



Completing the Prerequisites for Upgrading the Firmware

This chapter includes the following sections:

- [Prerequisites for Upgrading and Downgrading Firmware, page 1](#)
- [Creating an All Configuration Backup File, page 2](#)
- [Faults Generated Due to Reboot During the Upgrade of a Fabric Interconnect, page 4](#)
- [Verifying the Overall Status of the Fabric Interconnects, page 5](#)
- [Verifying the High Availability Status and Roles of a Cluster Configuration, page 5](#)
- [Verifying the Status of I/O Modules, page 6](#)
- [Verifying the Status of Servers, page 7](#)
- [Verifying the Status of Adapters on Servers in a Chassis, page 8](#)
- [Obtaining Cisco UCS PowerTool and Running the Duplicate IQN Script, page 8](#)

Prerequisites for Upgrading and Downgrading Firmware

All endpoints in a Cisco UCS domain must be fully functional and all processes must be complete before you begin a firmware upgrade or downgrade on those endpoints. You cannot upgrade or downgrade an endpoint that is not in a functional state. For example, the firmware on a server that has not been discovered cannot be upgraded or downgraded. An incomplete process, such as an FSM that has failed after the maximum number of retries, can cause the upgrade or downgrade on an endpoint to fail. If an FSM is in progress, Cisco UCS Manager queues up the update and activation and runs them when the FSM has completed successfully.

Colored boxes around components on the **Equipment** tab may indicate that an endpoint on that component cannot be upgraded or downgraded. Verify the status of that component before you attempt to upgrade the endpoints.



Note

The **Installed Firmware** tab in Cisco UCS Manager GUI does not provide sufficient information to complete these prerequisites.

Before you upgrade or downgrade firmware in a Cisco UCS domain, complete the following prerequisites:

- Review the Release Notes.
- Review the relevant [Hardware and Software Interoperability Matrix](#) to ensure the operating systems on all servers have the right driver levels for the release of Cisco UCS to which you plan to upgrade.
- Back up the configuration into an All Configuration backup file.
- For a cluster configuration, verify that the high availability status of the fabric interconnects shows that both are up and running.
- For a standalone configuration, verify that the Overall Status of the fabric interconnect is Operable.
- Verify that the data path is up and running. For more information, see the Verifying that the Data Path is Ready section in the appropriate [Firmware Management Guide](#).
- Verify that all servers, I/O modules, and adapters are fully functional. An inoperable server cannot be upgraded.
- Verify that the Cisco UCS domain does not include any critical or major faults. If such faults exist, you must resolve them before you upgrade the system. A critical or major fault may cause the upgrade to fail.
- Verify that all servers have been discovered. They do not need to be powered on or associated with a service profile.
- If you want to integrate a rack-mount server into the Cisco UCS domain, follow the instructions in the appropriate [C-Series Rack-Mount Server Integration Guide](#) for installing and integrating a rack-mount server in a system managed by Cisco UCS Manager.

Creating an All Configuration Backup File

This procedure assumes that you do not have an existing backup operation for an All Configuration backup file.

Before You Begin

Obtain the backup server IPv4 or IPv6 address and authentication credentials.

Procedure

-
- Step 1** In the **Navigation** pane, click **Admin**.
 - Step 2** Click the **All** node.
 - Step 3** In the **Work** pane, click the **General** tab.
 - Step 4** In the **Actions** area, click **Backup Configuration**.
 - Step 5** In the **Backup Configuration** dialog box, click **Create Backup Operation**.
 - Step 6** In the **Create Backup Operation** dialog box, do the following:
 - a) Complete the following fields:
 - **Admin State** field—Click the **Enabled** radio button to run the backup operation as soon as you click OK.

- **Type** field—Click the **All Configuration** radio button to create an XML backup file that includes all system and logical configuration information.

- **Preserve Identities** check box—If the Cisco UCS domain includes any identities derived from pools that you need to preserve, check this check box.

If this checkbox is selected for **Logical Configuration** type of backup operation, the backup file preserves all identities derived from pools, including vHBAs, WWPNs, WWNN, vNICs, MACs and UUIDs.

Note If this check box is not selected the identities will be reassigned and user labels will be lost after a restore.

- **Protocol** field—Click the one of the following radio buttons to indicate the protocol you want to use to transfer the file to the backup server:

- **FTP**

- **TFTP**

- **SCP**

- **SFTP**

- **USB A**—The USB drive inserted into fabric interconnect A.

This option is only available for certain system configurations.

- **USB B**—The USB drive inserted into fabric interconnect B.

