, 10GBASE-SR SFP+, 10GBASE-LRM SFP+, and 10GBASE-T SFP+ pluggable transceiver modules
## HPE Virtual Connect Flex-10 10Gb Ethernet Module LEDs

<table>
<thead>
<tr>
<th>Item</th>
<th>LED description</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Module locator (UID)</td>
<td>Blue = Module ID is selected. Off = Module ID is not selected.</td>
</tr>
</tbody>
</table>
| 2    | Module status | Green = Normal operation  
                      Amber = Degraded condition  
                      Amber flashing = Fault condition  
                      Off = Power off |
| 3    | X1 port status (10GBASE-CX4) | Green = Port is configured and operating as an uplink port connected to a data center fabric.  
                                   Amber = Port is operating as a stacking link interconnecting Virtual Connect modules.  
                                   Blue = Port locator (PID)  
                                   Off = Unconfigured |
| 4    | X1 link/port activity | Green = Link  
                                   Green flashing = Activity  
                                   Off = No link |
| 5    | X1-X6 link/port activity | Green = 10G link  
                                   Green flashing = 10G activity  
                                   Amber = 1G link  
                                   Amber flashing = 1G activity  
                                   Off = No link |
| 6    | X7/X8 link/port activity | Green = 10G link  
                                   Green flashing = 10G activity  
                                   Amber = 1G link  
                                   Amber flashing = 1G activity  
                                   Off = No link |
| 7    | X7/X8 shared port activity | Green = Port is active.  
                                   Off = Port is inactive. |
| 8    | X7/X8 port status | Green = Port is configured and operating as an uplink port connected to a data center fabric.  
                                   Amber = Port is operating as a stacking link interconnecting Virtual Connect modules.  
                                   Blue = Port locator (PID)  
                                   Off = Unconfigured |
<table>
<thead>
<tr>
<th>Item</th>
<th>LED description</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>X1/X6 port status</td>
<td>Green = Port is configured and operating as an uplink port connected to a data center fabric. Amber = Port is operating as a stacking link interconnecting Virtual Connect modules. Blue = Port locator (PID) Off = Unconfigured</td>
</tr>
<tr>
<td>10</td>
<td>X1 shared port activity</td>
<td>Green = Port is active. Off = Port is inactive.</td>
</tr>
</tbody>
</table>

Shared port operation

Port X1 (10BASE-CX4) and Port X1 (SFP+)

Port X1 (10BASE-CX4) is multiplexed with Port X1 (SFP+). Either the CX-4 port is active or the SFP+ port is active, but not both. The triangle LED underneath each port indicates which port is active. The SFP+ port always has precedence over the CX4 port.

- If there is a module installed in the SFP+ port, the SFP+ port is the active port.
  - The LED under the SFP+ port is on.
  - The LED under the CX4 port is off.
- If there is no module installed in the SFP+ port, the CX4 port is the active port.
  - The LED under the CX4 port is on.
  - The LED under the SFP+ port is off.

Port X7 and port X8

- Port X7 (SFP+) and port X8 (SFP+) are each multiplexed with an internal 10Gb interface cross-link, which is provided on the enclosure midplane between two horizontally adjacent VC modules to establish stacking links. Either the port is active or the internal cross-link is active, but not both. The triangle LEDs underneath ports X7 and X8 indicate whether the SFP+ port is active or the internal cross-link is active. The SFP+ port always has precedence over the internal cross-link port. Port X7 is shared with internal cross-link 1, and Port X8 is shared with internal cross-link 2.
- If there is a module installed in the SFP+ port, the SFP+ port is the active port. The LED under the SFP+ port is on.
- If there is no module installed in the SFP+ port, and the port has not been configured as an uplink in a VC Ethernet network, then the corresponding internal cross-link is the active port. The LED under the SFP+ port is off.
- If there is no module installed in the SFP+ port, and the port has been configured as an uplink in a VC Ethernet network, then the SFP+ port is the active port. The LED under the SFP+ port is on.
HPE Virtual Connect Flex-10 10Gb Ethernet Module system maintenance switch

<table>
<thead>
<tr>
<th>Function</th>
<th>Switch positions*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default setting</td>
<td>OFF OFF OFF OFF (0000)</td>
</tr>
<tr>
<td>Password/DNS reset</td>
<td>ON OFF OFF OFF (1000)</td>
</tr>
<tr>
<td>FIPS mode</td>
<td>OFF OFF ON OFF (0010)</td>
</tr>
</tbody>
</table>

*Switch positions are from 1 to 4.

See the following sections for function procedures:

- "Resetting the Administrator password and DNS settings (on page 121)"
- "Virtual Connect FIPS mode of operation (on page 32)"

HPE Virtual Connect Flex-10/10D Module components and LEDs

HPE Virtual Connect Flex10/10D Module components

Ports X1 through X10 support Ethernet traffic only.
### Component Identification

<table>
<thead>
<tr>
<th>Item</th>
<th>Component Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>USB 2.0 mini AB port (covered)</td>
<td>For support purposes only</td>
</tr>
<tr>
<td>2</td>
<td>Next button</td>
<td>For support purposes only</td>
</tr>
<tr>
<td>3</td>
<td>Port X1 SFP+ port</td>
<td>1Gb or 10Gb Ethernet</td>
</tr>
<tr>
<td>4</td>
<td>Port X2 SFP+ port</td>
<td>1Gb or 10Gb Ethernet</td>
</tr>
<tr>
<td>5</td>
<td>Port X3 SFP+ port</td>
<td>1Gb or 10Gb Ethernet</td>
</tr>
<tr>
<td>6</td>
<td>Port X4 SFP+ port</td>
<td>1Gb or 10Gb Ethernet</td>
</tr>
<tr>
<td>7</td>
<td>Port X5 SFP+ port</td>
<td>1Gb or 10Gb Ethernet</td>
</tr>
<tr>
<td>8</td>
<td>Port X6 SFP+ port</td>
<td>1Gb or 10Gb Ethernet</td>
</tr>
<tr>
<td>9</td>
<td>Port X7 SFP+ port</td>
<td>1Gb or 10Gb Ethernet</td>
</tr>
<tr>
<td>10</td>
<td>Port X8 SFP+ port</td>
<td>1Gb or 10Gb Ethernet</td>
</tr>
<tr>
<td>11</td>
<td>Port X9 SFP+ port</td>
<td>1Gb or 10Gb Ethernet</td>
</tr>
<tr>
<td>12</td>
<td>Port X10 SFP+ port</td>
<td>1Gb or 10Gb Ethernet</td>
</tr>
</tbody>
</table>

The connectors support 1000BASE-T SFP, 1000BASE-SX SFP, 10GBASE-LR SFP+, 10GBASE-SR SFP+, 10GBASE-LRM SFP+, 10GBASE-T SFP+, and 10GBASE-DAC SFP+ pluggable Ethernet transceiver modules. For more information, see the Virtual Connect QuickSpecs on the Hewlett Packard Enterprise website (http://www.hpe.com/info/vc/manuals).

### HPE Virtual Connect Flex10/10D Module LEDs

#### Item LED Description

<table>
<thead>
<tr>
<th>Item</th>
<th>LED Description</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Module locator (UID)</td>
<td>Blue = Module ID is selected. Off = Module ID is not selected.</td>
</tr>
<tr>
<td>2</td>
<td>Module status</td>
<td>Green = Normal operation Amber = Degraded condition Amber flashing = Fault condition Off = Power off</td>
</tr>
<tr>
<td>3</td>
<td>X1–X10 link/port activity</td>
<td>Green = 10G link Green flashing = 10G activity Amber = 1G link Amber flashing = 1G activity Off = No link</td>
</tr>
<tr>
<td>4</td>
<td>X1–X10 port status</td>
<td>Green = Port is configured and operating as an uplink port connected to a data center fabric. Amber = Port is operating as a stacking link interconnecting Virtual Connect modules. Blue = Port locator (PID) Off = Unconfigured</td>
</tr>
</tbody>
</table>
HPE Virtual Connect Flex10/10D Module system maintenance switch

<table>
<thead>
<tr>
<th>Function</th>
<th>Switch positions*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default setting</td>
<td>OFF OFF OFF OFF (0000)</td>
</tr>
<tr>
<td>Password/DNS reset</td>
<td>ON OFF OFF OFF (1000)</td>
</tr>
<tr>
<td>FIPS mode</td>
<td>OFF OFF ON OFF (0010)</td>
</tr>
</tbody>
</table>

*Switch positions are from 1 to 4.

