Upgrading the Firmware to Release 1.4(3)

This chapter includes the following sections:

Required Order of Steps When Upgrading from Release 1.4(1) or 1.4(2)

Note If you do not follow this order, the firmware upgrade may fail and the servers may experience communication issues with Cisco UCS Manager.

The order of steps in this document and the recommended options minimize the disruption to data traffic. Therefore, when you upgrade from any version of release 1.4 to a later version of release 1.4, upgrade the components in the following order.

1 Download the following firmware images:

- Cisco UCS Infrastructure Software Bundle—Required for all Cisco UCS instances.

- Cisco UCS B-Series Blade Server Software Bundle—Required for all Cisco UCS instances that include blade servers.
- Cisco UCS C-Series Rack-Mount Server Software Bundle—Only required for Cisco UCS instances that include integrated rack-mount servers. This bundle contains firmware to enable Cisco UCS Manager to manage those servers and is not applicable to standalone C-Series rack-mount servers.

2. (Optional) Disable Call Home—If the Cisco UCS instance includes Call Home or Smart Call Home, disable Call Home to ensure you do not receive unnecessary alerts when Cisco UCS Manager restarts components.
3. Update adapters, CIMC, and IOMs—If you prefer, you can upgrade the adapters in a host firmware package as part of the last upgrade step.
4. Activate adapters—Choose **Ignore Compatibility Check** and **Set Startup Version Only** when performing this step.
5. Activate CIMC—Choose **Ignore Compatibility Check** when performing this step.
6. Activate Cisco UCS Manager—Choose **Ignore Compatibility Check** when performing this step.
7. Activate I/O modules—Choose **Ignore Compatibility Check** and **Set Startup Version Only** when performing this step.
8. Activate subordinate fabric interconnect—Choose **Ignore Compatibility Check** when performing this step.
9. Verify that the data path has been restored.
10. Activate primary fabric interconnect—Choose **Ignore Compatibility Check** when performing this step.
11. Update management firmware package(s) for servers—You do not need to perform this step if you updated and activated the CIMC on the servers directly.
12. Update host firmware package(s) for servers—Must be the last firmware upgraded. We recommend that you upgrade the board controller firmware during this step to avoid an additional reboot of servers with that firmware. You must upgrade the following firmware in a host firmware package:
    - BIOS
    - Storage controller
    - Certain adapters
13. (Optional) Enable Call Home—If you disabled Call Home before the upgrading the firmware, enable Call Home.

Disabling Call Home

This step is optional.

When you upgrade a Cisco UCS instance, Cisco UCS Manager restarts the components to complete the upgrade process. This restart causes events that are identical to service disruptions and component failures that trigger Call Home alerts to be sent. If you do not disable Call Home before you begin the upgrade, you can ignore the alerts generated by the upgrade-related component restarts.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, expand **All** > **Communication Management** > **Call Home**.

Step 3 In the **Work** pane, click the **General** tab.

Step 4 In the **Admin** area, click **off** in the **State** field.

Note If this field is set to **off**, Cisco UCS Manager hides the rest of the fields on this tab.

Step 5 Click **Save Changes**.

Updating the Firmware on the Adapters, CIMCs, and IOMs

Caution Do not remove the hardware that contains the endpoint or perform any maintenance on it until the update process has completed. If the hardware is removed or otherwise unavailable due to maintenance, the firmware update fails. This failure may corrupt the backup partition. You cannot update the firmware on an endpoint with a corrupted backup partition.

Before You Begin

This procedure describes how to update the firmware on all of these endpoints in a Cisco UCS system simultaneously. Before you begin this procedure, answer the following questions to determine the appropriate type of upgrade for each of these endpoints:

- Are all endpoints configured with the same backup version? If yes, continue with the next question. If no, update all backup versions to the same firmware version before continuing.
- Does the service profile associated with one or more of the servers include a host or management firmware package? If yes, update the firmware for that server through the firmware packages. You can update all other firmware and servers through this procedure. If no, continue with the next question.

  If you want to update the firmware for a server directly, you must remove all host and management firmware packages from the associated service profiles. Removing the firmware from the host or management firmware package does not enable you to update them directly.
- Does the server include a Cisco UCS gen-2 adapter? If yes, you must update the adapter firmware for that server through the host firmware package. If no, you can use this procedure for that server.

