# UCS 2.1 to 2.2 Upgrade Process Guide

## Enterprise Services VMware Virtualization Team

### 2015-04-13

[Cisco Language 4](#_Toc415208134)

[Cautions and Guidelines 4](#_Toc415208135)

[Domain Details 5](#_Toc415208136)

[Pre Upgrade Check List 5](#_Toc415208137)

[Compare Equipment to Release Notes for FW Compatibility 7](#_Toc415208138)

[Verify Cluster Status 7](#_Toc415208139)

[Backup UCS Domain 7](#_Toc415208140)

[(Back out) Restore Backup 7](#_Toc415208141)

[Obtaining Software Bundles from Cisco 8](#_Toc415208142)

[Downloading Firmware Images to the Fabric Interconnect from the Local File System 8](#_Toc415208143)

[Procedure 8](#_Toc415208144)

[Upgrading the Infrastructure Firmware 9](#_Toc415208145)

[Upgrade with Auto Install 10](#_Toc415208146)

[Verify the Ethernet Data Path 10](#_Toc415208147)

[Verifying the Fiber Channel End-Host Mode Data Path 11](#_Toc415208148)

[Procedure 11](#_Toc415208149)

[Upgrade the Server Firmware 13](#_Toc415208150)

[Create new Firmware Policy 13](#_Toc415208151)

[Upgrade with Auto Install 13](#_Toc415208152)

[Procedure 13](#_Toc415208153)

# Cisco Language

* Most UCS components have the ability to store 2 pieces of firmware, the “Running Version” and the “Backup Version”. The running version is the version that the component booted from, the other non-active image is the backup image.
* A UCS “Update” process pushes the firmware to the backup slot in the component, the running version is not changed.
* A UCS “Activate” process sets the firmware in the backup slot as active and reboots the component, the start-up version is set as the firmware in the backup slot and the running firmware is switched between the backup slot and the running slot at the time of the reboot.
* Some components can have the start-up version changed to the backup firmware so that next time the component is rebooted it will start with the firmware in the backup slot, but will make no change until the equipment is rebooted.
* Software bundles are required for various components, the Infrastructure bundle is required for all updates then the B series (blade), and C series (rack) are also needed depending on whether the environment contains blade and rack mounted UCS servers.

# Cautions and Guidelines

<http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/sw/upgrading/from2-1/to2-2/b_UpgradingCiscoUCSFrom2-1To2-2.html>

* Clear any faults before you upgrade the firmware.
* Not a must, but check alerts that may cause issues for upgrade.
* Default Maintenance Policy Should be Configured for User Acknowledgment
* Overlapping FCoE VLAN IDs and Ethernet VLAN IDs Are No Longer Allowed with Cisco UCS Release 2.0 and Higher
* The default Ethernet VLAN ID is 1.
* The default FCoE VLAN ID is 4048.
* No Server or Chassis Maintenance
* Do Not Activate All Endpoints Simultaneously in Cisco UCS Manager GUI
* Time, Date, and Time Zone on Fabric Interconnects Must Be Identical
* Cannot Upgrade Infrastructure and Server Firmware Simultaneously

# Domain Details

|  |  |  |  |
| --- | --- | --- | --- |
| Nodes | IP | Ping | Initial Role |
| VIP |  |  |  |
| FI-A |  |  |  |
| FI-B |  |  |  |