See the following sections for function procedures:

- "Resetting the Administrator password and DNS settings (on page 121)"
- "Virtual Connect FIPS mode of operation (on page 32)"
HPE Virtual Connect FlexFabric 10Gb/24-port Module components and LEDs

HPE Virtual Connect FlexFabric 10Gb/24-port Module components

Ports X1 through X4 support Ethernet or Fibre Channel traffic. Ports X5 through X8 support Ethernet traffic only. Ports X7 and X8 are multiplexed with the internal 10Gb interface cross-link.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Capable speed</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>USB 2.0 mini AB port (covered)</td>
<td>—</td>
</tr>
<tr>
<td>2</td>
<td>Next button</td>
<td>—</td>
</tr>
<tr>
<td>3</td>
<td>Port X1 SFP+ port*</td>
<td>10Gb Ethernet 2Gb, 4Gb, or 8Gb FC</td>
</tr>
<tr>
<td>4</td>
<td>Port X2 SFP+ port*</td>
<td>10Gb Ethernet 2Gb, 4Gb, or 8Gb FC</td>
</tr>
<tr>
<td>5</td>
<td>Port X3 SFP+ port*</td>
<td>10Gb Ethernet 2Gb, 4Gb, or 8Gb FC</td>
</tr>
<tr>
<td>6</td>
<td>Port X4 SFP+ port*</td>
<td>10Gb Ethernet 2Gb, 4Gb, or 8Gb FC</td>
</tr>
<tr>
<td>7</td>
<td>Port X5 SFP+ port**</td>
<td>1Gb or 10Gb Ethernet</td>
</tr>
<tr>
<td>8</td>
<td>Port X6 SFP+ port**</td>
<td>1Gb or 10Gb Ethernet</td>
</tr>
<tr>
<td>9</td>
<td>Port X7 SFP+ port**</td>
<td>1Gb or 10Gb Ethernet</td>
</tr>
<tr>
<td>10</td>
<td>Port X8 SFP+ port**</td>
<td>1Gb or 10Gb Ethernet</td>
</tr>
</tbody>
</table>

*Supports 10GBASE-LR SFP+, 10GBASE-SR SFP+, or 10GBASE-DAC SFP+ pluggable Ethernet transceiver modules and 2/4/8Gb SFP+ pluggable Fibre Channel transceiver modules

**Supports 1000BASE-T-SFP, 1000BASE-SX-SFP, 1000BASE-RJ45-SFP, 10GBASE-LR SFP+, 10GBASE-SR SFP+, 10GBASE-LRM SFP+, 10GBASE-T SFP+, and 10GBASE-DAC SFP+ pluggable Ethernet transceiver modules
<table>
<thead>
<tr>
<th>Item</th>
<th>LED description</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Module locator (UID)</td>
<td>Blue = Module ID is selected. Off = Module ID is not selected.</td>
</tr>
<tr>
<td>2</td>
<td>Module status</td>
<td>Green = Normal operation Amber = Degraded condition Amber flashing = Fault condition Off = Power off</td>
</tr>
<tr>
<td>3</td>
<td>X1-X4 port status</td>
<td>Ethernet mode Green = Port is configured and operating as an uplink port connected to a data center fabric. Amber = Port is operating as a stacking link interconnecting Virtual Connect modules. Amber flashing = SFP module is invalid for Ethernet mode. Purple flashing = Port is configured as a mirror to port. Blue = Port locator (PID) Off = Unconfigured</td>
</tr>
<tr>
<td>4</td>
<td>X1-X4 link/port activity</td>
<td>Ethernet mode Green = 10GbE link Green flashing = 10GbE activity Off = No link</td>
</tr>
<tr>
<td>5</td>
<td>6</td>
<td>7</td>
</tr>
<tr>
<td>11</td>
<td>X5-X8 port status</td>
<td>Green = Port is configured and operating as an uplink port connected to a data center fabric.</td>
</tr>
<tr>
<td>Item</td>
<td>LED description</td>
<td>Status</td>
</tr>
<tr>
<td>------</td>
<td>----------------</td>
<td>--------</td>
</tr>
<tr>
<td>15</td>
<td></td>
<td>fabric.</td>
</tr>
<tr>
<td>17</td>
<td></td>
<td>Amber = Port is operating as a stacking link interconnecting Virtual Connect modules. Amber flashing = SFP module is invalid for Ethernet mode. Purple flashing = Port is configured as a mirror to port. Blue = Port locator (PID) Off = Unconfigured</td>
</tr>
<tr>
<td>12</td>
<td>X5-X8 link/port activity</td>
<td>Green = 10GbE link Green flashing = 10GbE activity Amber = 1GbE link Amber flashing = 1GbE activity Off = No link</td>
</tr>
<tr>
<td>14</td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td></td>
<td></td>
</tr>
<tr>
<td>18</td>
<td></td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>X8 shared port indicator</td>
<td>Green = Port is multiplexed to the external SFP+ connector. Off = Port is multiplexed to the internal 10Gb interface crosslink.</td>
</tr>
<tr>
<td>20</td>
<td>X7 shared port indicator</td>
<td>Green = Port is multiplexed to the external SFP+ connector. Off = Port is multiplexed to the internal 10Gb interface crosslink.</td>
</tr>
<tr>
<td>21</td>
<td>Fibre Channel mode indicators</td>
<td>Green = The port is configured for Fibre Channel traffic. Off = The port is not configured for this mode.</td>
</tr>
<tr>
<td>23</td>
<td></td>
<td></td>
</tr>
<tr>
<td>26</td>
<td></td>
<td></td>
</tr>
<tr>
<td>28</td>
<td></td>
<td></td>
</tr>
<tr>
<td>22</td>
<td>Ethernet mode indicators</td>
<td>Green = The port is configured for Ethernet traffic. Off = The port is not configured for this mode.</td>
</tr>
<tr>
<td>24</td>
<td></td>
<td></td>
</tr>
<tr>
<td>25</td>
<td></td>
<td></td>
</tr>
<tr>
<td>27</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Function Switch positions*

<table>
<thead>
<tr>
<th>Function</th>
<th>Switch positions*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default setting</td>
<td>OFF OFF OFF OFF (0000)</td>
</tr>
<tr>
<td>Password/DNS reset</td>
<td>ON OFF OFF OFF (1000)</td>
</tr>
<tr>
<td>FIPS mode</td>
<td>OFF OFF ON OFF (0010)</td>
</tr>
</tbody>
</table>

*Switch positions are from 1 to 4.

See the following sections for function procedures:

- "Resetting the Administrator password and DNS settings (on page 121)"
HPE Virtual Connect FlexFabric-20/40 F8 Module components and LEDs

**HPE Virtual Connect FlexFabric-20/40 F8 Module components**

Ports Q1 through Q4 support Ethernet. Ports X1 through X8 support Ethernet and Fibre Channel traffic. Port pairs X5/X6 and X7/X8 carry a single type of network traffic, either Ethernet or Fibre Channel.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Capable speed</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Port Q1 QSFP+ port*</td>
<td>10Gb, 40Gb or 4x10Gb</td>
</tr>
<tr>
<td>2</td>
<td>Port Q2 QSFP+ port*</td>
<td>10Gb, 40Gb or 4x10Gb</td>
</tr>
<tr>
<td>3</td>
<td>Port Q3 QSFP+ port*</td>
<td>10Gb, 40Gb or 4x10Gb</td>
</tr>
<tr>
<td>4</td>
<td>Port Q4 QSFP+ port*</td>
<td>10Gb, 40Gb or 4x10Gb</td>
</tr>
<tr>
<td>5</td>
<td>Next button</td>
<td>Toggles port LED mode through PID, L/A, FC and Ethernet. See &quot;Port LED modes when toggled using the Next button (on page 112).&quot;</td>
</tr>
<tr>
<td>6</td>
<td>USB 2.0 mini AB port(covered)</td>
<td>—</td>
</tr>
<tr>
<td>7</td>
<td>Port X1 SFP+ port**</td>
<td>1Gb, 10Gb Ethernet, 2Gb, 4Gb, or 8Gb FC</td>
</tr>
<tr>
<td>8</td>
<td>Port X2 SFP+ port**</td>
<td>1Gb, 10Gb Ethernet, 2Gb, 4Gb, or 8Gb FC</td>
</tr>
<tr>
<td>9</td>
<td>Port X3 SFP+ port**</td>
<td>1Gb, 10Gb Ethernet, 2Gb, 4Gb, or 8Gb FC</td>
</tr>
<tr>
<td>10</td>
<td>Port X4 SFP+ port**</td>
<td>1Gb, 10Gb Ethernet, 2Gb, 4Gb, or 8Gb FC</td>
</tr>
<tr>
<td>11</td>
<td>Port X8 SFP+ port** †</td>
<td>1Gb, 10Gb Ethernet, 2Gb, 4Gb, or 8Gb FC</td>
</tr>
<tr>
<td>12</td>
<td>Port X7 SFP+ port** †</td>
<td>1Gb, 10Gb Ethernet, 2Gb, 4Gb, or 8Gb FC</td>
</tr>
<tr>
<td>13</td>
<td>Port X6 SFP+ port** †</td>
<td>1Gb, 10Gb Ethernet, 2Gb, 4Gb, or 8Gb FC</td>
</tr>
<tr>
<td>14</td>
<td>Port X5 SFP+ port** †</td>
<td>1Gb, 10Gb Ethernet, 2Gb, 4Gb, or 8Gb FC</td>
</tr>
</tbody>
</table>
Port LED modes when toggled using the Next button

The port status LEDs are in one of four modes, indicated by the mode LED that is lit green. Use the Next button to toggle between these modes.