Even if you answered yes to either of the last two questions above, you can use this procedure to update the I/O modules and any servers for which you answered no.

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, click the **Equipment** node.

Step 3 In the **Work** pane, click the **Firmware Management** tab.

Step 4 On the **Installed Firmware** subtab, click **Update Firmware**.
Cisco UCS Manager GUI opens the **Update Firmware** dialog box and verifies the firmware versions for all endpoints in the Cisco UCS instance. This step may take a few minutes, depending upon the number of chassis and servers.

Step 5 In the **Update Firmware** dialog box, do the following:

a) From the **Filter** drop-down list on the menu bar, choose **ALL**.
If you would prefer to update one type of endpoint at a time, choose that endpoint from the **Filter** drop-down list.

b) From the **Set Version** drop-down list on the menu bar, choose the firmware version included in the Release 1.4(3) firmware bundle from the drop-down list.

c) Click **Apply** to begin the updates and leave the dialog box open so you can monitor the progress of the updates to each endpoint.
If one or more endpoints cannot be directly updated, Cisco UCS Manager displays a notification message. After you acknowledge the notification message, Cisco UCS Manager updates the firmware for all other endpoints on servers that can be directly updated.

Cisco UCS Manager copies the selected firmware image to the backup memory partition and verifies that the image is not corrupt. The image remains as the backup version until you explicitly activate it. Cisco UCS Manager begins all updates at the same time. However, some updates may complete at different times.

The update is complete when the **Update Firmware** dialog box displays **ready** in the **Update Status** column for all updated endpoints.

Step 6 When all updates are completed, click **OK**.

What to Do Next

Activate the firmware.

Activating the Firmware on the Adapters and CIMCs

This procedure ensures that the firmware activation for these endpoints causes minimal disruption to data traffic. If you do not activate the endpoints in the following order with the correct options configured, the endpoints may reboot and cause a temporary disruption in data traffic.

Caution Do not select **ALL** from the **Filter** drop-down list in the **Activate Firmware** dialog box to activate all endpoints simultaneously. Many firmware releases and patches have dependencies that require the endpoints to be activated in a specific order for the firmware update to succeed. This order can change depending upon the contents of the release or patch. Activating all endpoints does not guarantee that the updates occur in the required order and can disrupt communications between the endpoints, the fabric interconnects, and Cisco UCS Manager. For information about the dependencies in a specific release or patch, see the release notes provided with that release or patch.

This procedure continues directly from the previous one and assumes you are on the **Firmware Management** tab.

Procedure

Step 1 In the **Installed Firmware** tab, choose **Activate Firmware**.
If one or more of the selected endpoints are not configured with the desired version as the backup version, Cisco UCS Manager GUI does not display that version in the **Set Version** drop-down list. You must select the version from the **Startup Version** column for each individual endpoint.

Step 2 If the adapter firmware is not updated through a host firmware package in a service profile, do the following in the **Activate Firmware** dialog box to activate the adapter firmware:

a) From the **Filter** drop-down list, choose **Adapters**.
b) From the **Set Version** drop-down list, choose the firmware version included in the Release 1.4(3) firmware bundle.
c) Check the **Ignore Compatibility Check** check box.
The firmware for this release is not compatible with previous releases. Therefore, you must check the **Ignore Compatibility Check** check box to ensure that the activation succeeds.
d) Check the **Set Startup Version Only** check box.

Note During a direct upgrade, you should configure **Set Startup Version Only** for an adapter. With this setting, the activated firmware moves into the pending-next-boot state, and the server is not immediately rebooted. The activated firmware does not become the running version of firmware on the adapter until the server is rebooted. You cannot configure **Set Startup Version Only** for an adapter in the host firmware package.

e) Click **Apply**.
When the **Activate Status** column for all adapters displays **pending-next-boot** or **ready**, continue with Step 3.

