

HP Virtual Connect Firmware Upgrade Steps and Procedures

Technical white paper

Table of contents

About this document	2
Firmware and Software Updates	2
Baseline Firmware Release Set contents	2
Onboard Administrator.....	3
Virtual Connect.....	3
Virtual Connect Support Utility	3
BladeSystem Firmware Installation Order.....	5
Firmware Update Requirements	5
General Requirements	5
Pre-installation Instructions	6
Firmware Update Instructions	10
Installation Notes	10
Installation Process	10
Firmware Update Process.....	10
Firmware Update Considerations	12
Installation Options	13
Firmware Downgrade Considerations	17
Firmware Downgrade Process	17
Virtual Connect Enterprise Manager.....	18
HP Smart Update Manager.....	18
Appendix A: Resetting VC Manager	19
For more information.....	21



About this document

This document specifies the versions of firmware and software as well as recommended steps for updates to Virtual Connect (VC) version 3.18 or later from previous versions in HP BladeSystem single and multi-enclosure VC Domain environments. The firmware and software versions listed in this document have been tested as a solution set and are fully supported by HP.

It is recommended that users read this entire document before attempting firmware update to the Virtual Connect environment and clearly understand all of the steps and procedures outlined in this document.

This document was last updated 6/17/2011



CAUTION: The specific firmware and software versions listed in this document provide support for HP Virtual Connect environment and must be used together to ensure complete solution component compatibility and full functionality, since these have been tested as a set. Using other version levels might result in operational issues.

Firmware and Software Updates

Setup of your HP BladeSystem c-Class enclosure with HP Virtual Connect modules and supported adapters (integrated and mezzanine cards) will require use of the latest HP BladeSystem Firmware Release Set 2011.05 with updates for specific components of the solution. For best results, follow the pre-deployment planning steps in the HP Virtual Connect for c-Class BladeSystem Setup and Installation Guide and the HP BladeSystem ProLiant Firmware Management Best Practices Implementer Guide (See Additional Resources sections for download sites) to deploy the baseline set with component updates.

Always install the firmware recommended for this release for the following items:

- HP BladeSystem Onboard Administrator
- HP Virtual Connect
- Server blade system ROMs
- Ethernet mezzanines
- Fibre Channel mezzanines
- iLO

For a complete list of recommended firmware and software versions for HP BladeSystem environments with VC modules and supported adapters, see the HP BladeSystem Firmware Maintenance website (<http://www.hp.com/go/ bladesystemupdates>). Click the **Compatibility & Downloads** tab and navigate to the **Additional Information** section to download the recommended HP Virtual Connect FlexFabric Solution Recipe White Paper.

Baseline Firmware Release Set contents

HP BladeSystem Firmware Release Set 2011.05	Latest Version
Smart Update Firmware DVD	9.30 ¹
Go to the 'Downloads' tab at HP Insight Foundation Suite for ProLiant site http://www.hp.com/go/foundation and look for the appropriate FW DVD version.	

¹ If the latest version of Virtual Connect firmware is not available on the Smart Update Firmware DVD, Windows and Linux Smart Components may be downloaded separately.

Onboard Administrator

Firmware	Latest Version
<p>HP BladeSystem c7000 Enclosure Onboard Administrator (OA)</p> <p>Go to http://h20180.www2.hp.com/apps/Nav?h_product=3709945&h_client=S-A-R163-1</p> <ol style="list-style-type: none"> 1. Select BladeSystem Enclosures and choose the appropriate enclosure 2. Select Download Drivers and Software 3. Select the appropriate Operating System 4. Select the "Firmware-Blade Infrastructure" category 5. Find "HP BladeSystem c-Class Onboard Administrator Firmware", select the latest version and click the "Download" button 	3.31

Virtual Connect

Firmware	Latest Version
<p>HP BladeSystem c-Class Virtual Connect Firmware, Ethernet plus 4/8Gb 20-port and 8Gb 24-port FC Edition</p> <p>HP BladeSystem c-Class Virtual Connect Firmware, Ethernet plus 4/8Gb 20-port and 8Gb 24-port FC Edition Component for Windows</p> <p>HP BladeSystem c-Class Virtual Connect Firmware, Ethernet plus 4/8Gb 20-port and 8Gb 24-port FC Edition Component for Linux</p> <p>Go to the "VC Support Page" http://www.hp.com/support/vc</p> <ol style="list-style-type: none"> 1. Select appropriate VC module 2. Select Download Drivers and Software 3. Select the appropriate Operating System 4. Select the "Firmware-Blade Infrastructure" category 5. Select the latest version of Smart Component or VCSU supported firmware image file and click Download button 	3.18

Virtual Connect Support Utility

Firmware	Latest Version
<p>Virtual Connect Support Utility v1.5.2 for Windows, Linux or HP-UX</p> <p>Go to the "VC Support Page" http://www.hp.com/support/vc</p> <ol style="list-style-type: none"> 1. Select appropriate VC module 2. Select Download Drivers and Software 3. Select the appropriate Operating System 4. Select the "Utility - Tools" category 5. Select the latest version of Virtual Connect Support Utility and click Download button 	1.5.2

Virtual Connect is a set of interconnect modules and embedded software for HP BladeSystem c-Class enclosures. HP Virtual Connect includes the following supported components:

- HP 1/10Gb Virtual Connect Ethernet Module for c-Class BladeSystem
- HP 1/10Gb-F Virtual Connect Ethernet Module for the c-Class BladeSystem
- HP Virtual Connect Flex-10 10Gb Ethernet Module for BladeSystem c-Class
- HP Virtual Connect FlexFabric 10Gb/24-Port Module for BladeSystem c-Class
- HP 4Gb Virtual Connect Fibre Channel Module for c-Class BladeSystem
- HP Virtual Connect 4Gb Fibre Channel Module for BladeSystem c-Class (enhanced NPIV)
- HP Virtual Connect 8Gb 24-Port Fibre Channel Module for BladeSystem c-Class

- HP Virtual Connect 8Gb 20-Port Fibre Channel Module for BladeSystem c-Class
- HP Virtual Connect Manager

NOTE: Virtual Connect FlexFabric Modules ship with VC 3.15 firmware installed, however, in the event a future firmware upgrade is required, Virtual Connect Support Utility (VCSU) v1.5.2 or greater is required.

BladeSystem Firmware Installation Order

For the new and existing Virtual Connect deployments where the Operating System has not yet been installed on the servers or servers are not yet present in the enclosure, HP recommends the following component update order:

1. Update the OA first by using the [Smart Update Firmware DVD](#) for Windows and Linux. Use a workstation connected to the same network as the OA.
2. Update the VC firmware using VCSU v1.5.2 or later from a workstation connected to the same network as the OA and VC Ethernet modules.
3. Update all server-specific offline and online firmware components with the HP Firmware Maintenance DVD.

For the new and existing Virtual Connect deployments where the Operating System has been installed on the servers, HP recommends the following component update order:

1. Update the blades and the OA by using the [Smart Update Firmware DVD](#) for Windows and Linux using a workstation connected to the same network as the OA.
2. Update any offline-only firmware components with the HP Firmware Maintenance DVD.
3. Update the VC firmware using VCSU v1.5.2 or later from a workstation connected to the same network as the OA and VC Ethernet modules. Be sure to update the VC firmware after all other updates are applied, after servers are rebooted, and after all other firmware is activated.

Firmware Update Requirements

The HP BladeSystem c-Class Virtual Connect Support Utility v1.5.2 or later is recommended to upgrade VC Ethernet, FlexFabric and VC-FC module firmware, as well as to perform other maintenance tasks remotely on both HP BladeSystem c-Class c7000 and c3000 enclosures with Virtual Connect deployments.