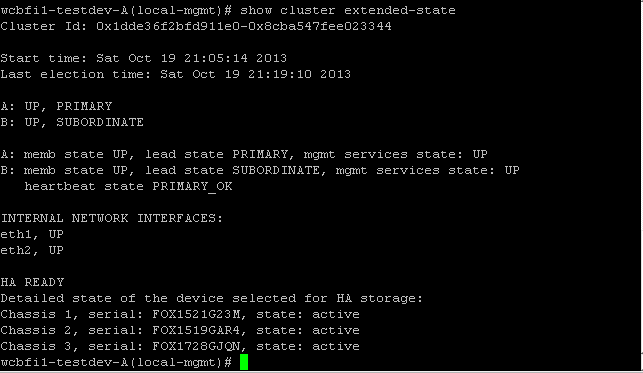
# Pre Upgrade Check List

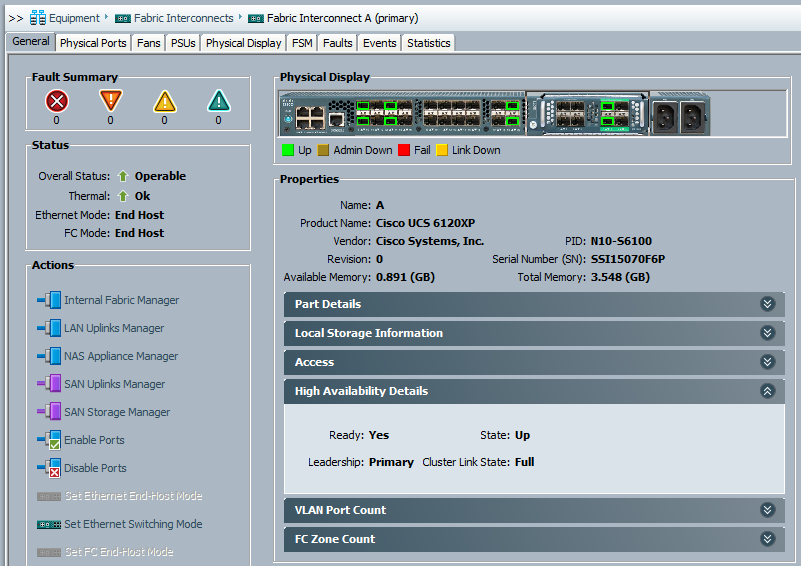
|  |  |  |
| --- | --- | --- |
| Check | Related Objects / Notes | Result |
| Current UCS Manager Version |  |  |
| Cluster HA |  | # show cluster extended-state |
| Verify Default VLAN and Default FCoE VLAN ID Do not Overlap | IMPORTANT, ALL CONNECTIVITY WILL BE LOST. Change the FCoE VLAN IF NEEDED | This change needs to occur in the appropriate maintenance window to occur, if this has not been taken care of PRE UCS Domain upgrade and was not accounted for, this will take down storage and networking connectivity for the entire environment. |
| Verify Ethernet Data Path on Each FI | Fabric A – Eth Interfaces | # show int br | grep -v down | wc -l |
| *(see section below for instructions)* | Fabric A – MAC Addresses | # show platform fwm info hw-stm | grep '1.' | wc –l |
|  | Fabric B – Eth Interfaces | # show int br | grep -v down | wc –l |
|  | Fabric B – MAC Addresses | # show platform fwm info hw-stm | grep '1.' | wc –l |
| Verify Fiber Channel Data Path on Each FI | Fabric A – Flogi Count | # show npv flogi-table |
| *(see section below for instructions)* | Fabric A – Servers Logged In | # show npv flogi-table | grep fc | wc -l |
|  | Fabric B – Flogi Count | # show npv flogi-table |
|  | Fabric B – Servers Logged In | # show npv flogi-table | grep fc | wc -l |
| Service Profile Fabric Redundancy | Verify vHBAs and vNICs |  |
| Components Supported on Target Firmware | N20-C6508 |  |
|  | 2104XP |  |
|  | 2208XP |  |
|  | B230 M1 |  |
|  | B200 M3 |  |
|  | B230 M2 |  |
|  | B22 M3 |  |
|  | M81KR   (N20-AC0002) |  |
|  | VIC 1240 (UCSB-MLOM-40G-01) |  |
|  | VIC 1280 (UCS-VIC-M82-8P) |  |
|  | 6120XP |  |
|  | 6248UP |  |
|  | 6296UP |  |
|  | 6140XP |  |
| Backup UCS Domain | Full and All Configurations |  |
| Maintenance Policy is Set to User Ack | On Service Profiles |  |
| Obtain Software Bundles From Cisco | Infrastructure and Blade Series |  |
| Upload Firmware to Fabric Interconnects | Staging |  |
| Create new Host Firmware Package | If applicable |  |
| (optional) Open Case with Cisco | A few hours before work |  |
| Remove Management Firmware Packages | No longer supported, blade firmware upgrades OR Discovery will fail if in use |  |