Step 3 If the CIMC firmware is not updated through a management firmware package in a service profile, do the following in the **Activate Firmware** dialog box to activate the CIMC firmware:

a) From the **Filter** drop-down list, choose **CIMC**.
b) From the **Set Version** drop-down list, choose the firmware version included in the Release 1.4(3) firmware bundle.
If one or more of the selected endpoints are not configured with the desired version as the backup version, Cisco UCS Manager GUI does not display that version in the **Set Version** drop-down list. You must select the version from the **Startup Version** column for each individual endpoint.
c) Check the **Ignore Compatibility Check** check box.
d) Click **Apply**.

The activation of firmware for a CIMC does not disrupt data traffic. However, it will interrupt all KVM sessions and disconnect any vMedia attached to the server.

When the **Activate Status** column for all CIMC components displays **ready** continue with Step 4.

Step 4 Click **OK**.

Activating the Board Controller Firmware on a Server

Only certain servers, such as the Cisco UCS B440 High Performance blade server and the Cisco UCS B230 blade server, have board controller firmware. The board controller firmware controls many of the server functions, including eUSBs, LEDs, and I/O connectors.

This procedure continues from the previous one and assumes that you are on the **Installed Firmware** tab.

Note This activation procedure causes the server to reboot. Depending upon whether or not the service profile associated with the server includes a maintenance policy, the reboot can occur immediately. To reduce the number of times a server needs to be rebooted during the upgrade process, we recommend that you upgrade the board controller firmware through the host firmware package in the service profile.

Procedure

Step 1 On the **Installed Firmware** subtab, click **Activate Firmware**.
Cisco UCS Manager GUI opens the **Update Firmware** dialog box and verifies the firmware versions for all endpoints in the Cisco UCS instance. This step may take a few minutes, depending upon the number of chassis and servers.

Step 2 From the **Filter** drop-down list on the menu bar of the **Activate Firmware** dialog box, select **Board Controller**.
Cisco UCS Manager GUI displays all servers that have board controllers in the **Activate Firmware** dialog box.

Step 3 From the **Set Version** drop-down list on the menu bar of the **Activate Firmware** dialog box, choose the board controller firmware version included in the Release 1.4(3) firmware bundle.

Step 4 Check the **Ignore Compatibility Check** check box.

Step 5 Click **OK**.

Activating the Cisco UCS Manager Software to Release 1.4

This procedure continues directly from the previous one and assumes you are on the **Firmware Management** tab.

Procedure

Step 1 On the **Installed Firmware** subtab, click **Activate Firmware**.
Cisco UCS Manager GUI opens the **Update Firmware** dialog box and verifies the firmware versions for all endpoints in the Cisco UCS instance. This step may take a few minutes, depending upon the number of chassis and servers.

Step 2 From the **Filter** drop-down list, choose **UCS Manager**.

Step 3 On the **UCS Manager** row of the **Activate Firmware** dialog box, do the following:

a) From the drop-down list in the **Startup Version** column, select the firmware version included in the Release 1.4 firmware bundle from the drop-down list.

b) Check the **Ignore Compatibility Check** check box.

Step 4 Click **OK**.
Cisco UCS Manager disconnects all active sessions, logs out all users, and activates the software. When the upgrade is complete, you are prompted to log back in.

Activating the Firmware on the IOMs to Release 1.4

This procedure ensures that the firmware activation for these endpoints causes minimal disruption to data traffic. If you do not activate the endpoints in the following order with the correct options configured, the endpoints may reboot and cause a temporary disruption in data traffic.

Caution Do not select **ALL** from the **Filter** drop-down list in the **Activate Firmware** dialog box to activate all endpoints simultaneously. Many firmware releases and patches have dependencies that require the endpoints to be activated in a specific order for the firmware update to succeed. This order can change depending upon the contents of the release or patch. Activating all endpoints does not guarantee that the updates occur in the required order and can disrupt communications between the endpoints, the fabric interconnects, and Cisco UCS Manager. For information about the dependencies in a specific release or patch, see the release notes provided with that release or patch.

This procedure continues directly from the previous one and assumes you are on the **Firmware Management** tab.

Procedure

Step 1 In the **Installed Firmware** tab, choose **Activate Firmware**.
If one or more of the selected endpoints are not configured with the desired version as the backup version, Cisco UCS Manager GUI does not display that version in the **Set Version** drop-down list. You must select the version from the **Startup Version** column for each individual endpoint.