- **PID mode**—The PID mode LED is lit green and the port LEDs are amber for Enet stacking links or an FC port is not online or logged in, green for Enet uplinks or an FC port is connected to a switch, light purple for Ethernet mirror-to-port, and red if the port has an error.
- **L/A mode**—The L/A mode LED is lit green and the color of the port LEDs indicates speed, and activity when flashing.
- **Ethernet mode**—The Ethernet mode LED is lit green. The port LEDs are solid green on ports configured for Ethernet. All other port LEDs are off.
- **FC mode**—The FC mode LED is lit green. The port LEDs are solid green on ports configured for FC. All other port LEDs are off.

HPE Virtual Connect FlexFabric-20/40 F8 Module LEDs

<table>
<thead>
<tr>
<th>Item</th>
<th>LED description</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Module locator (UID)</td>
<td>Blue = Module ID is selected. Off = Module ID is not selected.</td>
</tr>
<tr>
<td>2</td>
<td>Module status</td>
<td>Green = Normal operation Amber = Degraded condition Amber flashing = Fault condition Off = Power off</td>
</tr>
<tr>
<td>3</td>
<td>L/A</td>
<td>Green = Port LEDs are in Link/Activity mode</td>
</tr>
<tr>
<td>4</td>
<td>PID</td>
<td>Green = Port LEDs are in Port Identifier mode</td>
</tr>
<tr>
<td>5</td>
<td>FC Mode</td>
<td>Green = Port LEDs are in FC mode</td>
</tr>
<tr>
<td>6</td>
<td>Ethernet</td>
<td>Green = Port LEDs are in Ethernet mode</td>
</tr>
<tr>
<td>Item</td>
<td>LED description</td>
<td>Status</td>
</tr>
<tr>
<td>------</td>
<td>----------------</td>
<td>--------</td>
</tr>
</tbody>
</table>
| 7    | X1-X8 port status | **PID mode**  
The PID mode LED is lit green. Port LEDs:  
Amber = The port is configured as an Enet stacking link or an FC port is not on-line or logged in.  
Green = The port is configured as an Enet uplink port or an FC port connected to a switch  
Light Purple = The port is configured as an Enet mirror-to-port.  
Red = The port has an error such as an invalid or unsupported pluggable module detected  
Blue = Port identification (locator) |
| 8    |                |        |
| 9    |                |        |
| 10   |                |        |
| 11   |                |        |
| 12   |                |        |
| 13   |                |        |
| 14   |                |        |
| 15   | Qx port status | **Fibre Channel mode**  
Green = Port is configured for FC.  
Off = Port is not configured for FC. **Ethernet mode**  
Green = Port is configured for Ethernet.  
Off = Port is not configured for Ethernet. |
<p>| 16   |                |        |
| 17   |                |        |
| 18   |                |        |</p>
<table>
<thead>
<tr>
<th>Item</th>
<th>LED description</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port LEDs:</td>
<td>Green = The port is configured and operating as an uplink port connected to a</td>
<td>data center fabric at 10GbE.</td>
</tr>
<tr>
<td></td>
<td>Green flashing = Port activity at 10GbE.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Purple = The port is configured and operating as an uplink port connected to a</td>
<td>data center fabric at 40GbE.</td>
</tr>
<tr>
<td></td>
<td>Purple flashing = Port activity at 40GbE.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Red = Port error, invalid or unsupported pluggable module detected.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Off = No link</td>
<td></td>
</tr>
<tr>
<td>Fibre Channel mode</td>
<td>Off = Port does not support FC.</td>
<td></td>
</tr>
<tr>
<td>Ethernet mode</td>
<td>Green = Port is configured for Ethernet.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Off = Port is not configured for Ethernet.</td>
<td></td>
</tr>
</tbody>
</table>

**HPE Virtual Connect FlexFabric-20/40 F8 Module system maintenance switch**

<table>
<thead>
<tr>
<th>Function</th>
<th>Switch positions*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default setting</td>
<td>OFF OFF OFF OFF (0000)</td>
</tr>
<tr>
<td>Password/DNS reset</td>
<td>ON OFF OFF OFF (1000)</td>
</tr>
<tr>
<td>FIPS mode</td>
<td>OFF OFF ON OFF (0010)</td>
</tr>
</tbody>
</table>

*Switch positions are from 1 to 4.

See the following sections for function procedures:

- "Resetting the Administrator password and DNS settings (on page 121)"
- "Virtual Connect FIPS mode of operation (on page 32)"
HPE Virtual Connect 8Gb 24-Port Fibre Channel Module components and LEDs

HPE VC 8Gb 24-Port FC Module components

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Device bays supported when in default configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>SFP/SFP+ ports supporting 8Gb SFP+ and 4Gb SFP transceivers</td>
<td>1-16</td>
</tr>
<tr>
<td>2</td>
<td>Reset button (recessed)</td>
<td>—</td>
</tr>
</tbody>
</table>
HPE VC 8Gb 24-Port FC Module LEDs

<table>
<thead>
<tr>
<th>Item</th>
<th>LED description</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Module locator (UID)</td>
<td>Blue = Module ID selected&lt;br&gt;Off = Module ID not selected</td>
</tr>
<tr>
<td>2</td>
<td>Module status</td>
<td>Green = Normal operation&lt;br&gt;Amber = Degraded condition&lt;br&gt;Off = Power off</td>
</tr>
<tr>
<td>3</td>
<td>Port link/activity</td>
<td>Green = Port is online, but not passing traffic&lt;br&gt;Green slow flashing = Port is online and not logged in&lt;br&gt;Green flickering = Port is online passing traffic&lt;br&gt;Amber = Port has light or signal, but not yet online&lt;br&gt;Amber slow flashing = Port is disabled (NPIV not enabled or supported on external devices)&lt;br&gt;Amber fast flashing = Port is faulty&lt;br&gt;Off = No power or signal on the port</td>
</tr>
<tr>
<td>4</td>
<td>Port indicator</td>
<td>Green = Logged in to an external Fibre Channel switch port&lt;br&gt;Off = Port down, offline, no sync, or error</td>
</tr>
<tr>
<td>5</td>
<td>Port speed indicator</td>
<td>Off = 2 Gb&lt;br&gt;Green = 4 Gb&lt;br&gt;Amber = 8 Gb</td>
</tr>
</tbody>
</table>
HPE VC 8Gb 24-Port FC Module system maintenance switch

<table>
<thead>
<tr>
<th>Switch</th>
<th>Default</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Off</td>
<td>Reserved (must be in &quot;Off&quot; position)</td>
</tr>
<tr>
<td>2</td>
<td>Off</td>
<td>Reserved (must be in &quot;Off&quot; position)</td>
</tr>
<tr>
<td>3</td>
<td>Off</td>
<td>Reserved (must be in &quot;Off&quot; position)</td>
</tr>
<tr>
<td>4</td>
<td>Off</td>
<td>Off = Module debug and test interface is inaccessible. On = Module debug and test interface is accessible.</td>
</tr>
</tbody>
</table>

When part of a Virtual Connect domain, Virtual Connect Manager overrides any system maintenance switch settings.
HPE Virtual Connect 8Gb 20-Port Fibre Channel Module components and LEDs

HPE VC 8Gb 20-Port FC Module components

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Device bays supported in default configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>SFP/SFP+ ports supporting 8Gb SFP+ and 4Gb SFP transceivers</td>
<td>1-16 (c7000) 1-8 (c3000)</td>
</tr>
<tr>
<td>2</td>
<td>Reset button (recessed)</td>
<td>—</td>
</tr>
</tbody>
</table>

In the default configuration, before a Virtual Connect domain is created, all uplink ports are grouped into an uplink port group and dynamically distribute connectivity from all server blades.
# HPE VC 8Gb 20-Port FC Module LEDs

<table>
<thead>
<tr>
<th>Item</th>
<th>LED description</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Module locator (UID)</td>
<td>Blue = Module ID is selected. Off = Module ID is not selected.</td>
</tr>
<tr>
<td>2</td>
<td>Module status</td>
<td>Green = Normal operation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Amber = Degraded condition</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Off = Power off</td>
</tr>
<tr>
<td>3</td>
<td>Logged in</td>
<td>Green = Logged in to an external Fibre Channel switch port</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Off = Port down, offline, no sync, or error</td>
</tr>
<tr>
<td>4</td>
<td>Activity</td>
<td>Green flashing (variable) = Link activity</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Green flashing (1 Hz) = External fabric switch does not support NPIV.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Off = No activity</td>
</tr>
<tr>
<td>5</td>
<td>Port indicator</td>
<td>Green = Port is configured as the uplink for one or more server HBAs.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Amber = Port is not configured. Blue = Port is selected.</td>
</tr>
</tbody>
</table>
HPE VC 8Gb 20-Port FC Module system maintenance switch

<table>
<thead>
<tr>
<th>Switch</th>
<th>Default</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Off</td>
<td>Reserved</td>
</tr>
<tr>
<td>2</td>
<td>Off</td>
<td>Reserved</td>
</tr>
<tr>
<td>3</td>
<td>Off</td>
<td>Reserved</td>
</tr>
<tr>
<td>4</td>
<td>Off</td>
<td>Reserved</td>
</tr>
</tbody>
</table>

When part of a Virtual Connect domain, Virtual Connect Manager overrides any system maintenance switch settings.