When the VCSU initiates a firmware upgrade process, by default, VC Ethernet modules' firmware activation is alternated between activation of all of the modules on one side of the enclosure before activating all of modules on the other side of the enclosure. This minimizes disruption to the network connectivity during the upgrades. Firmware activation on VC Fibre Channel modules is done serially starting from the highest IO Bay. The utility displays a progress message indicating that an update is in progress and the percentage completed. After the module firmware updates are complete, the utility activates all modules. Alternative firmware activation methods are available in VCSU as optional parameters and allow activation in parallel, serially, or manually.

General Requirements

There are a number of general requirements that need to be met to update Virtual Connect firmware using VCSU utility.

- VCSU 1.5.2 or earlier must be run on a client outside of the VC Domain. If VCSU resides on a server blade inside the domain that is being updated, VCSU might lose network connectivity to the VC Ethernet and Fibre Channel modules, causing unexpected firmware update failures and potentially leaving the Virtual Connect Manager in non-operational state. Note: Later versions of VCSU starting with VCSU 1.6.0 will have capability to be run from a client inside the VC Domain that is being updated.
- For Windows users – Microsoft® Windows® XP (Service Pack 1 or 2), Windows Server® 2003, Windows Server® 2008 or Windows Vista® operating systems must be installed on the client system.
- For Linux users – RedHat 4, RedHat 5, SLES 10, and SLES 11 for x86 Servers must be installed on the client system (only VCSU version 1.5.2 or newer).
- For HP-UX users – HPUX 11.23 and 11.31 must be installed on the client system (only VCSU version 1.5.2 or newer).
- VCSU supports only IPv4 addresses. IPv6 support is not yet available.
- When upgrading Virtual Connect Fibre Channel modules utilizing VCSU version 1.5.2 or newer, users must have Administrative or Power User privileges on the client system to install and run the utility.

- A valid HP Virtual Connect firmware package must be available to install. Download the firmware from the HP website (<http://www.hp.com>). Click Software and Driver Downloads, and then search for "Virtual Connect Firmware."
- Do not close the VCSU console application when a firmware update is in progress. If the application is closed before the update completes, the module firmware might not update properly, resulting in an incomplete update and causing the module firmware to become inoperative.
- If VCSU firmware update process is terminated, any future VCSU firmware update operations as well as the user attempts to login into the VC Manager GUI or CLI will be rejected until VC-Ethernet modules are restarted via a "Reset" Interconnect Bay operation from the Onboard Administrator management interface.
- An Onboard Administrator user account with Administrative privileges and access to all Onboard Administrators and interconnect bays in the domain must be available for use. If the enclosure is imported into a Virtual Connect domain, a Virtual Connect user account with Domain privileges is also required.
- In a multi-enclosure environment, the Onboard Administrator username and password must be identical across the local and all remote enclosures in the Virtual Connect Domain. Otherwise, a firmware update of the remote enclosures will not succeed.
- The user must have Ethernet network connectivity between the VCSU client system and the enclosure Onboard Administrator. To validate this connectivity, open a web browser to the enclosure Onboard Administrator before running the utility.
- All Virtual Connect Modules must have valid IP addresses on the OA management network from EBIPA or external DHCP and be reachable from the client system.
- If utilizing VCSU v1.5.2 or newer, it is no longer required to add the VCSU application to the list of exceptions for any host-based firewalls on the client system.
- If utilizing VCSU v1.5.2 or newer, the user is no longer required to disable network or host-based firewalls, open up TCP port 21, disable local Windows firewalls, Symantec Endpoint Protection (SEP), or McAfee firewall protection.
- Only one instance of the VCSU utility accessing a single enclosure or Virtual Connect domain can be run on the same client system at one time.
- During a firmware update operation, the Virtual Connect Manager User Interfaces will become temporarily inaccessible. Any attempt to reset or remove the modules during the update process may result in a corrupted firmware image. In addition, do not remove or reset the Onboard Administrator of the target enclosure or update its firmware while Virtual Connect modules are being updated. Doing so can interfere with the firmware update process and cause it to fail.
- If the firmware update client is interrupted or loses network connectivity during the update, reset the affected module and restart the firmware update process.
- If Virtual Connect Enterprise Manager (VCEM) is used, VCEM must be at a revision that is compatible with the target VC firmware version prior to the VC firmware upgrade attempt. For the correct VCEM version, refer to [Virtual Connect Enterprise Manager Support](#) section of this document.
- In order to update VC Domains that are under VCEM control, the Virtual Connect domain must be placed into a Maintenance Mode first or the firmware updates will be blocked.
- When updating environments with HP VC 8Gb 24-port FC modules and utilizing VCSU v1.5.2, one would have to ensure that a healthy VC-Enet backup module is installed in either IO Bay 2 or IO Bay 1 (if primary VC module is in IO Bay 2). If no backup module is available, VCSU will revert to the old FTP-based method and if there is a firewall blocking FTP communication, the firmware update will fail.

Pre-installation Instructions

Before using VCSU to update VC firmware, perform the following pre-installation checks to ensure the health of the VC domain.

1. VCSU automatically creates a backup of the Virtual Connect domain configuration during firmware update process to a file on the workstation where VCSU is installed (typically under C:\Program Files\Hewlett-Packard\Virtual Connect Support Utility\). If such a file was not created or appears to be zero size, back up the VC domain configuration using steps outlined below.

Virtual Connect GUI:

- Log in to VCM through a supported browser by browsing to the IP address or DNS name of the VCM and providing administrator credentials.
- Select "Tools → Backup/Restore Domain Configuration" from top menu.
- Select "Backup Configuration", and then click OK.
- Save the file to your system in case it is needed for recovery at a later time.
- Log out of VCM, and close your browser.

As an alternative, back up the current VC configuration using interactive mode of VCSU v1.5.2 or later:

```

hp Virtual Connect Support Utility - Interactive
-----
HP BladeSystem c-Class Virtual Connect Support Utility
Version 1.5.2 (Build 173)
Build Date: Jan 6 2011 11:26:43
Copyright (C) 2007-2010 Hewlett-Packard Development Company, L.P.
All Rights Reserved
-----
Please enter action ("help" for list): configbackup
Please enter Onboard Administrator IP Address: 192.168.1.1
Please enter Onboard Administrator Username: Administrator
Please enter Onboard Administrator Password: *****
Please enter the file location (Optional):
Please enter Configuration backup password (Optional):
Initializing, please wait...

```

Note: In a multi-enclosure environment or when redundant OA modules are present, Onboard Administrator IP Address must be the IP address of the active OA in the primary enclosure.

A non-interactive method to back up the current VC configuration is also available. The following command may be used for this operation:

```
vcsu -a configbackup -i <IP> -u <USER> -p <PWD> [-vcu <VCM USER> -vcp <VCM PASS>] [-l <FILE>] [-cp <CFG PASS>]
```

IP = IP Address of the active Onboard Administrator in enclosure

USER = Name of the Onboard Administrator user with privileges to access all enclosure interconnect bays

PWD = Password of the Onboard Administrator user. Use * to prompt for password

VCM USER = Name of Virtual Connect user with Domain privileges is required if Enclosure is in a Virtual Connect Domain. N/A if Enclosure is not in a Virtual Connect Domain

VCM PASS = Password for VCM USER

FILE = File name or full path of the file on the local file system to which the Virtual Connect Domain configuration will be saved (optional parameter).

CFG PASS = Password for Config Backup of Virtual Connect Domain Only used in Virtual Connect 3.00 and later.