Step 2 To activate the IOM firmware, do the following in the **Activate Firmware** dialog box:

a) From the **Filter** drop-down list, choose **IO Modules**.

b) From the **Set Version** drop-down list, select the firmware version included in the Release 1.4 firmware bundle.
c) Check the **Ignore Compatibility Check** check box.
d) Check the **Set Startup Version Only** check box.

Important When you configure **Set Startup Version Only** for an I/O module, the I/O module is rebooted when the fabric interconnect in its data path is rebooted. If you do not configure **Set Startup Version Only** for an I/O module, the I/O module reboots and disrupts traffic. In addition, if Cisco UCS Manager detects a protocol and firmware version mismatch between the fabric interconnect and the I/O module, Cisco UCS Manager automatically updates the I/O module with the firmware version that matches the firmware in the fabric interconnect and then activates the firmware and reboots the I/O module again.

e) Click **Apply**.

Step 3 When the **Activate Status** column for all IOMs displays **pending-next-boot**, click **OK**.

Activating the Fabric Interconnect Firmware for a Cluster Configuration

Activating the Firmware on a Subordinate Fabric Interconnect to Release 1.4

Before You Begin

Determine which fabric interconnect in the cluster is the subordinate fabric interconnect. For more information, see Verifying the High Availability Status and Roles of a Cluster Configuration.

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.
Step 2 On the **Equipment** tab, click the **Equipment** node.
Step 3 In the **Work** pane, click the **Firmware Management** tab.
Step 4 On the **Installed Firmware** subtab, click **Activate Firmware**.
Cisco UCS Manager GUI opens the **Update Firmware** dialog box and verifies the firmware versions for all endpoints in the Cisco UCS instance. This step may take a few minutes, depending upon the number of chassis and servers.
Step 5 From the **Filter** drop-down list on the menu bar, choose **Fabric Interconnects**.
Step 6 On the menu bar, check the **Ignore Compatibility Check** check box.
Step 7 On the row of the **Activate Firmware** dialog box for the subordinate fabric interconnect, do the following:
a) In the **Kernel** row, choose the firmware version included in the Release 1.4 firmware bundle from the drop-down list in the **Startup Version** column.
b) In the **System** row, choose the firmware version included in the Release 1.4 firmware bundle from the drop-down list in the **Startup Version** column.
Step 8 Click **Apply**.

Cisco UCS Manager updates and activates the firmware and reboots the fabric interconnect and any I/O module in the data path to that fabric interconnect, disrupting data traffic to and from that fabric interconnect. However, assuming the Cisco UCS instance is configured to permit traffic and port failover, data traffic fails over to the primary fabric interconnect and is not disrupted.

Step 9 Verify the high availability status of the subordinate fabric interconnect.

Note If the **High Availability Details** area for the fabric interconnect does not show the following values, contact Cisco Technical Support immediately. Do not continue to update the primary fabric interconnect.

Field Name	Required Value
Ready field	**Yes**
State field	**Up**

What to Do Next

If the high availability status of the subordinate fabric interconnect contains the required values, update and activate the primary fabric interconnect.

Verifying that the Data Path is Ready

Before you continue to the next step in the upgrade, you must verify that the data path for the new the primary fabric interconnect has been restored and is ready to handle data traffic.

Verifying that Dynamic vNICs Are Up and Running

When you upgrade a Cisco UCS that includes dynamic vNICs and an integration with VMware vCenter, you must verify that all dynamic VNICs are up and running on the new primary fabric interconnect before you activate the new software on the former primary fabric interconnect to avoid data path disruption.

Perform this step in the Cisco UCS Manager GUI.

Procedure

Step 1 In the **Navigation** pane, click the **VM** tab.

Step 2 On the **VM** tab, expand **All** > **VMware** > **Virtual Machines**.

Step 3 Expand the virtual machine for which you want to verify the dynamic vNICs and choose a dynamic vNIC.

Step 4 In the **Work** pane, click the **VIF** tab.

Step 5 On the **VIF** tab, verify that the **Status** column for each VIF is **Online**.

Step 6 Repeat Steps 3 through 5 until you have verified that the VIFs for all dynamic vNICs on all virtual machines have a status of **Online**.