HPE Virtual Connect 16Gb 24-Port FC Module components and LEDs

HPE VC 16Gb 24-Port FC Module components

<table>
<thead>
<tr>
<th>Item</th>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>SFP+ ports 1–8</td>
<td>4Gb, 8Gb, or 16Gb Fibre Channel</td>
</tr>
<tr>
<td>2</td>
<td>Reset button (recessed)</td>
<td>Resets the module</td>
</tr>
</tbody>
</table>

Only short-wave B-series transceivers are supported:
HPE B-series 8Gb SFP+ FC pluggable
HPE B-series 16Gb SFP+ FC pluggable
For a complete list of supported transceivers, see the product QuickSpecs.

HPE VC 16Gb 24-Port FC Module LEDs

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Port ID LED</td>
<td>Solid green = The port is configured as an uplink port by VCM. Off = The port is not configured.</td>
</tr>
<tr>
<td>2</td>
<td>Port status LED</td>
<td>Solid green = The port is online, but not passing traffic. Flashing green = The port is online, but not logged in. Flickering green = The port is online and passing traffic. Solid amber = A signal is detected, but the port is not yet online. Flashing amber (slow) = The port is disabled.* Flashing amber (fast) = The port is faulty or an invalid transceiver is installed. Off = No power or signal is detected.</td>
</tr>
<tr>
<td>3</td>
<td>Health LED</td>
<td>Green = Normal operation Amber = Degraded operation Off = No power</td>
</tr>
<tr>
<td>4</td>
<td>UID LED</td>
<td>Solid blue = Module selected or being managed Off = Module not selected or being managed</td>
</tr>
</tbody>
</table>

*Be sure NPIV is enabled in the upstream switch and the port is not manually disabled.

HPE VC 16Gb 24-Port FC Module system maintenance switch
No maintenance switch exists for this module.

Resetting the Administrator password and DNS settings
To return the VC-Enet module to factory default settings for the Administrator password and DNS settings, you must access the system maintenance switch. For switch locations, see the appropriate module system maintenance switch information.

When the VC-Enet module system maintenance switch 1 is in the ON position, the following actions occur:
• The firmware restores the Administrator account password and DNS Settings to the factory defaults listed on the module label (without disturbing any other local user accounts).

• The VC-Enet module management console displays the Administrator account password. To access the console, see the HPE BladeSystem Onboard Administrator User Guide (http://www.hpe.com/info/BladeSystemOA-UG).

While switch 1 is in the ON position and reserved switches are in the OFF position, passwords are restored during each power-up sequence, but changes are not allowed.

After switch 1 is returned to the OFF position, the following conditions exist:

• Users with appropriate privileges can change the Administrator password.

• The VC-Enet module management console no longer displays the Administrator password.

To recover a password:

1. Remove the Virtual Connect Ethernet module from interconnect bay 1.
2. Remove the access panel from the Virtual Connect Ethernet module.
3. Set switch 1 to the ON position. Be sure that all other switches remain in the OFF position.
4. Install the access panel.
5. Install the Virtual Connect Ethernet module into bay 1 and allow the module to power up and reach a fully booted and operational state (approximately 1 minute).
6. Remove the Virtual Connect Ethernet module from interconnect bay 2.
   This action forces the module in interconnect bay 1 to run the active VC Manager. Because switch 1 is set, the Administrator password remains at the factory default for interconnect bay 1 (not overwritten by the change of state because of the failover).
7. Wait to ensure that the VC Manager has had time to become active on the module in interconnect bay 1. Log in to the VC Manager to confirm it is active.
8. Insert the Virtual Connect Ethernet module into interconnect bay 2 and allow the module to power on and reach a fully booted and operational state (approximately 1 minute).
9. Remove the Virtual Connect Ethernet module from interconnect bay 1.
10. Remove the access panel from the Virtual Connect Ethernet module.
11. Set switch 1 to the OFF position. Ensure that all other switches remain in the OFF position.
12. Install the access panel.
13. Install the Virtual Connect Ethernet module into interconnect bay 1 and allow the module to power up and reach a fully booted and operation state (approximately 1 minute).
14. Log in to the active VC Manager. Use the factory default user name and password to log in to the module, regardless of its location in interconnect bay 1 or interconnect bay 2.
15. Change the Administrator password.
Warranty and regulatory information

Warranty information

HPE ProLiant and x86 Servers and Options  
(https://www.hpe.com/support/ProLiantServers-Warranties)
HPE Enterprise Servers (https://www.hpe.com/support/EnterpriseServers-Warranties)
HPE Storage Products (https://www.hpe.com/support/Storage-Warranties)

Regulatory information

Safety and regulatory compliance


Belarus Kazakhstan Russia marking

Manufacturer and Local Representative Information

Manufacturer information:
Hewlett Packard Enterprise Company, 3000 Hanover Street, Palo Alto, CA 94304 U.S.

Local representative information Russian:

- **Russia:**
  ООО «Хьюлетт Паккард Энтерпрайз», Российская Федерация, 125171, г. Москва, Ленинградское шоссе, 16А, стр.3, Телефон/факс: +7 495 797 35 00

- **Belarus:**
  ИООО «Хьюлетт-Паккард Бел», Республика Беларусь, 220030, г. Минск, ул. Интернациональная, 36-1, Телефон/факс: +375 17 392 28 20

- **Kazakhstan:**
  ТОО «Хьюлетт-Паккард (К)», Республика Казахстан, 050040, г. Алматы, Бостандыкский район, проспект Аль-Фараби, 77/7, Телефон/факс: + 7 727 355 35 52
Local representative information Kazakh:

- **Russia:**
  ЖШС "Хьюлетт Паккард Энтерпрайз", Ресей Федерациясы, 125171, Мәскеу, Ленинград тас жолы, 16А блок 3, Телефон/факс: +7 495 797 35 00

- **Belarus:**
  «HEWLETT-PACKARD Bel» ЖШС, Беларусь Республикасы, 220030, Минск к., Интернациональная кешеси, 36/1, Телефон/факс: +375 17 392 28 20

- **Kazakhstan:**
  ЖШС «Хьюлетт-Паккард (Қ)», Қазақстан Республикасы, 050040, Алматы к., Бостандык ауданы, Әл-Фараби даяң ылы, 77/7, Телефон/факс: +7 727 355 35 52

**Manufacturing date:**
The manufacturing date is defined by the serial number.

CCSYWWZZZZ (serial number format for this product)

Valid date formats include:

- **YWW,** where Y indicates the year counting from within each new decade, with 2000 as the starting point; for example, 238: 2 for 2002 and 38 for the week of September 9. In addition, 2010 is indicated by 0, 2011 by 1, 2012 by 2, 2013 by 3, and so forth.

- **YYWW,** where YY indicates the year, using a base year of 2000; for example, 0238: 02 for 2002 and 38 for the week of September 9.

**Turkey RoHS material content declaration**

Türkiye Cumhuriyeti: EEE Yönetmeligine Uygundur

**Ukraine RoHS material content declaration**

Обладнання відповідає вимогам Технічного регламенту щодо обмеження використання деяких небезпечних речовин в електричному та електронному обладнанні, затвердженого постановою Кабінету Міністрів України від 3 грудня 2008 № 1057
Electrostatic discharge

Preventing electrostatic discharge

To prevent damaging the system, be aware of the precautions you need to follow when setting up the system or handling parts. A discharge of static electricity from a finger or other conductor may damage system boards or other static-sensitive devices. This type of damage may reduce the life expectancy of the device.

To prevent electrostatic damage:

- Avoid hand contact by transporting and storing products in static-safe containers.
- Keep electrostatic-sensitive parts in their containers until they arrive at static-free workstations.
- Place parts on a grounded surface before removing them from their containers.
- Avoid touching pins, leads, or circuitry.
- Always be properly grounded when touching a static-sensitive component or assembly.

Grounding methods to prevent electrostatic discharge

Several methods are used for grounding. Use one or more of the following methods when handling or installing electrostatic-sensitive parts:

- Use a wrist strap connected by a ground cord to a grounded workstation or computer chassis. Wrist straps are flexible straps with a minimum of 1 megohm ±10 percent resistance in the ground cords. To provide proper ground, wear the strap snug against the skin.
- Use heel straps, toe straps, or boot straps at standing workstations. Wear the straps on both feet when standing on conductive floors or dissipating floor mats.
- Use conductive field service tools.
- Use a portable field service kit with a folding static-dissipating work mat.