Example:

```
vcsu -a configbackup -i 192.168.1.100 -u Admin -p password
```

2. Run a health check for new and existing Virtual Connect deployments using VCSU v1.5.2 or later:

```

hp Virtual Connect Support Utility - Interactive
-----
HP BladeSystem c-Class Virtual Connect Support Utility
Version 1.5.2 (Build 173)
Build Date: Jan 6 2011 11:26:43
Copyright (C) 2007-2010 Hewlett-Packard Development Company, L.P.
All Rights Reserved
-----
Please enter action ("help" for list): healthcheck
Please enter Onboard Administrator IP Address: 192.168.1.1
Please enter Onboard Administrator Username: Administrator
Please enter Onboard Administrator Password: *****
Initializing, please wait...

```

Note: In a multi-enclosure environment or when redundant OA modules are present, Onboard Administrator IP Address must be the IP address of the active OA in the primary enclosure.

Verify that the status of all VC Ethernet and FlexFabric modules is

- Health = OK
- IP Connectivity = Passed
- Module Configuration = In Sync
- Domain Configuration = In Sync (Primary and Backup modules only)

A non-interactive method to execute health check operation is also available. The following command may be used for this operation:

```
vcsu -a healthcheck -i <IP> -u <USER> -p <PWD> [-vcu <VCM USER> -vcp <VCM PASS>]
```

IP = IP Address of the active Onboard Administrator in enclosure

USER = Name of the Onboard Administrator user with privileges to access all enclosure interconnect bays

PWD = Password of the Onboard Administrator user. Use * to prompt for password

VCM USER = Name of Virtual Connect user with Domain privileges is required if Enclosure is in a Virtual Connect Domain. N/A if Enclosure is not in a Virtual Connect Domain

VCM PASS = Password for VCM USER

Example:

```
vcsu -a healthcheck -i 192.168.1.100 -u Administrator -p password
```

```
hp Virtual Connect Support Utility - Command Prompt
-----
Bay 1 : HP UC Flex-10 Enet Module
Power           : On
Health          : Ok
IP Address      : 16.119.79.117
IP Connectivity : Passed
Mode            : Primary
Domain Configuration : In Sync
Module Configuration : In Sync
-----
Bay 2 : HP UC Flex-10 Enet Module
Power           : On
Health          : Ok
IP Address      : 16.119.76.122
IP Connectivity : Passed
Mode            : Backup
Domain Configuration : In Sync
Module Configuration : In Sync
-----
Bay 5 : HP UC FlexFabric 10Gb/24-Port Module
Power           : On
Health          : Ok
IP Address      : 16.119.79.220
IP Connectivity : Passed
Mode            : Subordinate
Module Configuration : In Sync
-----
Bay 6 : HP UC FlexFabric 10Gb/24-Port Module
Power           : On
Health          : Ok
IP Address      : 16.119.76.146
IP Connectivity : Passed
Mode            : Subordinate
Module Configuration : In Sync
```

Verify that the status of all VC Fibre Channel modules is

- Health = OK
- IP Connectivity = Passed


```
hp Virtual Connect Support Utility - Command Prompt
-----
Bay 3 : HP UC 8Gb 24-Port FC Module
Power           : On
Health          : Ok
IP Address      : 15.119.77.245
IP Connectivity : Passed
-----
Bay 4 : HP UC 8Gb 24-Port FC Module
Power           : On
Health          : Ok
IP Address      : 15.119.78.243
IP Connectivity : Passed
-----
Bay 7 : HP UC 8Gb 20-Port FC Module
Power           : On
Health          : Ok
IP Address      : 15.119.79.240
IP Connectivity : Passed
-----
Bay 8 : HP UC 8Gb 20-Port FC Module
Power           : On
Health          : Ok
IP Address      : 15.119.76.245
IP Connectivity : Passed
```

If any modules in enclosure exhibit the following status, take the action mentioned below

- Health = Degraded/Failed

The health of this module is being reported by the Onboard Administrator as not OK. Log in to the Onboard Administrator for additional information to determine the potential problem. A reset of the failed module may help to clear up this condition.

- Domain Configuration = Not In Sync

The domain configuration is not in sync between the Primary and Backup VC modules. This may be a transient condition. Wait up to 5 minutes and rerun "healthcheck" command. If the Domain Configuration is still "Not In Sync", collect VC Support Information and Contact HP Support. A reset of the VCM may help to clear up this condition. Please refer to [Appendix A](#) for instructions on how to reset VC Manager.

- Module Configuration = invalid/Not In Sync

The interconnect module configuration is not in sync with the VC domain configuration. This may be a transient condition. Wait up to 5 minutes and rerun "healthcheck" command. If the Module Configuration is still "Not In Sync", collect VC Support Information and Contact HP Support. A reset of the VCM may help to clear up this condition. Please refer to [Appendix A](#) for instructions on how to reset VC Manager.

For any instance where "Contact HP Support" is recommended, please

1. Login into Virtual Connect Manager, Select "Tools→Export Support Information".
2. Login to Onboard Administrator CLI, execute "show all" command and save the output to a file.
3. On a local system, collect all fwupdate-xxx.log files from where VCSU is installed (typically under C:\Program Files\Hewlett-Packard\Virtual Connect Support Utility\)

Firmware Update Instructions

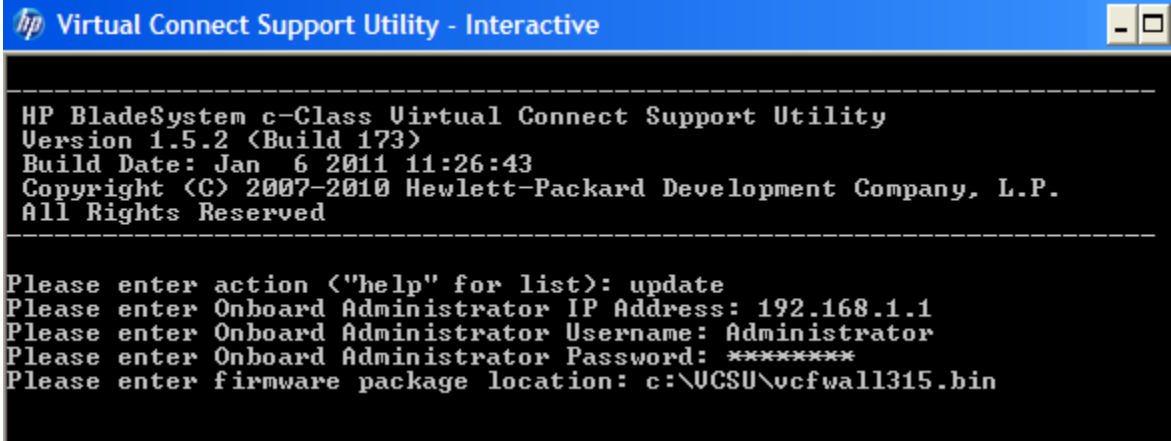
Installation Notes

- If you are using the Virtual Connect Enterprise Manager (VCEM) to manage your Virtual Connect domains, you will need to place them in "Maintenance" mode before using the VCSU utility.
- The VCSU utility does not update modules that are not physically present, are powered off, or are non-functional. Please run VCSU "healthcheck" command to determine module's state and status.
- The utility does not update non-VC modules, including pass-thru and switch modules.
- If a firmware image location is specified in VCSU as a hyperlink to an HTTP and HTTPS website, this site must not require additional authentication.
- If a firmware image location is specified in VCSU as a link to an FTP site, this site must be non-SSL/TLS, Passive Transfer Mode FTP site, and user must include the authentication information in the link. For example: <ftp://user:password@hostname-or-ipaddress/directory/filename>.
- If a firmware image location is specified in VCSU as a Windows path and any of the directory names in the path have spaces in them, the entire path with filename should be enclosed in double quotation marks.