# Compare Equipment to Release Notes for FW Compatibility

<http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/release/notes/ucs_2_2_rn.html>

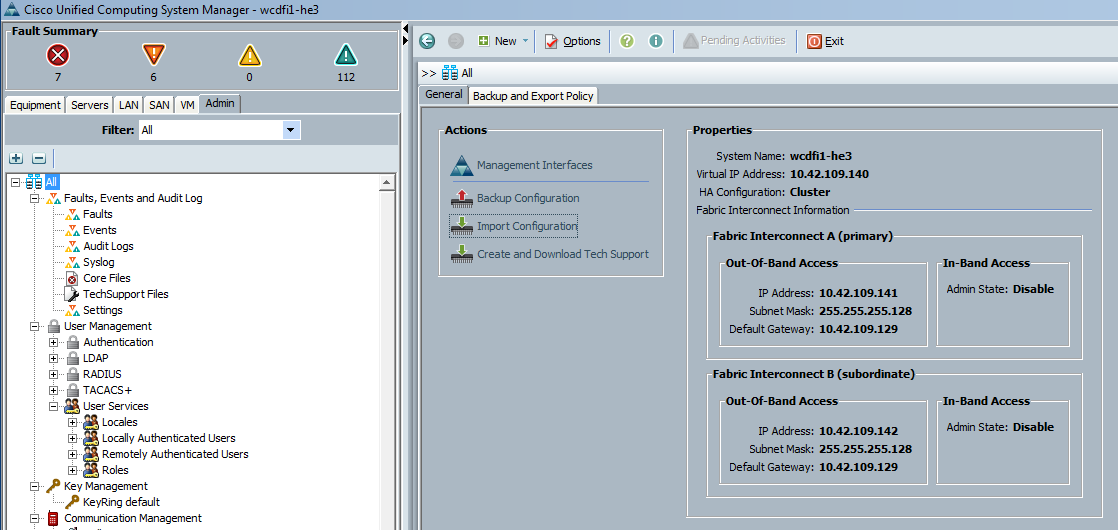
# Verify Cluster Status





# Backup UCS Domain

Full and All Configuration Backups



# (Back out) Restore Backup

Continue with upgrade fully before rolling back. Call Cisco for support to roll back.

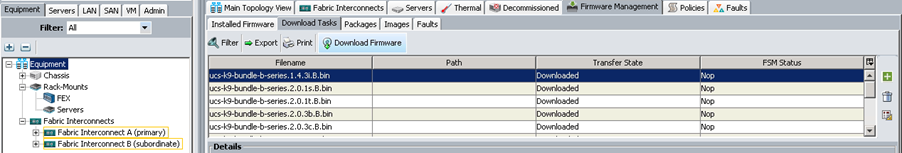
# Obtaining Software Bundles from Cisco

Download all the required software bundles, this will include the Infrastructure Bundle, and the B or C Series Bundle. The software can be downloaded from: <http://software.cisco.com/download/>.

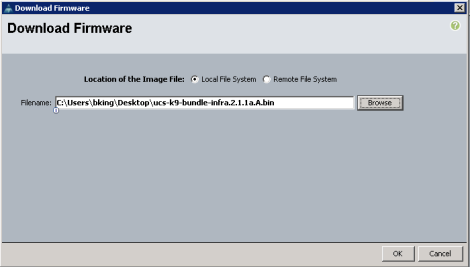
## Downloading Firmware Images to the Fabric Interconnect from the Local File System

### Procedure

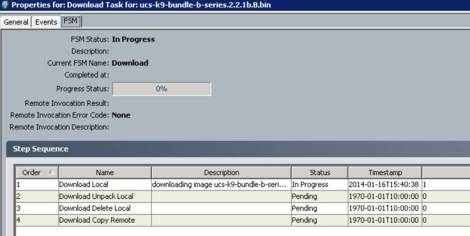
1. In the Navigation pane, click the Equipment tab.
2. On the Equipment tab, click the Equipment node.
3. In the Work pane, click the Firmware Management tab.
4. Click the Installed Firmware tab.
5. Click Download Firmware.