If you do not have any of the suggested equipment for proper grounding, have an authorized reseller install the part.

For more information on static electricity or assistance with product installation, contact an authorized reseller.
Support and other resources

Accessing Hewlett Packard Enterprise Support

- For live assistance, go to the Contact Hewlett Packard Enterprise Worldwide website ([http://www.hpe.com/assistance](http://www.hpe.com/assistance)).
- To access documentation and support services, go to the Hewlett Packard Enterprise Support Center website ([http://www.hpe.com/support/hpesc](http://www.hpe.com/support/hpesc)).

Information to collect

- Technical support registration number (if applicable)
- Product name, model or version, and serial number
- Operating system name and version
- Firmware version
- Error messages
- Product-specific reports and logs
- Add-on products or components
- Third-party products or components

Accessing updates

- Some software products provide a mechanism for accessing software updates through the product interface. Review your product documentation to identify the recommended software update method.
- To download product updates, go to either of the following:
  - Hewlett Packard Enterprise Support Center Get connected with updates page ([http://www.hpe.com/support/e-updates](http://www.hpe.com/support/e-updates))

**IMPORTANT:** Access to some updates might require product entitlement when accessed through the Hewlett Packard Enterprise Support Center. You must have an HP Passport set up with relevant entitlements.

Websites

- Hewlett Packard Enterprise Information Library ([http://www.hpe.com/info/enterprise/docs](http://www.hpe.com/info/enterprise/docs))
- Contact Hewlett Packard Enterprise Worldwide ([http://www.hpe.com/assistance](http://www.hpe.com/assistance))
• Subscription Service/Support Alerts ([http://www.hpe.com/support/e-updates](http://www.hpe.com/support/e-updates))
• Software Depot ([http://www.hpe.com/support/softwaredepot](http://www.hpe.com/support/softwaredepot))
• Customer Self Repair ([http://www.hpe.com/support/selfrepair](http://www.hpe.com/support/selfrepair))
• Insight Remote Support ([http://www.hpe.com/info/insightremotesupport/docs](http://www.hpe.com/info/insightremotesupport/docs))
• Serviceguard Solutions for HP-UX ([http://www.hpe.com/info/hpux-serviceguard-docs](http://www.hpe.com/info/hpux-serviceguard-docs))
• Single Point of Connectivity Knowledge (SPOCK) Storage compatibility matrix ([http://www.hpe.com/storage/spock](http://www.hpe.com/storage/spock))
• Storage white papers and analyst reports ([http://www.hpe.com/storage/whitepapers](http://www.hpe.com/storage/whitepapers))

Customer Self Repair

Hewlett Packard Enterprise products are designed with many Customer Self Repair (CSR) parts to minimize repair time and allow for greater flexibility in performing defective parts replacement. If during the diagnosis period Hewlett Packard Enterprise (or Hewlett Packard Enterprise service providers or service partners) identifies that the repair can be accomplished by the use of a CSR part, Hewlett Packard Enterprise will ship that part directly to you for replacement. There are two categories of CSR parts:

- **Mandatory**—Parts for which customer self repair is mandatory. If you request Hewlett Packard Enterprise to replace these parts, you will be charged for the travel and labor costs of this service.
- **Optional**—Parts for which customer self repair is optional. These parts are also designed for customer self repair. If, however, you require that Hewlett Packard Enterprise replace them for you, there may or may not be additional charges, depending on the type of warranty service designated for your product.

**NOTE:** Some Hewlett Packard Enterprise parts are not designed for customer self repair. In order to satisfy the customer warranty, Hewlett Packard Enterprise requires that an authorized service provider replace the part. These parts are identified as "No" in the Illustrated Parts Catalog.

Based on availability and where geography permits, CSR parts will be shipped for next business day delivery. Same day or four-hour delivery may be offered at an additional charge where geography permits. If assistance is required, you can call the Hewlett Packard Enterprise Support Center and a technician will help you over the telephone. Hewlett Packard Enterprise specifies in the materials shipped with a replacement CSR part whether a defective part must be returned to Hewlett Packard Enterprise. In cases where it is required to return the defective part to Hewlett Packard Enterprise, you must ship the defective part back to Hewlett Packard Enterprise within a defined period of time, normally five (5) business days. The defective part must be returned with the associated documentation in the provided shipping material. Failure to return the defective part may result in Hewlett Packard Enterprise billing you for the replacement. With a customer self repair, Hewlett Packard Enterprise will pay all shipping and part return costs and determine the courier/carrier to be used.

For more information about the Hewlett Packard Enterprise CSR program, contact your local service provider. For the North American program, go to the Hewlett Packard Enterprise CSR website ([http://www.hpe.com/support/selfrepair](http://www.hpe.com/support/selfrepair)).

Réparation par le client (CSR)

Les produits Hewlett Packard Enterprise comportent de nombreuses pièces CSR (Customer Self Repair = réparation par le client) afin de minimiser les délais de réparation et faciliter le remplacement des pièces défectueuses. Si pendant la période de diagnostic, Hewlett Packard Enterprise (ou ses partenaires ou mainteneurs agrées) détermine que la réparation peut être effectuée à l'aide d'une pièce CSR, Hewlett Packard Enterprise vous l'envoie directement. Il existe deux catégories de pièces CSR :
• **Obligatoire**—Pièces pour lesquelles la réparation par le client est obligatoire. Si vous demandez à Hewlett Packard Enterprise de remplacer ces pièces, les coûts de déplacement et main d'œuvre du service vous seront facturés.

• **Facultatif**—Pièces pour lesquelles la réparation par le client est facultative. Ces pièces sont également conçues pour permettre au client d'effectuer lui-même la réparation. Toutefois, si vous demandez à Hewlett Packard Enterprise de remplacer ces pièces, l'intervention peut ou non vous être facturée, selon le type de garantie applicable à votre produit.

**REMARQUE**: Certaines pièces Hewlett Packard Enterprise ne sont pas conçues pour permettre au client d'effectuer lui-même la réparation. Pour que la garantie puisse s'appliquer, Hewlett Packard Enterprise exige que le remplacement de la pièce soit effectué par un Mainteneur Agréé. Ces pièces sont identifiées par la mention "Non" dans le Catalogue illustré.

Les pièces CSR sont livrées le jour ouvré suivant, dans la limite des stocks disponibles et selon votre situation géographique. Si votre situation géographique le permet et que vous demandez une livraison le jour même ou dans les 4 heures, celle-ci vous sera facturée. Pour toute assistance, appelez le Centre d’assistance Hewlett Packard Enterprise pour qu'un technicien vous aide au téléphone. Dans les documents envoyés avec la pièce de rechange CSR, Hewlett Packard Enterprise précise s'il est nécessaire de lui retourner la pièce défectueuse. Si c'est le cas, vous devez le faire dans le délai indiqué, généralement cinq (5) jours ouvrés. La pièce et sa documentation doivent être retournées dans l'emballage fourni. Si vous ne retournez pas la pièce défectueuse, Hewlett Packard Enterprise se réserve le droit de vous facturer les coûts de remplacement. Dans le cas d'une pièce CSR, Hewlett Packard Enterprise supporte l'ensemble des frais d'expédition et de retour, et détermine la société de courses ou le transporteur à utiliser.

Pour plus d'informations sur le programme CSR de Hewlett Packard Enterprise, contactez votre Mainteneur Agréé local. Pour plus d'informations sur ce programme en Amérique du Nord, consultez le site Web Hewlett Packard Enterprise ([http://www.hpe.com/support/selfrepair](http://www.hpe.com/support/selfrepair)).

Riparazione da parte del cliente

Per abbreviare i tempi di riparazione e garantire una maggiore flessibilità nella sostituzione di parti difettose, i prodotti Hewlett Packard Enterprise sono realizzati con numerosi componenti che possono essere riparati direttamente dal cliente (CSR, Customer Self Repair). Se in fase di diagnostica Hewlett Packard Enterprise (o un centro di servizi o di assistenza Hewlett Packard Enterprise) identifica il guasto come riparabile mediante un ricambio CSR, Hewlett Packard Enterprise lo spedirà direttamente al cliente per la sostituzione. Vi sono due categorie di parti CSR:

• **Obbligatorie**—Parti che devono essere necessariamente riparate dal cliente. Se il cliente ne affida la riparazione ad Hewlett Packard Enterprise, deve sostenere le spese di spedizione e di manodopera per il servizio.

• **Opzionali**—Parti la cui riparazione da parte del cliente è facoltativa. Si tratta comunque di componenti progettati per questo scopo. Se tuttavia il cliente ne richiede la sostituzione ad Hewlett Packard Enterprise, potrebbe dover sostenere spese addizionali a seconda del tipo di garanzia previsto per il prodotto.

**NOTA**: alcuni componenti Hewlett Packard Enterprise non sono progettati per la riparazione da parte del cliente. Per rispettare la garanzia, Hewlett Packard Enterprise richiede che queste parti siano sostituite da un centro di assistenza autorizzato. Tali parti sono identificate da un "No" nel Catalogo illustrato dei componenti.