Installation Process

After all of the checks have been performed and completed successfully, the VC firmware must be downloaded from the web. The latest version of the firmware can be found on the **Compatibility & Downloads** tab of the HP BladeSystem Firmware Maintenance page <http://www.hp.com/go/bladeupdates>.

Once the VC firmware package is downloaded from the web, launch VCSU 1.5.2 or later from local Windows, Linux or HP-UX workstation.



```
hp Virtual Connect Support Utility - Interactive
-----
HP BladeSystem c-Class Virtual Connect Support Utility
Version 1.5.2 (Build 173)
Build Date: Jan 6 2011 11:26:43
Copyright (C) 2007-2010 Hewlett-Packard Development Company, L.P.
All Rights Reserved
-----
Please enter action ("help" for list): update
Please enter Onboard Administrator IP Address: 192.168.1.1
Please enter Onboard Administrator Username: Administrator
Please enter Onboard Administrator Password: *****
Please enter firmware package location: c:\VCSU\vcfwal1315.bin
```

Both the OA and VC credentials are required for the update process. The OA credentials must be Administrator equivalent credentials so that VCSU could access specific OA data to perform the upgrade.

Under no circumstances should VC modules be restarted or the VCSU Window closed while the update process is in progress. Otherwise, the firmware update will fail potentially rendering modules inoperable. If VCSU firmware update process is terminated, any future VCSU firmware update operations as well as the user attempts to login into the VC Manager GUI or CLI will be rejected until VC-Ethernet modules are restarted via a "Reset" Interconnect Bay operation from the Onboard Administrator management interface.

Firmware Update Process

A typical firmware update process that most everyone is familiar with is an update of a single switch which generally has a deterministic update time. Note that updating the firmware of the VC modules is not as deterministic and predictable and so may be unexpected to some users. The update process may take approximately 20 minutes for a

VC-Enet module and 5 minutes for a VC-FC module. These times greatly depend on the number and types of the modules in the enclosure, as well as presence and complexity of the VC Domain configuration. They will also vary based on a Single- vs. Multi-Enclosure domain configuration.

There are two key reasons why the VC experience is different:

1. When updating Virtual Connect Domain, one is updating a system that is trying to maintain online connectivity and provide uninterrupted services to the servers within an enclosure or multiple enclosures with redundant VC modules.
2. Virtual Connect maintains a configuration database for the overall VC Domain as well as individual VC Ethernet and Fibre Channel modules. Due to this capability, VC has to ensure that each module has the correct configuration prior to bringing this module back online after the upgrade. This process takes time and is variable based on the size and complexity of the VC Domain.

When updating a VC Domain, VCSU performs the following steps required for a successful update:

Step #'s	Stages	Detailed Description	VCSU % completion
1	Initialization	Download firmware package (local file or HTTP/HTTPS/FTP site) and unpack it locally	N/A
2		Gather current running firmware information from the modules in Domain.	
3		Compare firmware package information with currently running firmware information.	
4		If enclosure(s) have been imported into the VCM domain: <ol style="list-style-type: none"> a. Store which IO Bay is currently Primary VC module. b. Verify that the VC Domain is stable, i.e. no operations are in progress. c. Backup VCM config and optionally password protect it. 	
5		Check for previously incomplete, in progress, or failed firmware update operations.	
6	Update	Temporarily make VC Manager inaccessible to the external management applications (GUI, CLI, and VCEM) in order to prevent VC configuration changes while firmware update is in progress.	0%
7		In parallel, via sFTP, move firmware image over to each of the VC Ethernet or FlexFabric modules.	28%
8		Simultaneously begin firmware update on all VC Ethernet and FlexFabric modules.	28%
9		Continuously monitor all modules' update progress and wait to complete the update operation.	57%
10		If enclosure(s) have been imported into the VCM domain: <ul style="list-style-type: none"> • Verify that the VC Domain is stable, i.e. no operations are in progress. 	71%
11	Activation	Make VC Manager accessible to the external management applications (GUI, CLI, and VCEM).	0%
12		If enclosure(s) have been imported into the VCM domain: <ul style="list-style-type: none"> • Verify that the VC Domain is stable, i.e. no operations are in progress. 	10%
13		Begin firmware activation process utilizing the default firmware activation method (odd-even)	10%
14		Reboot all VC Ethernet or FlexFabric modules in the enclosure(s) that are on the same side of the enclosure(s) as the Backup VC module.	20%
15		Wait for all of the rebooted modules to come back online and report the correct firmware version.	25%
16		If enclosure(s) have been imported into the VCM domain: <ul style="list-style-type: none"> • Verify that the VC Domain is stable, i.e. no operations are in progress. 	25%
17		Reboot all VC Ethernet or FlexFabric modules in the enclosure(s) that are on the same side of the enclosure(s) as the Primary VC module EXCEPT for the Primary VC module itself.	30%
18		Wait for all of the rebooted modules to come back online and report the correct firmware version.	35%
19		If enclosure(s) have been imported into the VCM domain: <ul style="list-style-type: none"> • Verify that the VC Domain is stable, i.e. no operations are in progress. 	35%
20		Force failover of the VC Manager from the Primary VC module to the adjacent IO Bay.	40%

21	Wait for previous backup VCM module to become new primary	40%
22	If enclosure(s) have been imported into the VCM domain: <ul style="list-style-type: none"> Verify that the VC Domain is stable, i.e. no operations are in progress. This operation may take an extended period of time since the VC Domain may be required to be reconfigured. 	40%
23	As the final step ¹ , reboot original Primary VC module to complete activation process.	45%

¹Above steps do not include VC-FC modules' update process. VC-FC modules are updated in parallel and then firmware is activated serially.

Firmware Update Considerations

VC Ethernet and FlexFabric modules do reboot during the firmware activation process and this will affect connectivity to those modules. However, the practical impact of module firmware activation is alleviated by having a redundant hardware configuration, proper networking connectivity setup and NIC teaming/bonding enabled on the server. Above mentioned network design methods are recommended and must be a prevalent practice. VC-FC modules "may" experience an outage depending on the old vs. new FW versions, but a majority of the time VC-FC modules utilize a Non-Disruptive Code Load and Activation (NDCLA) where no current I/O paths are affected by the update. Regardless of this VC-FC module feature, SAN connectivity must always be configured redundantly to avoid application outages.

When designing VC Domain connectivity options, one always must take into consideration all of the dependencies that may influence VC Domain's ability to sustain a firmware update while still passing traffic without interruption. The following aspects of a redundant design have to be verified prior to firmware update in downtime sensitive environments:

1. Properly configured stacking links between VC modules and enclosures. Proper stacking configuration will provide connectivity for any blade server to any uplink port in the VC domain, regardless of the server location. It will not only reduce the overall number of cables needed for uplink connectivity, provide the ability to move a server profile between enclosures, reduce datacenter core switch traffic, but also play a major role in sustainability of the individual VC module outage during firmware upgrade.
Please consult both the [Virtual Connect Multi-Enclosure Stacking Reference Guide](#) and [Virtual Connect Setup and Install Guide](#) for recommended stacking link configurations and requirements.
2. Order of module activation in the VCSU plays a crucial role in how network and storage connectivity will be interrupted or preserved during a firmware update. When the VCSU initiates the firmware activation process, by default, VC Ethernet modules' activation is alternated between left and right (odd and even) side modules to minimize disruption to the network and storage connectivity during the upgrade.
3. In order to minimize potential of an outage, VC networks and SAN fabrics should be created with an A and B side connectivity to allow either all links to be in an active state at all times or to allow for a failover in a controlled fashion. More physical uplinks could be utilized and additional Virtual Connect networks defined to reduce latency and provide more bandwidth to the networking layer, based on needs and application demands.
4. Blade host operating system configuration is vital in order to maintain uptime during the firmware update process. Properly configured NIC teaming/bonding and vSwitches will ensure both redundancy of the network connectivity, fast network path failure detection and timely failover to a redundant path, if available.