This option is only available for certain system configurations.

- **Hostname** field—Enter the IP address or hostname of the location where the backup file is to be stored. This can be a server, storage array, local drive, or any read/write media that the fabric interconnect can access through the network. If you use a hostname, you must configure Cisco UCS Manager to use a DNS server.

- **Filename** field—Enter the full path to the backup configuration file. This field can contain the filename as well as the path. If you omit the filename, the backup procedure assigns a name to the file.

- **User** field—Enter the username that Cisco UCS Manager should use to log in to the backup location. You do not need to complete this field if you selected TFTP for the protocol.

- **Password** field—Enter the password associated with the username. You do not need to complete this field if you selected TFTP for the protocol.

b) Click **OK**.

Step 7 If Cisco UCS Manager displays a confirmation dialog box, click **OK**.

If you set the **Admin State** field to enabled, Cisco UCS Manager takes a snapshot of the configuration type that you selected and exports the file to the network location. The backup operation displays in the **Backup Operations** table in the **Backup Configuration** dialog box.

Step 8 (Optional) To view the progress of the backup operation, do the following:

- If the operation does not display in the **Properties** area, click the operation in the **Backup Operations** table.
- In the **Properties** area, click the down arrows on the **FSM Details** bar.

The **FSM Details** area expands and displays the operation status.

- Step 9** Click **OK** to close the **Backup Configuration** dialog box.
The backup operation continues to run until it is completed. To view the progress, re-open the **Backup Configuration** dialog box.
-

Faults Generated Due to Reboot During the Upgrade of a Fabric Interconnect

During firmware upgrade, to ensure proper functioning of all services on the fabric interconnect, it is essential to ensure that port configurations and services that go down when the fabric interconnect reboots are re-established after the fabric interconnect comes back up.

Cisco UCS Manager displays any service that is not re-established after the last reboot of a fabric interconnect. Cisco UCS Manager creates a baseline of the outstanding faults before a fabric interconnect is to be rebooted. After the fabric interconnect reboots and comes up, you can view the new faults generated since the last baseline to identify the services that went down because of the fabric reboot.

When a specific interval of time has passed after Cisco UCS Manager created a baseline of the outstanding faults, baselining is cleared and all faults show up as new faults. This interval is called baseline expiration interval. [Modifying Baseline Expiration Interval for Faults](#), on page 4 provides detailed information about modifying a baseline expiration interval in Cisco UCS Manager.

Cisco recommends that you resolve service-impacting faults before you continue with the fabric interconnect reboot or evacuation.

Modifying Baseline Expiration Interval for Faults

You can modify a baseline expiration interval in Cisco UCS Manager.

Procedure

- Step 1** In the **Navigation** pane, click **Admin**.
- Step 2** Expand **All > Faults, Events, and Audit Log**.
- Step 3** In the **Work** pane, click the **Settings** tab, and then click the **Global Fault Policy** subtab.
- Step 4** In the **Baseline Expiration Interval** area, update the **dd:hh:mm:ss** field.
The **dd:hh:mm:ss** field specifies the number of days, hours, minutes, and seconds that should pass before Cisco UCS Manager clears the fault baseline.
The default baseline expiration interval is 24 hours.
- Step 5** Click **Save Changes**.
-

Viewing Faults Generated During the Upgrade of a Fabric Interconnect

Procedure

- Step 1** In the **Navigation** pane, click **Admin**.
 - Step 2** Expand **All > Faults, Events, and Audit Log**.
 - Step 3** In the **Work** pane, click the **New Faults** radio button.
All faults generated after creating the baseline are displayed.
-

Verifying the Overall Status of the Fabric Interconnects

Procedure

- Step 1** In the **Navigation** pane, click **Equipment**.
 - Step 2** Expand **Equipment > Fabric Interconnects**.
 - Step 3** Click the node for the fabric interconnect that you want to verify.
 - Step 4** In the **Work** pane, click the **General** tab.
 - Step 5** In the **Status** area, verify that the **Overall Status** is **operable**.
If the status is not **operable**, create and download a Tech Support file, and contact Cisco Technical Support. Do not proceed with the firmware upgrade. For more information about Tech Support files, see the *Cisco UCS Manager B-Series Troubleshooting Guide*.
-

Verifying the High Availability Status and Roles of a Cluster Configuration

The high availability status is the same for both fabric interconnects in a cluster configuration.