In base alla disponibilità e alla località geografica, le parti CSR vengono spedite con consegna entro il giorno lavorativo seguente. La consegna nel giorno stesso o entro quattro ore è offerta con un supplemento di costo solo in alcune zone. In caso di necessità si può richiedere l'assistenza telefonica di un addetto del centro di supporto tecnico Hewlett Packard Enterprise. Nel materiale fornito con una parte di ricambio CSR, Hewlett Packard Enterprise specifica se il cliente deve restituire dei componenti. Qualora sia richiesta la resa ad Hewlett Packard Enterprise del componente difettoso, lo si deve spedire ad Hewlett Packard Enterprise entro un determinato periodo di tempo, generalmente cinque (5) giorni lavorativi. Il componente difettoso deve essere restituito con la documentazione associata nell'imbollo di
Customer Self Repair

Hewlett Packard Enterprise Produkte enthalten viele CSR-Teile (Customer Self Repair), um Reparaturzeiten zu minimieren und höhere Flexibilität beim Austausch defekter Bauteile zu ermöglichen. Wenn Hewlett Packard Enterprise (oder ein Hewlett Packard Enterprise Servicepartner) bei der Diagnose feststellt, dass das Produkt mithilfe eines CSR-Teils repariert werden kann, sendet Ihnen Hewlett Packard Enterprise dieses Bauteil zum Austausch direkt zu. CSR-Teile werden in zwei Kategorien unterteilt:

- **Zwingend**—Teile, für die das Customer Self Repair-Verfahren zwingend vorgegeben ist. Wenn Sie den Austausch dieser Teile von Hewlett Packard Enterprise vornehmen lassen, werden Ihnen die Anfahrt- und Arbeitskosten für diesen Service berechnet.


Reparaciones del propio cliente

Los productos de Hewlett Packard Enterprise incluyen muchos componentes que el propio usuario puede reemplazar (Customer Self Repair, CSR) para minimizar el tiempo de reparación y ofrecer una mayor flexibilidad a la hora de realizar sustituciones de componentes defectuosos. Si, durante la fase de diagnóstico, Hewlett Packard Enterprise (o los proveedores o socios de servicio de Hewlett Packard Enterprise) identifica que una reparación puede llevarse a cabo mediante el uso de un componente CSR, Hewlett Packard Enterprise le enviará dicho componente directamente para que realice su sustitución. Los componentes CSR se clasifican en dos categorías:
• **Obligatorio**—componentes cuya reparación por parte del usuario es obligatoria. Si solicita a Hewlett Packard Enterprise que realice la sustitución de estos componentes, tendrá que hacerse cargo de los gastos de desplazamiento y de mano de obra de dicho servicio.

• **Opcional**—componentes cuya reparación por parte del usuario es opcional. Estos componentes también están diseñados para que puedan ser reparados por el usuario. Sin embargo, si precisa que Hewlett Packard Enterprise realice su sustitución, puede o no conllevar costes adicionales, dependiendo del tipo de servicio de garantía correspondiente al producto.

**NOTA:** Algunos componentes de Hewlett Packard Enterprise no están diseñados para que puedan ser reparados por el usuario. Para que el usuario haga valer su garantía, Hewlett Packard Enterprise pone como condición que un proveedor de servicios autorizado realice la sustitución de estos componentes. Dichos componentes se identifican con la palabra "No" en el catálogo ilustrado de componentes.

Según la disponibilidad y la situación geográfica, los componentes CSR se enviarán para que lleguen a su destino al siguiente día laborable. Si la situación geográfica lo permite, se puede solicitar la entrega en el mismo día o en cuatro horas con un coste adicional. Si precisa asistencia técnica, puede llamar al Centro de asistencia técnica de Hewlett Packard Enterprise y recibirá ayuda telefónica por parte de un técnico. Con el envío de materiales para la sustitución de componentes CSR, Hewlett Packard Enterprise especificará si los componentes defectuosos deberán devolverse a Hewlett Packard Enterprise. En aquellos casos en los que sea necesario devolver algún componente a Hewlett Packard Enterprise, deberá hacerlo en el periodo de tiempo especificado, normalmente cinco días laborables. Los componentes defectuosos deberán devolverse con toda la documentación relacionada y con el embalaje de envío. Si no enviara el componente defectuoso requerido, Hewlett Packard Enterprise podrá cobrarle por el de sustitución. En el caso de todas sustituciones que lleva a cabo el cliente, Hewlett Packard Enterprise se hará cargo de todos los gastos de envío y devolución de componentes y escogerá la empresa de transporte que se utilice para dicho servicio.

Para obtener más información acerca del programa de Reparaciones del propio cliente de Hewlett Packard Enterprise, póngase en contacto con su proveedor de servicios local. Si está interesado en el programa para Norteamérica, visite la página web de Hewlett Packard Enterprise CSR ([http://www.hpe.com/support/selfrepair](http://www.hpe.com/support/selfrepair)).

---

**Customer Self Repair**

Veel onderdelen in Hewlett Packard Enterprise producten zijn door de klant zelf te repareren, waardoor de reparatieduur tot een minimum beperkt kan blijven en de flexibiliteit in het vervangen van defecte onderdelen groter is. Deze onderdelen worden CSR-onderdelen (Customer Self Repair) genoemd. Als Hewlett Packard Enterprise (of een Hewlett Packard Enterprise Service Partner) bij de diagnose vaststelt dat de reparatie kan worden uitgevoerd met een CSR-onderdeel, verzendt Hewlett Packard Enterprise dat onderdeel rechtstreeks naar u, zodat u het defecte onderdeel daarmee kunt vervangen. Er zijn twee categorieën CSR-onderdelen:

• **Verplicht**—Onderdelen waarvoor reparatie door de klant verplicht is. Als u Hewlett Packard Enterprise verzoekt deze onderdelen voor u te vervangen, worden u voor deze service reiskosten en arbeidsloon in rekening gebracht.

• **Optioneel**—Onderdelen waarvoor reparatie door de klant optioneel is. Ook deze onderdelen zijn ontworpen voor reparatie door de klant. Als u echter Hewlett Packard Enterprise verzoekt deze onderdelen voor u te vervangen, kunnen daarvoor extra kosten in rekening worden gebracht, afhankelijk van het type garantieservice voor het product.

**OPMERKING:** Sommige Hewlett Packard Enterprise onderdelen zijn niet ontwikkeld voor reparatie door de klant. In verband met de garantievoorwaarden moet het onderdeel door een geautoriseerde Service Partner worden vervangen. Deze onderdelen worden in de geïllustreerde onderdelencatalogus aangemerkt met "Nee".

Afhankelijk van de leverbaarheid en de locatie worden CSR-onderdelen verzonden voor levering op de eerstvolgende werkdag. Levering op dezelfde dag of binnen vier uur kan tegen meer kosten worden aangeboden, indien dit mogelijk is gezien de locatie. Indien assistentie is gewenst, belt u het Hewlett Packard Enterprise Support Center om via de telefoon ondersteuning van een technicus te ontvangen.

Neem contact op met een Service Partner voor meer informatie over het Customer Self Repair programma van Hewlett Packard Enterprise. Informatie over Service Partners vindt u op de Hewlett Packard Enterprise website (http://www.hpe.com/support/selfrepair).

Reparo feito pelo cliente

Os produtos da Hewlett Packard Enterprise são projetados com muitas peças para reparo feito pelo cliente (CSR) de modo a minimizar o tempo de reparo e permitir maior flexibilidade na substituição de peças com defeito. Se, durante o período de diagnóstico, a Hewlett Packard Enterprise (ou fornecedores/parceiros da Hewlett Packard Enterprise) concluir que o reparo pode ser efetuado pelo uso de uma peça CSR, a Hewlett Packard Enterprise enviará a peça diretamente ao cliente. Há duas categorias de peças CSR:

- **Obrigatória**—Peças cujo reparo feito pelo cliente é obrigatório. Se desejar que a Hewlett Packard Enterprise substitua essas peças, serão cobradas as despesas de transporte e mão-de-obra do serviço.

- **Opcional**—Peças cujo reparo feito pelo cliente é opcional. Essas peças também são projetadas para o reparo feito pelo cliente. No entanto, se desejar que a Hewlett Packard Enterprise as substitua, pode haver ou não a cobrança de taxa adicional, dependendo do tipo de serviço de garantia destinado ao produto.

**OBSERVAÇÃO:** Algumas peças da Hewlett Packard Enterprise não são projetadas para o reparo feito pelo cliente. A fim de cumprir a garantia do cliente, a Hewlett Packard Enterprise exige que um técnico autorizado substitua a peça. Essas peças estão identificadas com a marca "No" (Não), no catálogo de peças ilustrado.