The following operating system settings provide means for a faster link failure detection and failover initialization.

- Under the normal operating conditions, the Virtual Connect SmartLink setting will alter the individual NIC state in the vSwitch, vDS, or teaming/bonding software by turning off the corresponding server NIC port. This will cause the vSwitch, vDS or NIC teaming/bonding to detect a failure and fail-over traffic to an alternate path. In order for the SmartLink functionality to operate as designed, valid DCC-compatible NIC firmware and drivers are required to be installed on a blade server. However, during the firmware update process when VC Ethernet and FlexFabric modules are reset for activation, SmartLink and DCC protocol will not be able to send a message to the NIC to inform it that link went down since the module is being rebooted. Therefore, during firmware update operation it is up to the NIC and OS to detect link failure.
 - Configuring the vSwitch or vNetwork Distributed Switch (vDS) Network Failover Detection option for Link Status Only in VMware ESX/ESXi Server network configuration is recommended.

- In some cases, during firmware update when VC Ethernet and FlexFabric modules are reset for activation and undergo graceful shutdown, there is a potential of up to 20 sec network outage. In these cases, enabling VMware ESX Beacon Probing, Linux ARP Monitoring and Windows Path Validation Heartbeat will work faster and more consistently. Please note that for VMware ESX Beacon Probing is most useful with three or more NICs in a team and only available with vSwitch and vDS, not with NX1000v. It is recommended to review VMware Knowledge Base articles specified below for pros and cons of enabling Beacon Probing.
 - <http://kb.vmware.com/selfservice/microsites/search.do?cmd=displayKC&externalId=1005577>
 - <http://kb.vmware.com/selfservice/microsites/search.do?cmd=displayKC&externalId=1017612>
 - <http://kb.vmware.com/selfservice/microsites/search.do?cmd=displayKC&externalId=1039177>
 - <http://kb.vmware.com/selfservice/microsites/search.do?cmd=displayKC&externalId=1024435>
 - <http://kb.vmware.com/selfservice/microsites/search.do?cmd=displayKC&externalId=1004373>
 - <http://kb.vmware.com/selfservice/microsites/search.do?cmd=displayKC&externalId=1012819>
 - In the VMware ESX/ESXi environments it is recommended to either turn OFF the High Availability (HA) mode or increase VMware HA timeout from the default of 13 seconds to 30-60 seconds. When the above options are configured, all guest OS's will be able to survive the upgrade with expected network outage due to the stacking link re-convergence and optimal network path recalculation by VCM.
 - For the customer environments where changing Network Failover Detection options or HA settings is not possible, utilizing VCSU manual firmware activation order (-of manual) is recommended. In this case, modules will be updated but not activated and the user will need to perform manual activation by resetting (rebooting) modules via OA GUI or CLI interface. This option will eliminate potential of up to 20 sec network outage that may occur on a graceful shutdown of VC Ethernet and FlexFabric modules.
 - The Spanning Tree Port Fast feature of Cisco switches allows a switch port to bypass the 'listening' and 'learning' stages of spanning tree and quickly transition to the 'forwarding' stage. By enabling this feature, edge devices are allowed to immediately begin communication on the network instead of having to wait on Spanning Tree to determine if it needs to block the port to prevent a loop – a process that can take 30+ seconds with default Spanning Tree timers. Since VC is an edge device, this feature would allow server NICs to begin immediate communication on the network rather than waiting for the additional 30 seconds to allow spanning tree to recalculate. To enable PortFast feature please execute following commands:
 - Catalyst switches use the commands:
 - spanning-tree portfast
 - spanning-tree portfast trunk
 - Nexus switches use the commands:
 - spanning-tree port type edge
 - spanning-tree port type edge trunk

*** Nexus switches will also accept the *portfast* commands.
5. In Multi-Enclosure VC Domains it is recommended to insert an additional 5 min delay into the VCSU utility execution script. This option will delay firmware activation of the VC modules between left and right hand sides of the enclosure, while allowing VC Manager to stabilize and checkpoint configuration across recently rebooted modules. At the same time, NIC teaming/bonding software and vSwitches, as well as multi-pathing storage software, will be allowed to properly recover from one path failure due to an update before failing over to a secondary path.
 6. When upgrading the HP VC 4Gb FC module's firmware from version 1.2x to version 1.4x, the HP VC 4Gb FC module will temporarily drop SAN connectivity during the activation process due a required module reset. Properly configured multi-pathing storage software will allow for a failover with no loss of application connectivity to the fabric.

Installation Options

The VCSU utility only updates supported VC modules that are reporting good status and that require an update. In addition to the default installation options, there are several optional parameters available.

1. One may update just a single VC-Enet or VC-FC module. Typically this option is not recommended when upgrading the entire VC Domain. However, if an update is only required to a single module in order to bring it to the same level of the firmware as the rest of the modules in the enclosure, this optional parameter is available.

In order to update a single VC-Enet module, it must be placed into an IO Bay that doesn't correspond to the location of the Primary or Backup VC-Enet module in the enclosure.

```
HP Virtual Connect Support Utility - Interactive

-----
HP BladeSystem c-Class Virtual Connect Support Utility
Version 1.5.2 (Build 173)
Build Date: Jan  6 2011 11:26:43
Copyright (C) 2007-2010 Hewlett-Packard Development Company, L.P.
All Rights Reserved
-----

Please enter action ("help" for list): update
Please enter Onboard Administrator IP Address: 192.168.1.1
Please enter Onboard Administrator Username: Administrator
Please enter Onboard Administrator Password: *****
Please enter firmware package location: c:\UCSU\vcfwall315.bin
Please enter Bay Number (Optional): 5
```

2. As one of the first steps during the firmware update process, VCSU will take a snapshot of the Virtual Connect Domain configuration and store it locally in the directory where it is installed. As an option, the user may choose to encrypt the configuration backup file.

```
HP Virtual Connect Support Utility - Interactive

-----
HP BladeSystem c-Class Virtual Connect Support Utility
Version 1.5.2 (Build 173)
Build Date: Jan  6 2011 11:26:43
Copyright (C) 2007-2010 Hewlett-Packard Development Company, L.P.
All Rights Reserved
-----

Please enter action ("help" for list): update
Please enter Onboard Administrator IP Address: 192.168.1.1
Please enter Onboard Administrator Username: Administrator
Please enter Onboard Administrator Password: *****
Please enter firmware package location: c:\UCSU\vcfwall315.bin
Please enter Bay Number (Optional): 5
Please enter Configuration backup password (Optional):
```