Procedure

- Step 1** In the **Navigation** pane, click **Equipment**.
- Step 2** Expand **Equipment** > **Fabric Interconnects**.
- Step 3** Click the node for one of the fabric interconnects in the cluster.
- Step 4** In the **Work** pane, click the **General** tab.
- Step 5** If the fields in the **High Availability Details** area are not displayed, click the **Expand** icon to the right of the heading.
- Step 6** Verify that the following fields display the following values:

Field Name	Required Value
Ready field	Yes
State field	Up

If the values are different, create and download a Tech Support file, and contact Cisco Technical Support. Do not proceed with the firmware upgrade. For more information about Tech Support files, see the *Cisco UCS Manager B-Series Troubleshooting Guide*.

- Step 7** Note the value in the **Leadership** field to determine whether the fabric interconnect is the primary or subordinate.
You need to know this information to upgrade the firmware on the fabric interconnects.

Verifying the Status of I/O Modules

Procedure

- Step 1** In the **Navigation** pane, click **Equipment**.
- Step 2** Expand **Equipment** > **Chassis**.
- Step 3** Click on the chassis for which you want to verify the status of the I/O modules.
- Step 4** In the **Work** pane, click the **IO Modules** tab.
- Step 5** For each I/O module, verify that the following columns display the following values:

Field Name	Desired Value
Overall Status column	ok
Operability column	operable

If the values are different, create and download a Tech Support file, and contact Cisco Technical Support. Do not proceed with the firmware upgrade. For more information about Tech Support files, see the *Cisco UCS Manager B-Series Troubleshooting Guide*.

- Step 6** Repeat Steps 3 through 5 to verify the status of the I/O modules in each chassis.
-

Verifying the Status of Servers

If a server is inoperable, you can proceed with the upgrade for other servers in the Cisco UCS domain. However, you cannot upgrade the inoperable server.

Procedure

- Step 1** In the **Navigation** pane, click **Equipment**.
- Step 2** On the **Equipment** tab, click **Equipment**.
- Step 3** In the **Work** pane, click the **Servers** tab to display a list of all servers in all chassis.
- Step 4** For each server, verify that the following columns display the following values:

Field Name	Desired Value
Overall Status column	ok , unassociated , or any value that does not indicate a failure. If the value indicates a failure, such as discovery-failed , the endpoints on that server cannot be upgraded.
Operability column	operable

- Step 5** If you need to verify that a server has been discovered, do the following:
- Right-click the server for which you want to verify the discovery status and choose **Show Navigator**.
 - In the **Status Details** area of the **General** tab, verify that the **Discovery State** field displays a value of **complete**.
If the fields in the **Status Details** area are not displayed, click the **Expand** icon to the right of the heading.
-

Verifying the Status of Adapters on Servers in a Chassis

Procedure

- Step 1** In the **Navigation** pane, click **Equipment**.
- Step 2** Expand **Equipment** > **Chassis** > *Chassis Number* > **Servers**.
- Step 3** Click the server for which you want to verify the status of the adapters.
- Step 4** In the **Work** pane, click the **Inventory** tab.
- Step 5** In the **Inventory** tab, click the **Adapters** subtab.
- Step 6** For each adapter, verify that the following columns display the following values:

Field Name	Desired Value
Overall Status column	ok
Operability column	operable

If the fields show a different value and the adapter is inoperable, you can proceed with the upgrade for other adapters on the servers in the Cisco UCS domain. However, you cannot upgrade the inoperable adapter.

Obtaining Cisco UCS PowerTool and Running the Duplicate IQN Script

If a Cisco UCS domain is configured for iSCSI boot, before you upgrade from Cisco UCS, Release 2.0(1) to Cisco UCS, Release 2.0(2) or higher, you must ensure that all iSCSI vNICs used across multiple service profile have unique initiator names.

You can use a script that runs in the Cisco UCS PowerTool to determine whether a Cisco UCS configuration for iSCSI boot includes duplicate IQNs.

Procedure

- Step 1** To download Cisco UCS PowerTool, do the following:
- In your web browser, navigate to the following website: <http://developer.cisco.com/web/unifiedcomputing/microsoft>
 - Scroll down to the **Cisco UCS PowerTool (PowerShell Toolkit) Beta Download** area.
 - Download the `CiscoUcs-PowerTool-0.9.6.0.zip` file.
 - Unzip the file and follow the prompts to install Cisco UCS PowerTool.
You can install Cisco UCS PowerTool on any Windows computer. You do not need to install it on a computer used to access Cisco UCS Manager.