1. In the Download Firmware dialog box, click the Local File System radio button in the Location of the Image File field.
2. Click Browse and navigate to the location of the file:

[](http://i2.wp.com/www.bkdatacentre.com/wp-content/uploads/2014/01/image005.png)

1. Click OK
2. Cisco UCS Manager GUI begins downloading the firmware bundle to the FI
3. Repeat this task until all the required firmware bundles have been downloaded to the FI
4. Before continuing it may take a few minutes for the packages to be synchronized to the subordinate FI and unpacked, the status and tasks can be viewed from the FSM tab:

[](http://i0.wp.com/www.bkdatacentre.com/wp-content/uploads/2014/01/image004.jpg)

# Upgrading the Infrastructure Firmware

## Upgrade with Auto Install

This upgrade path requires that the pre-upgrade level of firmware in the Cisco UCS domain be at version 2.1. It is important the steps are completed in order, otherwise the update may fail or traffic may be disrupted.

There will be loss of access to UCSM for a few moments; you can utilize a continuous ping to monitor the response of USCM. Also, accessing UCSM through a browser will allow you to verify the new version is applied.

### Verify the Ethernet Data Path

1. SSH to both of the the FI’s
   1. Connect to NXOS with the command “connect nxos”
   2. The command **“show int br | grep -v down | wc –l”** will show the number of active Ethernet interfaces, record this to ensure it matches post upgrade, and repeat for the other FI.
   3. The command **“show platform fwm info hw-stm | grep ‘1.’ | wc –l”** will show the number of MAC addresses, record this to ensure it matches post upgrade, and repeat for the other FI.

[](http://i2.wp.com/www.bkdatacentre.com/wp-content/uploads/2014/01/image011.jpg)

### Verifying the Fiber Channel End-Host Mode Data Path

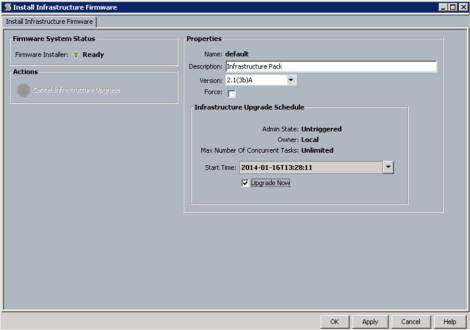
1. SSH to the FI
   1. Connect to NXOS with the command “connect nxos”
   2. The command “show npv flogi-table” will show the number of active FC logins, record this to ensure it matches post upgrade, and repeat for the other FI.
   3. The command “show npv flogi-table | grep fc | wc -l” will show the number of servers logged into the fabric interconnect, record this to ensure it matches post upgrade, and repeat for the other FI.

[](http://i2.wp.com/www.bkdatacentre.com/wp-content/uploads/2014/01/image013.jpg)

### Procedure

1. To commence the Auto Install update, In Cisco UCS Manager, choose Equipment > Firmware Management > Firmware Auto Install, click Install Infrastructure Firmware

[](http://i1.wp.com/www.bkdatacentre.com/wp-content/uploads/2014/01/image015.jpg)

1. Select the Version from the drop down menu, and click Upgrade Now tick box, and click OK[](http://i1.wp.com/www.bkdatacentre.com/wp-content/uploads/2014/01/image017.jpg)
2. This process can take some time and the subordinate FI will be rebooted as part of this process, once complete we will be prompted to reboot the primary FI by the flashing Pending Activities box, beforehand we need to verify the Ethernet Data Path to ensure that our hosts have re-established the connection to the network on the subordinate path, to do this we run the commands we ran in Verify the Ethernet Data Path on page 6 and confirm the values match the values in Verify the Ethernet Data Path on page 6.
3. Primary FI Failover Check List.