Verifying the Ethernet Data Path

Procedure

	Command or Action	Purpose
Step 1	UCS-A /fabric-interconnect # **connect nxos** {**a** | **b**}	Enters NX-OS mode for the fabric interconnect.
Step 2	UCS-A(nxos)# **show int br | grep -v down | wc –1**	Returns the number of active Ethernet interfaces. Verify that this number matches the number of Ethernet interfaces that were up prior to the upgrade.
Step 3	UCS-A(nxos)# **show platform fwm info hw-stm | grep '1.' | wc –1**	Returns the total number of MAC addresses. Verify that this number matches the number of MAC addresses prior to the upgrade.

The following example returns the number of active Ethernet interfaces and MAC addresses for subordinate fabric interconnect A so that you can verify that the Ethernet data path for that fabric interconnect is up and running:

```
UCS-A /fabric-interconnect # connect nxos a
UCS-A(nxos)# show int br | grep -v down  | wc -l
86
UCS-A(nxos)# show platform fwm info hw-stm | grep '1.' | wc -l
80
```

Verifying the Data Path for Fibre Channel End-Host Mode

For best results when upgrading a Cisco UCS instance, we recommend that you perform this task before you begin the upgrade and after you activate the subordinate fabric interconnect, and then compare the two results.

Procedure

	Command or Action	Purpose
Step 1	UCS-A /fabric-interconnect # **connect nxos** {**a** | **b**}	Enters NX-OS mode for the fabric interconnect.
Step 2	UCS-A(nxos)# **show npv flogi-table**	Displays a table of flogi sessions.
Step 3	UCS-A(nxos)# **show npv flogi-table | grep fc | wc -1**	Returns the number of servers logged into the fabric interconnect. The output should match the output you received when you performed this verification prior to beginning the upgrade.

The following example displays the flogi-table and number of servers logged into subordinate fabric interconnect A so that you can verify that the Fibre Channel data path for that fabric interconnect in Fibre Channel End-Host mode is up and running:

```
UCS-A /fabric-interconnect # connect nxos a
UCS-A(nxos)# show npv flogi-table
--------------------------------------------------------------------------------
SERVER                                                                  EXTERNAL
INTERFACE VSAN FCID            PORT NAME               NODE NAME       INTERFACE
--------------------------------------------------------------------------------
vfc705    700  0x69000a 20:00:00:25:b5:27:03:01 20:00:00:25:b5:27:03:00 fc3/1
vfc713    700  0x690009 20:00:00:25:b5:27:07:01 20:00:00:25:b5:27:07:00 fc3/1
vfc717    700  0x690001 20:00:00:25:b5:27:08:01 20:00:00:25:b5:27:08:00 fc3/1

Total number of flogi = 3.

UCS-A(nxos)# show npv flogi-table | grep fc | wc -l
3
```

Verifying the Data Path for Fibre Channel Switch Mode

For best results when upgrading a Cisco UCS instance, we recommend that you perform this task before you begin the upgrade and after you activate the subordinate fabric interconnect, and then compare the two results.

Procedure

	Command or Action	Purpose
Step 1	UCS-A /fabric-interconnect # **connect nxos** {**a** | **b**}	Enters NX-OS mode for the fabric interconnect.
Step 2	UCS-A(nxos)# **show flogi database**	Displays a table of flogi sessions.
Step 3	UCS-A(nxos)# **show flogi database | grep –I fc | wc –1**	Returns the number of servers logged into the fabric interconnect. The output should match the output you received when you performed this verification prior to beginning the upgrade.