Conforme a disponibilidade e o local geográfico, as peças CSR serão enviadas no primeiro dia útil após o pedido. Onde as condições geográficas permitirem, a entrega no mesmo dia ou em quatro horas pode ser feita mediante uma taxa adicional. Se precisar de auxílio, entre em contato com o Centro de suporte técnico da Hewlett Packard Enterprise para que um técnico o ajude por telefone. A Hewlett Packard Enterprise especifica nos materiais fornecidos com a peça CSR de reposição se a peça com defeito deve ser devolvida à Hewlett Packard Enterprise. Nos casos em que isso for necessário, é preciso enviar a peça com defeito à Hewlett Packard Enterprise, você deverá enviar a peça com defeito de volta para a Hewlett Packard Enterprise dentro do período de tempo definido, normalmente em 5 (cinco) dias úteis. A peça com defeito deve ser enviada com a documentação correspondente no material de transporte fornecido. Caso não o faça, a Hewlett Packard Enterprise poderá cobrar a reposição. Para as peças de reparo feito pelo cliente, a Hewlett Packard Enterprise paga todas as despesas de transporte e de devolução da peça e determina a transportadora/serviço postal a ser utilizado.

カスタマーセルフリペア

修理時間を短縮し、故障部品の交換における高い柔軟性を確保するために、Hewlett Packard Enterprise製品には多数のカスタマーセルフリペア（CSR）部品があります。診断の際に、CSR部品を使用すれば修理ができると考え、Hewlett Packard Enterprise（Hewlett Packard EnterpriseまたはHewlett Packard Enterprise正規保守代理店）が判断した場合、Hewlett Packard Enterpriseはその部品を直接、お客様に発送し、お客様に交換していただきます。CSR部品には以下の2種類があります。

- 必須 - カスタマーセルフリペアが必須の部品。当該部品について、もしもお客様がHewlett Packard Enterpriseに交換作業を依頼される場合には、その修理サービスに関する交通費および人件費がお客様に請求されます。
- 任意 - カスタマーセルフリペアが任意である部品。この部品もカスタマーセルフリペア用です。当該部品について、もしもお客様がHewlett Packard Enterpriseに交換作業を依頼される場合には、お買い上げの製品に適用される保証サービス内容の範囲内においては、別途費用を負担していただくことなく保証サービスを受けることができます。

注：Hewlett Packard Enterprise製品の一部の部品は、カスタマーセルフリペアの対象外です。製品の保証を継続するためには、Hewlett Packard EnterpriseまたはHewlett Packard Enterprise正規保守代理店による交換作業が必須となります。部品カタログには、当該部品がカスタマーセルフリペア外品である旨が記載されています。

部品供給が可能な場合、地域によっては、CSR部品を翌営業日に届くように発送します。また、地域によっては、追加費用を負担いただくことにより同日または4時間以内に届くように発送することも可能な場合があります。サポートが必要なときは、Hewlett Packard Enterpriseの修理受付窓口に電話いただければ、技術者が電話でアドバイスします。交換用のCSR部品または同様物には、故障部品をHewlett Packard Enterpriseに返送する必要があるかどうかが表示されています。故障部品をHewlett Packard Enterpriseに返送する必要がある場合は、指定期間内（通常は5営業日以内）に故障部品をHewlett Packard Enterpriseに返送してください。故障部品を返送する場合は、届いた時の梱包箱に関連書類とともに入れてください。故障部品を返送しない場合、Hewlett Packard Enterpriseから部品費用が請求されます。カスタマーセルフリペアの際には、Hewlett Packard Enterpriseは送料および部品返送費を全額負担し、使用する宅配便会社や運送会社を指定します。
客戶自行維修

Hewlett Packard Enterprise 產品提供許多客戶自行維修 (CSR) 部件，以尽可能缩短维修时间和提升维修效率。如在诊断期间 Hewlett Packard Enterprise (或 Hewlett Packard Enterprise 服务供应商或服务合作伙伴) 确定可以通过使用 CSR 部件进行维修，则将直接为该部件免费更换。有两类 CSR 部件：

- 强制性的 — 要求客户必须自行维修的部件。如果您请求 Hewlett Packard Enterprise 更换这些部件，必须为该服务支付差旅费和人工费用。

- 可选的 — 客户可以选择是否自行维修的部件。这些部件也是为客户提供维修设计的。如果您希望更换这些部件，必须为您的产品指定的保修服务类型为 Hewlett Packard Enterprise 可能收取或不再收取任何附加费用。

注：某些 Hewlett Packard Enterprise 部件的设计并未考虑客户自行维修。为了满足客户保修的需求，Hewlett Packard Enterprise 要求授权服务提供商更换有关部件。这些部件在部件图解目录中标注为“否”。

CSR 部件将在下一个工作日运达（取决于备货情况和允许的地理范围）。在允许的地理范围内，可在当天或四小时内运达，但须收取额外费用。如果需要帮助，您可以致电 Hewlett Packard Enterprise 技术支持中心，将会有技术人员通过电话为您提供帮助。Hewlett Packard Enterprise 会随更换的 CSR 部件发送的材料中指明是否必须将有缺陷的部件返还给 Hewlett Packard Enterprise。如果需要您将有缺陷的部件返还给 Hewlett Packard Enterprise，那么您必须在规定的期限内（通常是五 (5) 个工作日内）将该部件发送给 Hewlett Packard Enterprise。有缺陷的部件必须随所提供的发送材料中的相关文件一起返还。如果未随发送有缺陷的部件，Hewlett Packard Enterprise 可能会要求您支付更换费用。客户自行维修时， Hewlett Packard Enterprise 将承担所有相关运输和部件运送费用，并指定快递商/承运商。

有关 Hewlett Packard Enterprise 客户自行维修计划的详细信息，请与您当地的服务提供商联系。有关北美地区的计划，请访问 Hewlett Packard Enterprise 网站 (http://www.hpe.com/support/selfrepair)。

客戶自行維修

Hewlett Packard Enterprise 產品設計了許多「客戶自行維修」(CSR) 的零件以減少維修時間，並且使得更換損耗零件時能有更大的彈性。如在診斷期間，Hewlett Packard Enterprise (或 Hewlett Packard Enterprise 供服務供應商或維修夥伴) 確認出此項維修工作可以藉由使用 CSR 零件來完成，則 Hewlett Packard Enterprise 將直接寄送該零件給您作更換。CSR 零件分為兩種類別：

- 強制的 — 客戶自行維修所使用的零件是強制性的，如果您要求 Hewlett Packard Enterprise 更換這些零件，Hewlett Packard Enterprise 會向您收取此服務所需的外出費用和勞動成本。

- 選購的 — 客戶自行維修所使用的零件是選購的。這些零件也設計用於客戶自行維修之用。不過，如果您要求 Hewlett Packard Enterprise 為您更換，則可能需要也可能不需要支付額外的費用，端視針對此產品指定的保固服務類型而定。

備註：某些 Hewlett Packard Enterprise 零件沒有消費者可自行維修的設計。為符合客戶保固，Hewlett Packard Enterprise 需要授權的服務供應商更換零件。這些零件在圖示的零件目錄中，被標示為「否」。

基於材料取得及環境允許的情況下，CSR 零件將於下一個工作日內寄送。在環境的允許下當天或四小時內送達，則可能需要額外的費用。若您需要協助，可電話 Hewlett Packard Enterprise 支援中心，會有一位技術人員透過電話來協助您。不論損壞的零件是否必須退回，Hewlett Packard Enterprise 會在與 CSR 替換零件一起遞送的資料中註明。若要將損壞的零件退回 Hewlett Packard Enterprise，您必須在指定的一段時間內（通常為五 (5) 個工作天）將損壞的零件寄回 Hewlett Packard Enterprise。損壞的零件必須與寄送資料中隨附的相關技術文件一同退回。如果無法退回損壞的零件，Hewlett Packard Enterprise 可能會向您收取替代費用。針對客戶自行維修情形，Hewlett Packard Enterprise 將負責所有運費及零件運費費用，並指定使用哪家快速/承運公司。

如需 Hewlett Packard Enterprise 的 CSR 方案詳細資訊，請連絡您當地的服務供應商。至於北美地區，請參閱 Hewlett Packard Enterprise 的 CSR 網站 repair (http://www.hpe.com/support/selfrepair)。
Remote support

Remote support is available with supported devices as part of your warranty or contractual support agreement. It provides intelligent event diagnosis, and automatic, secure submission of hardware event notifications to Hewlett Packard Enterprise, which will initiate a fast and accurate resolution based on your product’s service level. Hewlett Packard Enterprise strongly recommends that you register your device for remote support.