|  |  |  |
| --- | --- | --- |
| Check | Related Objects / Notes | Result |
| Cluster HA |  | # show cluster extended-state |
| Verify Ethernet Data Path on Each FI | Fabric A – Eth Interfaces | # show int br | grep -v down | wc -l |
| *(see section below for instructions)* | Fabric A – MAC Addresses | # show platform fwm info hw-stm | grep '1.' | wc –l |
|  | Fabric B – Eth Interfaces | # show int br | grep -v down | wc -l |
|  | Fabric B – MAC Addresses | # show platform fwm info hw-stm | grep '1.' | wc -l |
| Verify Fiber Channel Data Path on Each FI | Fabric A – Flogi Count | # show npv flogi-table |
| *(see section below for instructions)* | Fabric A – Servers Logged In | # show npv flogi-table | grep fc | wc -l |
|  | Fabric B – Flogi Count | # show npv flogi-table |
|  | Fabric B – Servers Logged In | # show npv flogi-table | grep fc | wc -l |

Inoperable message possible, this is normal. If it stays for longer then call Cisco. There will be loss of access again to UCSM during failover to secondary.

1. Acknowledge the reboot of the primary fabric interconnect on the User Acknowledged Activities tab of the Pending Activities dialog box.
2. Click the Pending Activities icon to open the dialog box,
3. Click the User Acknowledged Activities tab
4. Click Fabric Interconnects
5. Click Reboot Now
6. Click OK. Cisco UCS Manager immediately reboots the primary fabric interconnect. You cannot stop this reboot after you click OK.

# Upgrade the Server Firmware

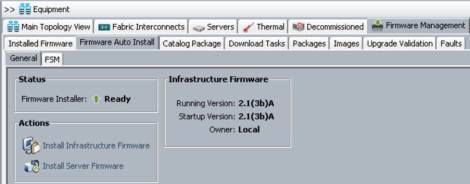
## Create new Firmware Policy

## Upgrade with Auto Install

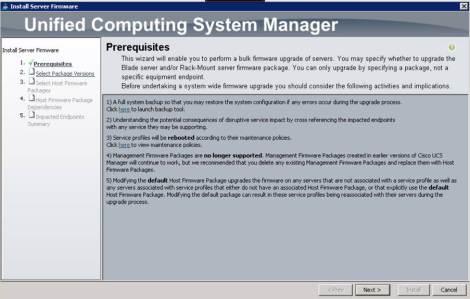
This upgrade path requires that the pre-upgrade level of firmware in the Cisco UCS domain be at version 2.1.

### Procedure

1. In Cisco UCS Manager, choose Equipment > Firmware Management > Firmware Auto Install, click Install Servers Firmware.

[](http://i1.wp.com/www.bkdatacentre.com/wp-content/uploads/2014/01/image019.jpg)

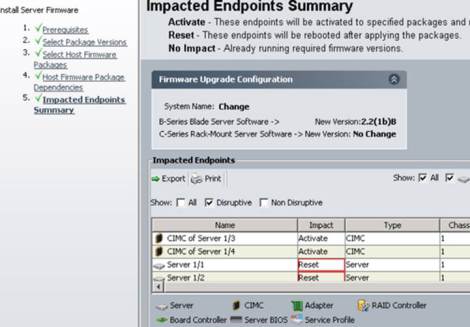
1. Review the Prerequisites and click Next

[](http://i0.wp.com/www.bkdatacentre.com/wp-content/uploads/2014/01/image021.jpg)

1. Select the required firmware version for both B and C series (if in use) and click Next.

[](http://i1.wp.com/www.bkdatacentre.com/wp-content/uploads/2014/01/image023.jpg)

1. Click on the host firmware policy, or select the root to update all servers, including those that do not have an associated service profile.
2. On Host Firmware Package Dependencies page, review the list of servers to be updated as selected in the previous step, and click Next.
3. On the Impacted Endpoints Summary page, review the list of servers that will be reset by this upgrade.

[](http://i0.wp.com/www.bkdatacentre.com/wp-content/uploads/2014/01/image027.jpg)

1. Wait for all the servers in the Cisco UCS domain to complete their upgrades.