The following example displays the flogi-table and number of servers logged into subordinate fabric interconnect A so that you can verify that the Fibre Channel data path for that fabric interconnect in Fibre Channel End-Host mode is up and running:

```
UCS-A /fabric-interconnect # connect nxos a
UCS-A(nxos)# show flogi database
--------------------------------------------------------------------------------
INTERFACE        VSAN    FCID           PORT NAME               NODE NAME
--------------------------------------------------------------------------------
vfc726           800   0xef0003  20:00:00:25:b5:26:07:02 20:00:00:25:b5:26:07:00
vfc728           800   0xef0007  20:00:00:25:b5:26:07:04 20:00:00:25:b5:26:07:00
vfc744           800   0xef0004  20:00:00:25:b5:26:03:02 20:00:00:25:b5:26:03:00
vfc748           800   0xef0005  20:00:00:25:b5:26:04:02 20:00:00:25:b5:26:04:00
vfc764           800   0xef0006  20:00:00:25:b5:26:05:02 20:00:00:25:b5:26:05:00
vfc768           800   0xef0002  20:00:00:25:b5:26:02:02 20:00:00:25:b5:26:02:00
vfc772           800   0xef0000  20:00:00:25:b5:26:06:02 20:00:00:25:b5:26:06:00
vfc778           800   0xef0001  20:00:00:25:b5:26:01:02 20:00:00:25:b5:26:01:00
```

```
Total number of flogi = 8.
UCS-A(nxos)# show flogi database | grep fc | wc -l
8
```

Activating the Firmware on a Primary Fabric Interconnect to Release 1.4

This procedure continues directly from the previous one and assumes you are on the **Firmware Management** tab.

Before You Begin

Activate the subordinate fabric interconnect.

Procedure

Step 1 On the **Installed Firmware** subtab, click **Activate Firmware**.
Cisco UCS Manager GUI opens the **Update Firmware** dialog box and verifies the firmware versions for all endpoints in the Cisco UCS instance. This step may take a few minutes, depending upon the number of chassis and servers.

Step 2 From the **Filter** drop-down list on the menu bar, choose **Fabric Interconnects**.

Step 3 On the menu bar, check the **Ignore Compatibility Check** check box.

Step 4 On the row of the **Activate Firmware** dialog box for the primary fabric interconnect, do the following:

a) In the **Kernel** row, choose the firmware version included in the Release 1.4 firmware bundle from the drop-down list in the **Startup Version** column.

b) In the **System** row, choose the firmware version included in the Release 1.4 firmware bundle from the drop-down list in the **Startup Version** column.

Step 5 Click **Apply**.
Cisco UCS Manager updates and activates the firmware and reboots the fabric interconnect and any I/O module in the data path to that fabric interconnect, disrupting data traffic to and from that fabric interconnect. However, assuming the Cisco UCS instance is configured to permit traffic and port failover, data traffic fails over to the other fabric interconnect, which becomes the primary. When it comes back up, this fabric interconnect is the subordinate fabric interconnect.

Step 6 Verify the high availability status of the fabric interconnect.

Note If the **High Availability Details** area for the fabric interconnect does not show the following values, contact Cisco Technical Support immediately.

Field Name	Required Value
Ready field	**Yes**
State field	**Up**

Activating the Firmware on a Standalone Fabric Interconnect to Release 1.4

For a standalone configuration with a single fabric interconnect, you can minimize the disruption to data traffic when you perform a direct firmware upgrade of the endpoints. However, you must reboot the fabric interconnect to complete the upgrade and, therefore, cannot avoid disrupting traffic.

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, click the **Equipment** node.

Step 3 In the **Work** pane, click the **Firmware Management** tab.

Step 4 On the **Installed Firmware** subtab, click **Activate Firmware**.
Cisco UCS Manager GUI opens the **Update Firmware** dialog box and verifies the firmware versions for all endpoints in the Cisco UCS instance. This step may take a few minutes, depending upon the number of chassis and servers.

Step 5 From the **Filter** drop-down list, choose **Fabric Interconnects**.

Step 6 On the menu bar, check the **Ignore Compatibility Check** check box.

Step 7 On the row of the **Activate Firmware** dialog box for the fabric interconnect, do the following:

a) In the **Kernel** row, choose the firmware version included in the Release 1.4 firmware bundle from the drop-down list in the **Startup Version** column.

b) In the **System** row, choose the firmware version included in the Release 1.4 firmware bundle from the drop-down list in the **Startup Version** column.

Step 8 Click **OK**.

Cisco UCS Manager activates the firmware and reboots the fabric interconnect and any I/O module in the data path to that fabric interconnect. For a standalone fabric interconnect, this disrupts all data traffic in the Cisco UCS instance.