3. A user may also choose to force an update of the modules under the following circumstances:
 - a. The target module contains a running firmware image that is the same version as the one in the source package.
 - b. The target module contains a running firmware image that is newer than the version in the source package.
 - c. The target module is in a degraded or failed state.

```
HP Virtual Connect Support Utility - Interactive

-----
HP BladeSystem c-Class Virtual Connect Support Utility
Version 1.5.2 (Build 173)
Build Date: Jan  6 2011 11:26:43
Copyright (C) 2007-2010 Hewlett-Packard Development Company, L.P.
All Rights Reserved
-----

Please enter action ("help" for list): update
Please enter Onboard Administrator IP Address: 192.168.1.1
Please enter Onboard Administrator Username: Administrator
Please enter Onboard Administrator Password: *****
Please enter firmware package location: c:\UCSU\vcfwall315.bin
Please enter Bay Number (Optional): 5
Please enter Configuration backup password (Optional):
Do you want to force an update on modules? (yes/NO): yes
Please enter Force Update options (eg: version,health):
```

- By default, VCSU will install the new firmware package on all VC modules simultaneously. Afterwards, VC Ethernet modules' firmware activation will be alternated between left and right hand side modules to minimize disruption to the network connectivity during the upgrades. Firmware activation on VC Fibre Channel modules will be done serially starting from the highest IO Bay.
Alternative firmware activation methods are available in VCSU as optional parameters and allow activation in parallel, serially, or manually. One must chose carefully before proceeding with one of the alternative methods and understand potential implications on the server network and storage connectivity. For more details on the alternative firmware activation methods please refer to the Virtual Connect Support Utility Version 1.5.2 User Guide.

```

hp Virtual Connect Support Utility - Interactive
-----
HP BladeSystem c-Class Virtual Connect Support Utility
Version 1.5.2 (Build 173)
Build Date: Jan  6 2011 11:26:43
Copyright (C) 2007-2010 Hewlett-Packard Development Company, L.P.
All Rights Reserved
-----
Please enter action ("help" for list): update
Please enter Onboard Administrator IP Address: 192.168.1.1
Please enter Onboard Administrator Username: Administrator
Please enter Onboard Administrator Password: *****
Please enter firmware package location: c:\VCSU\vcfwall1315.bin
Please enter Bay Number (Optional): 5
Please enter Configuration backup password (Optional):
Do you want to force an update on modules? (yes/NO): no
Do you want to Specify UC-Enet module activation order? (yes/NO): yes
Please enter UC-Enet module activation order (eg: parallel or odd-even or
serial or manual):

```

- When the VCSU initiates the firmware activation process, VC Ethernet modules' activation is alternated between left and right (odd an even) side modules to minimize disruption to the network and storage connectivity during the upgrade. In some instances is it recommended to insert an additional 5 min delay into VCSU utility execution script which will delay activation of the VC modules' firmware between left and right hand sides of the enclosure, therefore allowing VC Manager and host operating system to stabilize before continuing with the update.

```

hp Virtual Connect Support Utility - Interactive
-----
HP BladeSystem c-Class Virtual Connect Support Utility
Version 1.5.2 (Build 173)
Build Date: Jan  6 2011 11:26:43
Copyright (C) 2007-2010 Hewlett-Packard Development Company, L.P.
All Rights Reserved
-----
Please enter action ("help" for list): update
Please enter Onboard Administrator IP Address: 192.168.1.1
Please enter Onboard Administrator Username: Administrator
Please enter Onboard Administrator Password: *****
Please enter firmware package location: c:\VCSU\vcfwall1315.bin
Please enter Bay Number (Optional): 5
Please enter Configuration backup password (Optional):
Do you want to force an update on modules? (yes/NO): no
Do you want to Specify UC-Enet module activation order? (yes/NO): yes
Please enter UC-Enet module activation order (eg: parallel or odd-even or
serial or manual): odd-even
Do you want to Specify UC-FC module activation order? (yes/NO): no
Do you want to Specify the amount of time(in minutes) to wait between
activating or rebooting UC-Enet modules? (yes/NO): yes
Please enter the time (in minutes)[max 60 mins]: 5

```

- Once all of the required and optional parameters have been specified, VCSU will begin to verify the validity of the firmware image file supplied by the user, gather information about the VC modules in the target enclosure as well as the firmware running on those modules, compare firmware package information with the currently running firmware information to determine if this operation will be an update or a downgrade. If all of the checks passed and no errors were detected, VCSU will produce a report with the types of the modules, their location, currently running firmware version and the new intended firmware version. At this point, user will be required to specify whether it is desirable to continue with the firmware update or not.

```

hp Virtual Connect Support Utility - Interactive
The following modules will be updated:
=====
Enclosure  Bay  Module                      Current Version              New Version
-----
USE822BEUW  1  HP UC Flex-10
      Enet Module              3.10                         3.15
      2010-09-03T06:16:45Z    2010-10-09T07:18:16Z
-----
USE822BEUW  2  HP UC Flex-10
      Enet Module              3.10                         3.15
      2010-09-03T06:16:45Z    2010-10-09T07:18:16Z
-----
USE822BEUW  3  HP UC 8Gb
      24-Port FC
      Module                   1.03 v6.1.0_49              1.03 v6.1.0_49
-----
USE822BEUW  4  HP UC 8Gb
      24-Port FC
      Module                   1.03 v6.1.0_49              1.03 v6.1.0_49
-----
USE822BEUW  5  HP UC
      FlexFabric
      10Gb/24-Port
      Module                   3.15                         3.15
      2010-10-09T08:13:18Z    2010-10-09T08:13:18Z
-----
USE822BEUW  6  HP UC
      FlexFabric
      10Gb/24-Port
      Module                   3.15                         3.15
      2010-10-09T08:13:18Z    2010-10-09T08:13:18Z
-----
USE822BEUW  7  HP UC 8Gb
      20-Port FC
      Module                   1.41 7.12.4.11             1.41 7.12.4.11
-----
USE822BEUW  8  HP UC 8Gb
      20-Port FC
      Module                   1.41 7.12.4.11             1.41 7.12.4.11
-----

During the update process, modules being updated will be temporarily
unavailable. In addition, the update process should NOT be interrupted by
removing or resetting modules, or by closing the application. Interrupting
the update or the modules being updated may cause the modules to not be updated
properly.

Please verify the above report before continuing.

Would you like to continue with this update? [YES/NO]: yes

```


Firmware Downgrade Considerations

Beginning with VC version 3.15 and later, any VC firmware downgrades will be blocked and the user will be required to delete the VC Domain via VCM GUI or CLI prior to attempting firmware downgrade. Therefore, even when downgrading from the same major revision (e.g. downgrading from 3.15 to 3.10), VC Domain deletion will be required and the VC Domain configuration will not be preserved through the downgrade process.

This limitation doesn't present any changes to the current behavior of the VC Manager in the multi-enclosure domain environments. Today, multi-enclosure domain downgrades already require domain deletion as a prerequisite to the firmware downgrade. With VC version 3.15 and later, the same requirement has been extended to single enclosure domains.

When the VC Domain is deleted, all VC modules revert to their default factory state. Server network and storage connectivity is removed. Any VC-assigned configuration parameters such as MAC addresses, WWNs, server serial numbers, boot target and boot order parameters are cleared from the servers. Any user accounts created under VCM are removed and only Administrator credentials remain valid.

VC users are strongly advised to maintain previous copies of their VC domain configuration files. Lack of the previously save configuration file will force VC users to reconstruct their VC Domain manually from scratch. Only a version of the VC Domain configuration file corresponding to the currently running firmware version can be utilized for a domain recovery. Table below summarizes the existing and future VC Domain firmware downgrade scenarios:

Table 1: VC Domain Firmware Downgrade Scenarios

VC version	VC version	VC Domain Preservation
1.xx	→ 1.yy (xx < yy)	Yes
2.xx	→ 1.xx	Yes, if Flex-10 is not configured
2.xx	→ 2.yy (xx < yy)	Yes
3.10	→ 3.01	Yes
3.xx	→ 1.xx	No
3.xx	→ 2.xx	No
3.xx (xx >= 15)	→ 3.yy (yy < xx)	No

Firmware Downgrade Process

When performing VC Domain downgrade, it is imperative to follow procedures outlined in this document. Below are the steps outlining required preparatory actions for a successful VC Domain downgrade for both single and multi-enclosure environments.