- Step 2** To launch Cisco UCS PowerTool, enter the following at a command line:
C:\Program Files (x86)\Cisco\Cisco UCS PowerTool>C:\Windows\System32\windowspowershell\v1.0\powershell.exe -NoExit -ExecutionPolicy RemoteSigned -File .\StartUcsPS.ps1

Example:

The following example shows what happens when you launch Cisco UCS PowerTool:

```
C:\Program Files (x86)\Cisco\Cisco UCS PowerTool>C:\Windows\System32\windowspowershell\v1.0\powershell.exe -NoExit -ExecutionPolicy RemoteSigned -File .\StartUcsPS.ps1
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.
```

- Step 3** In Cisco UCS PowerTool, do the following:

- a) Connect to Cisco UCS Manager, as follows:

```
PS C:\> Connect-Ucs IP_address
```

- b) Enter your username and password when prompted for your credential as shown in the following example:

```
cmdlet Connect-Ucs at command pipeline position 1
```

Supply values for the following parameters:

Credential

Cisco UCS PowerTool outputs the following to your screen after you log in.

```
Cookie           : 1331303969/2af0afde-6627-415c-b85f-a7cae6233de3
Domains          :
LastUpdateTime   : 3/9/2012 6:20:42 AM
Name             : 209.165.201.15
NoSsl            : False
NumPendingConfigs : 0
NumWatchers      : 0
Port             : 443
Priv             : {admin, read-only}
RefreshPeriod    : 600
SessionId        : web_49846_A
TransactionInProgress : False
Ucs              : ucs-4
Uri              : https://209.165.201.15
UserName         : admin
VirtualIpv4Address : 209.165.201.15
Version          : 2.0(2i)3.0(1a)
WatchThreadStatus : None
```

- Step 4** In the Cisco UCS PowerTool, run the following script to validate your iSCSI boot configuration and check for duplicate IQNs :

```
PS C:\> Get-UcsServiceProfile -type instance | Get-UcsVnicIscsi | ? { $_.InitiatorName -ne "" } | select Dn,InitiatorName | group InitiatorName | ? { $_.Count -gt 1 } | % { $obj = New-Object PSObject ; $obj | Add-Member NoteProperty Count $_.Count; $obj | Add-Member NoteProperty InitiatorName $_.Name; $obj | Add-Member NoteProperty Dn ($_ | select -exp Group | % { $_.Dn } ); $obj }
```

Cisco UCS PowerTool outputs the results to your screen, as follows:

```
Count InitiatorName Dn
----
2 iqn.2012-01.cisco.com:s... {org-root/ls-SP_1_6/is...
2 iqn.2012-01.cisco.com:s... {org-root/ls-SP_2_1/is...
```

```
2 iqn.2012-01.cisco.com:s... {org-root/ls-SP_2_41/i...
4 iqn.2012-01.cisco.com:s... {org-root/ls-SP_2_7/is...
2 iqn.2012-01.cisco.com:s... {org-root/org-sub1/ls-...
2 iqn.2012-01.cisco.com:s... {org-root/org-sub2/ls-...
```

Step 5 (Optional) If you have .NET Framework 3.5 Service Pack 1 installed, you can use the following script to view the output in the GUI:

```
PS C:\> Get-UcsServiceProfile -type instance | Get-UcsVnicIscsi | ? { $_.InitiatorName -ne "" } | select
Dn,InitiatorName | group InitiatorName | ? { $_.Count -gt 1 } | % { $obj = New-Object PSObject ; $obj
| Add-Member NoteProperty Count $_.Count; $obj | Add-Member NoteProperty InitiatorName $_.Name;
$obj | Add-Member NoteProperty Dn ($_ | select -exp Group | % { $_.Dn } ); $obj } | ogv
```

Step 6 Disconnect from Cisco UCS Manager, as follows:

```
PS C:\> Disconnect-Ucs
```

What to Do Next

If duplicate IQNs exist across multiple service profiles in the Cisco UCS domain, reconfigure the iSCSI vNICs with unique IQNs in Cisco UCS Manager before you upgrade to Cisco UCS, Release 2.1 or greater.

If you do not ensure that all iSCSI vNICs are unique across all service profiles in a Cisco UCS domain before you upgrade, Cisco UCS Manager raises a fault on the iSCSI vNICs to warn you that duplicate IQNs are present. Also, if you do not ensure that there are no duplicate IQN names within a service profile (for example, the same name used for both iSCSI vNICs), Cisco UCS reconfigures the service profile to have a single IQN. For information on how to clear this fault and reconfigure the duplicate IQNs, see the [Cisco UCS B-Series Troubleshooting Guide](#).