Updating Host and Management Firmware Packages

Effect of Updates to Host Firmware Packages and Management Firmware Packages

To update firmware through a host firmware package or a management firmware package, you need to update the firmware in the package. What happens after you save the changes to a host or management firmware package depends upon how the Cisco UCS instance is configured.

The following table describes the most common options for upgrading servers with a host or management firmware package.

Note Maintenance policies are available in Cisco UCS, Release 1.4 and later.

Service Profile	Maintenance Policy	Upgrade Actions
Host or management firmware package is not included in a service profile or an updating service profile template. OR You want to upgrade the firmware without making any changes to the existing service profile or updating service profile template.	No maintenance policy	After you update the firmware package, do one of the following: • To reboot and upgrade some or all servers simultaneously, follow the procedure in the Cisco UCS Manager configuration guides for the appropriate release to add the firmware package to one or more service profiles that are associated with servers or to an updating service profile template. • To reboot and upgrade one server at a time, do the following for each server: **1** Create a new service profile and include the firmware package in that service profile. **2** Dissociate the server from its service profile. **3** Associate the server with the new service profile. **4** After the server has been rebooted and the firmware upgraded, disassociate the server from the new service profile and associate it with its original service profile. **Caution** If the original service profile includes a scrub policy, this procedure may result in data loss when the disk or the BIOS is scrubbed upon association with the new service profile.

Service Profile	Maintenance Policy	Upgrade Actions
Host or management firmware package is included in one or more service profiles, and the service profiles are associated with one or more servers. OR Host or management firmware package is included in an updating service profile template, and the service profiles created from that template are associated with one or more servers.	No maintenance policy OR A maintenance policy configured for immediate updates.	The following occurs when you update the firmware package: **1** The changes to the firmware package take effect as soon as you save them. **2** Cisco UCS Manager verifies the model numbers and vendor against all servers associated with service profiles that include this policy. If the model numbers and vendor match a firmware version in the policy, Cisco UCS Manager reboots the servers and updates the firmware. All servers associated with service profiles that include the firmware package are rebooted at the same time.
Host or management firmware package is included in one or more service profiles, and the service profiles are associated with one or more servers. OR Host or management firmware package is included in an updating service profile template, and the service profiles created from that template are associated with one or more servers.	Configured for user acknowledgment	The following occurs when you update the firmware package: **1** Cisco UCS Manager asks you to confirm your change and advises that a user-acknowledged reboot of the servers is required. **2** Click the flashing **Pending Activities** button to select the servers you want to reboot and apply the new firmware. **3** Cisco UCS Manager verifies the model numbers and vendor against all servers associated with service profiles that include this policy. If the model numbers and vendor match a firmware version in the policy, Cisco UCS Manager reboots the server and updates the firmware. A manual reboot of the servers does not cause Cisco UCS Manager to apply the firmware package, nor does it cancel the pending activities. You must acknowledge or cancel the pending activity through the **Pending Activities** button.

Service Profile	Maintenance Policy	Upgrade Actions
Host or management firmware package is included in one or more service profiles, and the service profiles are associated with one or more servers. OR Host or management firmware package is included in an updating service profile template, and the service profiles created from that template are associated with one or more servers.	Configured for changes to take effect during a specific maintenance window.	The following occurs when you update the firmware package: **1** Cisco UCS Manager asks you to confirm your change and advises that a user-acknowledged reboot of the servers is required. **2** Click the flashing **Pending Activities** button to select the servers you want to reboot and apply the new firmware. **3** Cisco UCS Manager verifies the model numbers and vendor against all servers associated with service profiles that include this policy. If the model numbers and vendor match a firmware version in the policy, Cisco UCS Manager reboots the server and updates the firmware. A manual reboot of the servers does not cause Cisco UCS Manager to apply the firmware package, nor does it cancel the scheduled maintenance activities.

Updating a Management Firmware Package

If the policy is included in one or more service profiles associated with a server and those service profiles do not include maintenance policies, Cisco UCS Manager updates and activates the management firmware in the server with the new versions and reboots the server as soon as you save the management firmware package policy

Before You Begin

Ensure that the appropriate firmware has been downloaded to the fabric interconnect.

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Servers** > **Policies**.