1. Locate a known good VC Domain configuration backup file corresponding to an intended firmware version. If this file is incompatible or corrupted, VC Manager will be unable to recovery domain configuration.
2. Execute VCSU *healthcheck* command as outlined in "Pre-installation Instructions" section of this document. Verify that the status of all VC Ethernet and FlexFabric modules, and take a note of the location of the Primary VC module (specifically the OA and Primary VC-Enet module IP Address information).
3. Login into the VC GUI or CLI and perform Delete Domain operation. When in a multi-enclosure environment, delete domain operation will release primary and non-primary enclosures back to an unintegrated state.
4. Using VCSU, downgrade individual enclosure (or enclosures when in a multi-enclosure environment). Specifying VCM username or password during VCSU firmware downgrade operation is not required since VC Domain is no longer present.
5. To begin recovery of the VC Domain, locate information about the OA and the Primary VC-Enet module from step #2 above. Connect to the IP Address of Primary VC-Enet module and login into the VC Manager GUI to begin recovery.

6. Once the enclosure is identified by the VCM and user is presented with the choices to either Import New Enclosure or Recover from previously saved configuration backup file, user must choose to recover from the previously save configuration backup file located in step #1.
7. VC Manager will verify validity of the specified file and proceed with the recovery if no issues are identified with the backup file.
8. Upon completion of the import of the configuration backup file, VC Manager will count down to 0 seconds remaining and reloaded the GUI login screen. "Loading, Please Wait..." message will be presented for the duration of the recovery and will to go away once domain is fully restored.
9. When VC Manager login screen is presented, proceed to login into the VCM.
10. In a multi-enclosure environment all of the secondary enclosures will not be seen by the VC Manager and user will be required to re-enter corresponding OA username and password credentials.
 11. In VC GUI, navigate to the name of the enclosure that is marked with "?" or red "X" and click on the enclosure name. Select Enclosure Status tab and re-enter OA username and password credentials.
 12. If VC Manager reports that the enclosure is already part of another VC Domain, connect to the corresponding OA CLI and issue the following command – "clear vcmode" and repeat step (10.a) above.
 13. Once VC Manager locates these enclosures, it will proceed with the import and reload the GUI login screen. "Loading, Please Wait..." message will be presented for the duration of the enclosure import and will to go away once the enclosure is fully imported.
14. VC Domain will be fully restored and all of the enclosures will be imported at this point.

Virtual Connect Enterprise Manager

Virtual Connect Enterprise Manager (VCEM) support matrix cross-references VCEM and VC supported versions.

Table 2: VCEM Support Matrix

VCEM Version	Support VC Firmware versions
6.1	2.1x, 2.2x, 2.3x, and 3.0x
6.2.2	2.1x, 2.2x, 2.3x, 3.0x, 3.1x, and 3.15 (pre-enabled)
6.3	2.1x, 2.2x, 2.3x, 3.0x, 3.10, 3.15, 3.17, and 3.18
6.3u2	2.1x, 2.2x, 2.3x, 3.0x, 3.10, 3.15, 3.17, 3.18, and 3.3x (pre-enabled)

Please verify that the intended VCM firmware version is supported by the appropriate VCEM version prior to updating a VC Domain that is controlled by VCEM. It is possible to add a VC Domain with a newer firmware version to an existing VC Domain Group (VCDG) by using compatibility mode. However, this will prevent a newly added VC Domain from being able to utilize new features.

For VCEM availability and full product details and support, visit the HP website (<http://www.hp.com/go/vcem>) or contact your HP representative.

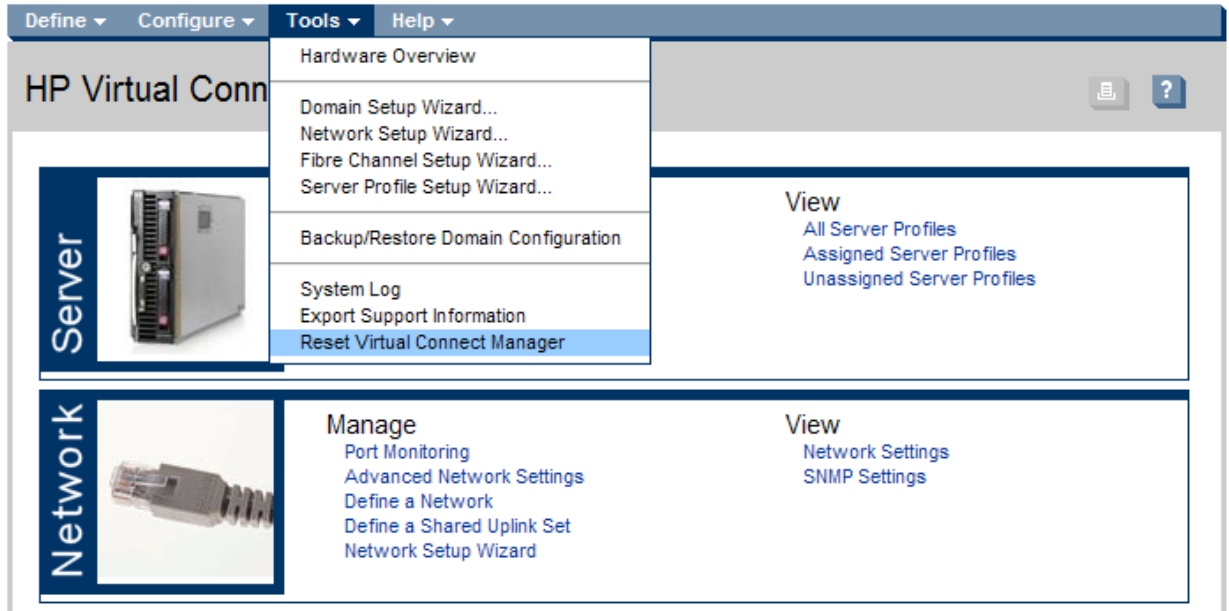
HP Smart Update Manager

An alternative method for updating VC firmware is to use the [Smart Update Firmware DVD](#) for Windows and Linux. VC firmware update support was added to the HP SUM beginning with version 3.5.0. HP SUM can deploy the VC firmware smart components using the VCSU embedded in the smart components to support VC firmware updates. If the desired version of VC firmware smart components is not included in the HP Firmware Maintenance DVD, it may be downloaded separately from HP.com website. To deploy smart components that are not on the HP Smart Update Firmware DVD, please refer to a "Deploying Components not on HP Smart Update Firmware DVD" section of the HP Smart Update Manager User Guide.