For more information and device support details, go to the Insight Remote Support website (http://www.hpe.com/info/insightremotesupport/docs).
Acronyms and abbreviations

BPDU
Bridge Protocol Data Unit

DAC
direct attach cable

DHCP
Dynamic Host Configuration Protocol

DNS
domain name system

FC
Fibre Channel

FCoE
Fibre Channel over Ethernet

FIPS
Federal Information Processing Standard

HBA
host bus adapter

iSCSI
Internet Small Computer System Interface

ISL
Inter-Switch Link

LACP
Link Aggregation Control Protocol

LAG
link aggregation group

LLDP
Link Layer Discovery Protocol
MAC
Media Access Control

MIB
management information base

NPIV
N_Port ID Virtualization

OA
Onboard Administrator

POST
Power-On Self Test

RDP
Rapid Deployment Pack

SFP
small form-factor pluggable

SSL
Secure Sockets Layer

TFTP
Trivial File Transfer Protocol

USB
universal serial bus

VCDG
Virtual Connect Domain Group

VCEM
Virtual Connect Enterprise Manager

VCM
Virtual Connect Manager

VCSU
Virtual Connect Support Utility

VLAN
virtual local-area network
**WWN**
World Wide Name

**XFP**
10 Gb small form factor pluggable
Hewlett Packard Enterprise is committed to providing documentation that meets your needs. To help us improve the documentation, send any errors, suggestions, or comments to Documentation Feedback (mailto:docsfeedback@hpe.com). When submitting your feedback, include the document title, part number, edition, and publication date located on the front cover of the document. For online help content, include the product name, product version, help edition, and publication date located on the legal notices page.
A
About menu 61
accessing HPE Virtual Connect 10, 58
ActiveX 57
adding enclosures 65
Advanced Network Settings 79
allowing double density device bays 63
assign server profiles 96
assigned MAC addresses 72, 74
assigned WWNs 88
authorized reseller 125, 126

B
backup module 10, 13, 27
bay configuration guidelines 16
browser requirements 57
BSMI notice 123
buttons 101

cabling 22, 45, 48
Canadian notice 123
check-pointing 50
Cisco Core switch 48
CLI (Command Line Interface) 59
command line interface, using 59
command line overview 59
components 101, 104, 107, 111, 115, 118, 120
components, HPE VC 16Gb 24-Port FC Module 120
components, HPE VC 8Gb 20-Port FC Module 118
components, HPE VC 8Gb 24-Port FC Module 115
components, HPE Virtual Connect 107
components, HPE Virtual Connect Flex-10 10Gb
  Ethernet Module 101
components, HPE Virtual Connect Flex-10/10D Module 104
components, HPE Virtual Connect FlexFabric-20/40 F8 Module 111
configuration example 48
configuration, default module 11
configuration, redundant 22
connecting multiple enclosures 27
connectors 101
contact information 126
contacting Hewlett Packard Enterprise 126
cookies 57
create server profile definition 94
create server profiles, Server Profile Wizard 98
customer self repair (CSR) 127
data center connections, verifying 99
Declaration of Conformity 123, 124
define network 78
define network connection 77, 84
define SAN fabric 89, 91
define shared uplink set 81
direct connect VC domains 32
DNS label 35, 37
DNS settings 121
documentation 6, 138
domain name 67
domain setup wizard 61
domains, directly connecting 32
double density device bays, allowing 63, 66
double-dense server blades 66

E
EBIPA (Enclosure Bay IP Addressing) 21
electrostatic discharge 125
enable local users 68
Enabling FIPS mode 34
enclosure import 63, 65
enclosure recovery 63, 66
Ethernet connections 95
Ethernet module, installing 35
European Union notice 123
external connections 45
external port connections, verifying 99
external uplink ports 78, 81

F
factory default settings 45
failover 13, 61
FC connections 95
FC module bay configuration, multiple enclosures 30
FC module, installing 40
Federal Communications Commission (FCC) notice 123
Fibre Channel settings (WWN) 86
finish wizard 71, 85, 92
FIPS Mode 32
FIPS mode guidelines 33
FIPS mode indicators 35
FIPS Mode, enabling 34
firmware, Onboard Administrator requirements 58
Flex-10 installation guidelines 18
FlexFabric module bay configuration, multiple enclosures 30
FlexFabric module, installation 37
FlexNIC 8

general settings 67
grounding methods 125

H
hardware setup 10, 35, 37, 40
help resources 126
Hewlett Packard Enterprise contact information 126
Hewlett Packard Enterprise Technical Support 126, 134
Hewlett Packard Enterprise website 126
high availability support 22, 50
HPE VC FlexFabric-20/40 F8 Module requirements 19
HPE Virtual Connect 16Gb 24-Port FC Module, upgrading to 51
HPE Virtual Connect 8Gb 20-Port FC Module, upgrading to 52
HPE Virtual Connect 8Gb 24-Port FC Module 115, 117
HPE Virtual Connect 8Gb 24-Port FC Module, upgrading to 52
HPE Virtual Connect Flex-10 10Gb Ethernet Module 104
HPE Virtual Connect Flex-10 10Gb Ethernet Module components and LEDs 101
HPE Virtual Connect Flex-10 module, upgrading to 53
HPE Virtual Connect Flex10/10D Module 18, 106
HPE Virtual Connect Flex-10/10D Module components and LEDs 104
HPE Virtual Connect Flex-10/10D module, upgrading to 53
HPE Virtual Connect FlexFabric 10Gb/24-port Module 110
HPE Virtual Connect FlexFabric 10Gb/24-port Module components and LEDs 107
HPE Virtual Connect FlexFabric-20/40 F8 Module components and LEDs 111
HPE Virtual Connect Manager 57
HP EVirtual Connect 8Gb 20-Port FC Module 115, 118, 120
installation, management card 13
installing, Ethernet module 35, 37
installing, FC module 40
interconnect modules, removing 50
interconnect modules, replacing 50
Internet Explorer support 57
iSCSI MAC address 72
iSCSI support 72

J
Japanese notice 123
Javascript 57

L
LACP timer configuration 78
LEDs 102, 105, 108, 112, 116, 119, 121
LEDs, HPE Virtual Connect 16Gb 24-Port FC module 121
LEDs, HPE Virtual Connect 8Gb 20-Port FC Module 119
LEDs, HPE Virtual Connect 8Gb 24-Port FC module 116
LEDs, HPE Virtual Connect Flex-10 10Gb Ethernet Module 102
LEDs, HPE Virtual Connect Flex10/10D Module 105
LEDs, HPE Virtual Connect FlexFabric 10Gb/24-port Module 108
LEDs, HPE Virtual Connect FlexFabric-20/40 F8 Module 112
licensed software and MACs or WWNs 58
local user accounts 68
logging in 60
logical interconnects 25
loop prevention 26

M
MAC address settings 72
mode, FIPS 32
modifications, FCC notice 123
module configuration, default 11
Mozilla support 57
multiple enclosures, adding and importing 65
multiple enclosures, FC module bay configuration 30
multiple enclosures, FlexFabric module bay configuration 30
multiple enclosures, managing 27, 29
multiple enclosures, using 29

N
name server profiles 97
native VLAN 81
network mapping 45
node WWN 86
NPIV 13
O
Onboard Administrator login credentials 63
Onboard Administrator module, removing 55
Onboard Administrator, accessing Virtual Connect Module 58
Onboard Administrator, required firmware revision 58

P
password, resetting 121
planning the installation 8
port WWN 86
pre-deployment planning 9
primary module 10, 13, 27, 50, 58
private networks 78

Q
QSFP+ transceiver, removing 44

R
RDP, using with Virtual Connect 9
recommended stacking connections 22
recovering remote enclosures 61
recovery, enclosure 66
Red Hat procedures 58
redundant configuration 22
regulatory compliance identification numbers 123
regulatory compliance notices 123, 124
remote enclosures, recovering 61
remove module from an enclosure 50
removing the Onboard Administrator 55
replacing the Onboard Administrator 55
resetting the administrator password 121
resetting the system 61
resources 126
running the setup wizards 61

S
SAN fabrics, defining available 89
serial number settings 93
series number 123
server profile troubleshooting 95
server profiles 95
setup wizard 61, 71, 92
SFP transceiver, removing 44
shared port operation 103
shared server links 75
Smart Link 78
Stacking link guidelines 21
stacking links 21
static electricity 125
strong password 68
support 126
support and other resources 126
supported configurations 14, 15
system maintenance switch 104, 106, 110, 114, 117, 120

T
technical support 126
troubleshooting, server profiles 95

U
upgrading to an HPE Virtual Connect 16Gb 24-Port FC Module 51
upgrading to an HPE Virtual Connect 8Gb 20-Port FC Module 52
upgrading to an HPE Virtual Connect 8Gb 24-Port FC Module 52
upgrading to an HPE Virtual Connect Flex-10 Module 53
upgrading to an HPE Virtual Connect Flex-10/10D module 53
Upgrading to an HPE Virtual Connect FlexFabric Module from a VC-FC module 55
user accounts 68
user settings 70
using multiple enclosures 29

V
VC domains, directly connecting 32
VC-assigned MAC addresses 74
verify data center connections 99
verify link and speed 99
verify network status 100
Virtual Connect documentation 6
Virtual Connect Manager setup overview 12
Virtual Connect overview 8
VLAN tagging 45, 75
VLAN tunneling, enable or disable 78

W
website, Hewlett Packard Enterprise 126
WWN settings 86
WWN, selecting a range 88