Step 3 Expand the node for the organization that includes the policy you want to update.
If the system does not include multitenancy, expand the **root** node.

Step 4 Expand **Management Firmware Packages** and choose the policy you want to update.

Step 5 In the **Work** pane, click the **General** tab.

Step 6 In the table on the right, do the following to delete the existing entry for the firmware you want to update:

a) Select the line in the table for the firmware version that you want to change.

b) Right-click and select **Delete**.

c) Click **Yes** to confirm that you want to delete that entry.

Step 7 In the **CIMC Firmware Packages** section on the left:

a) Click the down arrows to expand the section.
By default, the entries in a section are sorted by vendor name. To sort the entries, click on a column heading.

b) Select the line in the table which lists the firmware version for the release that you want to add to the firmware package.
The firmware version must match the model numbers (PID) on the servers that are associated with the firmware package . If you select a firmware version with the wrong model number, Cisco UCS Manager cannot install the firmware update.

c) Drag the line to the table on the right.

d) Click **Yes** to confirm that you selected the correct version.

Step 8 If you need to include CIMC firmware for servers with different model numbers (PIDs) in this management firmware package, repeat Step 6.

Step 9 Click **Save Changes**.
Cisco UCS Manager verifies the model numbers and vendor against all servers associated with service profiles that include this policy. If the model numbers and vendor match a firmware version in the policy, Cisco UCS Manager updates the firmware according to the settings in the maintenance policies included in the service profiles.

Updating a Host Firmware Package

You must upgrade the BIOS and storage controller firmware through the host firmware package when you upgrade to Release 1.4(3). If you do not upgrade those packages, the servers may experience communication issues with Cisco UCS Manager and the CIMC.

Caution If the policy is included in one or more service profiles associated with a server and those service profiles do not include maintenance policies, Cisco UCS Manager updates and activates the firmware in the server and adapter with the new versions and reboots the server as soon as you save the host firmware package policy.

This procedure assumes that the host firmware package already exists and that you have upgraded Cisco UCS Manager to Release 1.4(2). For information on how to create a host firmware package or on how to update an existing one in a previous release , see the appropriate *Cisco UCS Manager GUI Configuration Guide* for the release that Cisco UCS Manager is running.

Before You Begin

Before you update a host firmware package, do the following:

- Upgrade Cisco UCS Manager and the fabric interconnects.
- Determine an appropriate maintenance window to reduce the impact of the disruption of data traffic when the server reboots.
- Ensure you know the firmware version and model number (PID) for the servers or servers.

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Servers** > **Policies**.

Step 3 Expand the node for the organization that includes the policy you want to update.
If the system does not include multitenancy, expand the **root** node.

Step 4 Expand **Host Firmware Packages** and choose the policy you want to update.

Step 5 On each subtab of the **General** tab, do the following for each type of firmware you want to include in the package:

a) In the **Select** column, ensure that the check box for the appropriate lines are checked.

b) In the **Vendor**, **Model**, and **PID** columns, verify that the information matches the servers you want to update with this package.
The model and model number (PID) must match the servers that are associated with this firmware package. If you select the wrong model or model number, Cisco UCS Manager cannot install the firmware update.

c) In the **Version** column, choose the firmware version from the Release 1.4(3) firmware image.

Step 6 Click **Save Changes**.
Cisco UCS Manager verifies the model numbers and vendor against all servers associated with service profiles that include this policy. If the model numbers and vendor match a firmware version in the policy, Cisco UCS Manager updates the firmware according to the settings in the maintenance policies included in the service profiles.

What to Do Next

Verify that the firmware on the endpoints included in the host firmware package has been updated to Release 1.4(3). If the firmware has not been updated, check the model numbers and vendors in the host firmware package against those on the endpoints that were not updated.

Enabling Call Home

This step is optional. You only need to enable Call Home if you disabled it before you began the firmware upgrades.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, expand **All** > **Communication Management** > **Call Home**.

Step 3 In the **Work** pane, click the **General** tab.

Step 4 In the **Admin** area, click **on** in the **State** field.

Note If this field is set to **On**, Cisco UCS Manager GUI displays the rest of the fields on this tab.

Step 5 Click **Save Changes**.