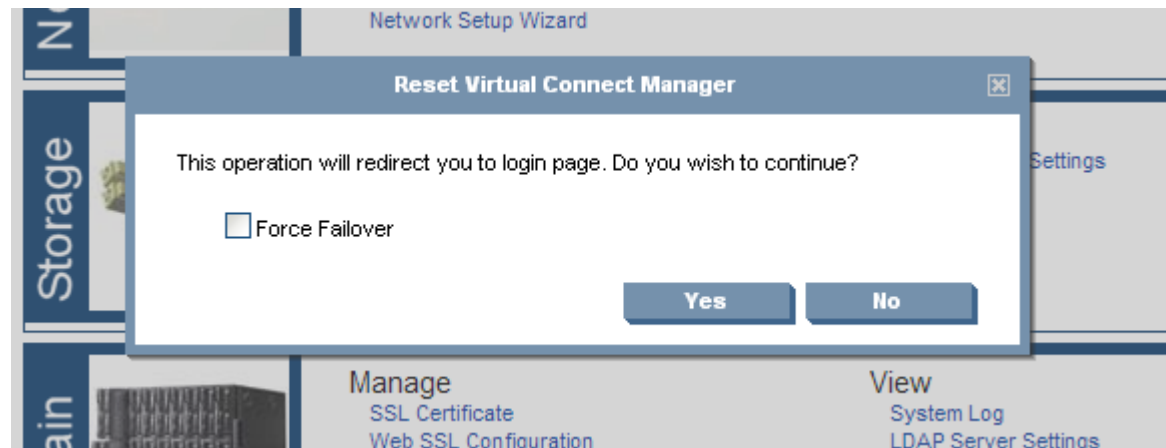
Appendix A: Resetting VC Manager

If a Reset of the Virtual Connect Manager is required or was recommended due to an incomplete or failed firmware update, please follow steps outlined below to perform this operation. The Network and FC SAN connectivity is not disturbed during reset or failover of the Virtual Connect Manager.

To reset the Virtual Connect Manager application running on the primary Virtual Connect Ethernet module from VC GUI, select "Tools→Reset Virtual Connect Manager".



The Reset Virtual Connect Manager popup is displayed.



- If the Force Failover checkbox is selected and a Virtual Connect Ethernet module is available in the horizontally adjacent IO Bay, the GUI is redirected to that Ethernet module after the Virtual Connect Manager reset operation completes.
- If the Force Failover checkbox is not selected or a Virtual Connect Ethernet module is not available in the horizontally adjacent IO Bay, the Virtual Connect Manager restarts on the current Ethernet module, and user is presented with the logon screen for the current Ethernet module after Virtual Connect Manager reset operation completes.
- Reset times depend on the size and complexity of the VC domain configuration.

To reset the Virtual Connect Manager application running on the primary Virtual Connect Ethernet module, use the **reset vcm** command:

```
> reset vcm
> reset vcm [-failover]
```

If the command line option 'failover' is included in the **reset vcm** command and a backup Virtual Connect Ethernet module is available, the command line displays the following message:

```
SUCCESS: The Virtual Connect Manager is being reset. Please wait...
```

User will be logged out of the session after approximately 1 minute. Any attempted to login to the same Virtual Connect Ethernet module will be rejected with the following error message:

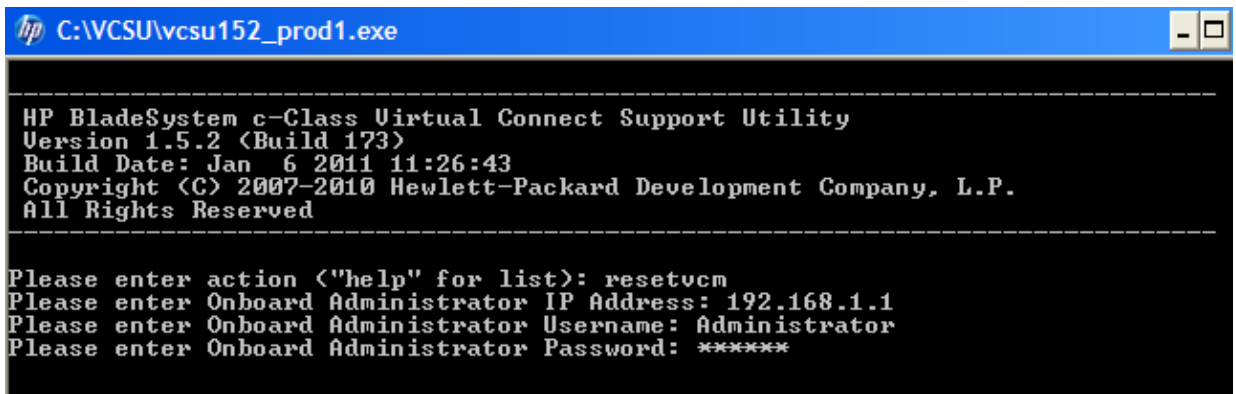
```
Virtual Connect Manager not found at this IP address.
```

Any attempted to login to the backup module will present the following error message:

```
Unable to communicate with the Virtual Connect Manager. Please retry again later.
```

Log into the specified interconnect bay and restart the Virtual Connect Manager service. This is the same process as the menu option "Reset VC Manager" from the Virtual Connect user interface.

As an alternative, the "Reset VC Manager" operation may be performed using interactive mode of VCSU v1.5.2 or later:



```
HP BladeSystem c-Class Virtual Connect Support Utility
Version 1.5.2 (Build 173)
Build Date: Jan 6 2011 11:26:43
Copyright (C) 2007-2010 Hewlett-Packard Development Company, L.P.
All Rights Reserved

Please enter action ("help" for list): resetsvc
Please enter Onboard Administrator IP Address: 192.168.1.1
Please enter Onboard Administrator Username: Administrator
Please enter Onboard Administrator Password: *****
```

Note: In a multi-enclosure environment or when redundant OA modules are present, Onboard Administrator IP Address must be the IP address of the active OA in the primary enclosure.

A VCSU non-interactive method to reset Virtual Connect Manager is also available. The following command may be used for this operation:

```
vcsu -a resetsvc -i <IP> -u <USER> -p <PWD> [-vcu <VCM USER> -vcp <VCM PASS>]
```

IP = IP Address of the active Onboard Administrator in enclosure.

USER = Name of the Onboard Administrator user with privileges to access all enclosure interconnect bays.

PWD = Password of the Onboard Administrator user. Use * to prompt for password.

VCM USER = Name of Virtual Connect user with Domain privileges required if Enclosure is in a Virtual Connect Domain. N/A if Enclosure is not in a Virtual Connect Domain.

VCM PASS = Password for VCM USER.

Example:

```
vcsu -a resetsvc -i 192.168.1.100 -u Administrator -p password
```

For more information

To read more about Virtual Connect, go to www.hp.com/go/virtualconnect

The following documents provide additional information regarding setup and operation of HP BladeSystem enclosures and HP Virtual Connect FlexFabric Modules and FlexFabric Adapters:

Deployment related resources

HP Virtual Connect Firmware 3.18 Release Notes

<http://h20000.www2.hp.com/bc/docs/support/SupportManual/c02791020/c02791020.pdf>

HP Virtual Connect for c-Class BladeSystem Setup and Installation Guide

<http://bizsupport1.austin.hp.com/bc/docs/support/SupportManual/c01732252/c01732252.pdf>

HP BladeSystem ProLiant Firmware Management Best Practices

HP BladeSystem ProLiant Firmware Management Best Practices Implementer Guide

<http://h18004.www1.hp.com/products/servers/management/literature.html>

HP BladeSystem Firmware Maintenance Website

www.hp.com/go/bladesystemupdates

HP BladeSystem c-Class Virtual Connect Support Utility Version 1.5.2 User Guide

<http://bizsupport1.austin.hp.com/bc/docs/support/SupportManual/c02657939/c02657939.pdf>

Best practice resources

HP Virtual Connect FlexFabric Cookbook

<http://h20000.www2.hp.com/bc/docs/support/SupportManual/c02616817/c02616817.pdf>

HP Virtual Connect Ethernet Cookbook: Single and Multi Enclosure Domain (Stacked) Scenarios

<http://h20000.www2.hp.com/bc/docs/support/SupportManual/c01990371/c01990371.pdf>

