Upgrading the Firmware to Release 2.0

This chapter includes the following sections:

- Summary of Steps for Upgrading from Release 1.4, page 1
- Disabling Call Home, page 3
- Updating the Firmware on the Adapters, BMCs, and IOMs, page 3
- Activating the Firmware on the Adapters and BMCs, page 4
- Activating the Board Controller Firmware on a Server, page 5
- Activating the Cisco UCS Manager Software to Release 2.0, page 6
- Activating the Firmware on the IOMs, page 7
- Activating the Fabric Interconnect Firmware for a Cluster Configuration, page 8
- Activating the Firmware on a Standalone Fabric Interconnect, page 14
- Updating Host and Management Firmware Packages, page 14
- Enabling Call Home, page 19

Summary of Steps for Upgrading from Release 1.4

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, upgrade the components in the following order.

1. Complete all prerequisite steps, as described in Prerequisites for Upgrading and Downgrading Firmware.
2. Obtain the following firmware images from Cisco.com and download them to the fabric interconnect. For more information, see Downloading the Cisco UCS, Release 2.1 Firmware.
   - Cisco UCS Infrastructure Software Bundle—Required for all Cisco UCS domains.

- Cisco UCS B-Series Blade Server Software Bundle—Required for all Cisco UCS domains that include blade servers.
- Cisco UCS C-Series Rack-Mount UCS-Managed Server Software Bundle—Only required for Cisco UCS domains 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.

3. (Optional) Disable Call Home—If the Cisco UCS domain includes Call Home or Smart Call Home, disable Call Home to ensure you do not receive unnecessary alerts when Cisco UCS Manager restarts components.
4. Update adapters, CIMC, and IOMs—If you prefer, you can upgrade the CIMC and the adapters in a host firmware package as part of the last upgrade step. Certain adapters must be upgraded in a host firmware package.
5. Activate adapters—Choose **Ignore Compatibility Check** and **Set Startup Version Only** when performing this step.
6. Activate CIMC—Choose **Ignore Compatibility Check** when performing this step.
7. Activate Cisco UCS Manager—Choose **Ignore Compatibility Check** when performing this step.
8. Activate the I/O modules—Choose **Ignore Compatibility Check** and **Set Startup Version Only** when performing this step.
9. Activate the subordinate fabric interconnect—Choose **Ignore Compatibility Check** when performing this step.
10. To avoid control plane disruption, manually failover the primary fabric interconnect to the fabric interconnect that has already been upgraded.
11. Verify that the data path has been restored.
12. Activate the primary fabric interconnect—Choose **Ignore Compatibility Check** when performing this step.
13. 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.
14. 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. While some of these components can be upgraded directly at the endpoint, such as the BIOS on M3 servers, we recommend that you upgrade the following firmware in a host firmware package:
    - BIOS
    - Storage controller
    - Certain adapters

    For information on how to upgrade these endpoints directly, see the Cisco UCS B-Series Firmware Management Guides.
15. (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 domain, 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, BMCs, 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.

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** tab, 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 domain. 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 version for the current 2.0 release.

c) Click **OK**.
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 (Optional) To monitor the progress of the update to a specific endpoint, right-click the endpoint and choose **Show Navigator**.
Cisco UCS Manager displays the progress in the **Update Status** area on the **General** tab. If the navigator has an **FSM** tab, you can also monitor the progress there. An entry in the **Retry #** field may not indicate that the update has failed. The retry count also includes retries that occur when Cisco UCS Manager retrieves the update status.

What to Do Next

Activate the firmware.

Activating the Firmware on the Adapters and BMCs

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 **Interface Cards**.
b) From the **Set Version** drop-down list, choose the version for the current 2.0 release.
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.

If a server is not associated with a service profile, the activated firmware remains in the pending-next-boot state. Cisco UCS Manager does not reboot the endpoints or activate the firmware until the server is associated with a service profile. If necessary, you can manually reboot or reset an unassociated server to activate the firmware.

Step 3 If the BMC 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 BMC firmware:

a) From the **Filter** drop-down list, choose **BMC**.
b) From the **Set Version** drop-down list, choose the version for the current 2.0 release.
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 BMC does not disrupt data traffic. However, it will interrupt all KVM sessions, disconnect any vMedia attached to the server, and interrupt all monitoring and IPMI polling.

When the **Activate Status** column for all BMC 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 M2 High Performance blade server and the Cisco UCS B230 M2 blade server, have M2 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 as the last step of upgrading a Cisco UCS domain, along with the server BIOS.

Procedure

Step 1 On the **Installed Firmware** tab, click **Activate Firmware**.
Cisco UCS Manager GUI opens the **Activate Firmware** dialog box and verifies the firmware versions for all endpoints in the Cisco UCS domain. 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 version for the current 2.0 release.

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

Step 5 Click **OK**.

Activating the Cisco UCS Manager Software to Release 2.0

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

Procedure

Step 1 On the **Installed Firmware** tab, click **Activate Firmware**.
Cisco UCS Manager GUI opens the **Activate Firmware** dialog box and verifies the firmware versions for all endpoints in the Cisco UCS domain. 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, choose the version for the current 2.0 release.

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. If you are prompted to re-login immediately after being disconnected, the login will fail. You must wait until the activation of Cisco UCS Manager is completed, which takes a few minutes.

Cisco UCS Manager makes the selected version the startup version and schedules the activation to occur when the fabric interconnects are upgraded.

Activating the Firmware on the IOMs

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, choose the version for the current 2.0 release.
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**.
When the **Activate Status** column for all IOMs displays **pending-next-boot**, continue with Step 3.

Step 3 Click **OK**.

Activating the Fabric Interconnect Firmware for a Cluster Configuration

To minimize the disruption to data traffic, always upgrade the subordinate fabric interconnect and ensure it is up and running before you upgrade the primary fabric interconnect.

Activating the Firmware on a Subordinate Fabric Interconnect

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** tab, click **Activate Firmware**.
Cisco UCS Manager GUI opens the **Activate Firmware** dialog box and verifies the firmware versions for all endpoints in the Cisco UCS domain. 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 version for the current 2.0 release from the drop-down list in the **Startup Version** column.

b) In the **System** row, choose the version for the current 2.0 release 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 domain 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

Force a fabric interconnect switchover to make this into the primary fabric interconnect. Then log into the new subordinate fabric interconnect (formerly the primary fabric interconnect) and verify that the data path is ready and has returned to normal operation. If the data path is not ready and the servers have not failed back over to the subordinate fabric interconnect, data traffic may be disrupted when you activate the primary fabric interconnect.

If the high availability status of the subordinate fabric interconnect contains the required values and the data path has returned to normal operation, activate the former primary fabric interconnect.

Forcing a Fabric Interconnect Failover

This operation can only be performed in the Cisco UCS Manager CLI.

You must force the failover from the primary fabric interconnect.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **show cluster state**	Displays the state of fabric interconnects in the cluster and whether the cluser is HA ready.
Step 2	UCS-A# **connect local-mgmt**	Enters local management mode for the cluster.
Step 3	UCS-A (local-mgmt) # **cluster** {**force primary** | **lead** {**a** | **b**}}	Changes the subordinate fabric interconnect to primary using one of the following commands: **force** Forces local fabric interconnect to become the primary. **lead** Makes the specified subordinate fabric interconnect the primary.

The following example changes fabric interconnect b from subordinate to primary:

```
UCS-A# show cluster state
Cluster Id: 0xfc436fa8b88511e0-0xa370000573cb6c04

A: UP, PRIMARY
B: UP, SUBORDINATE

HA READY
UCS-A# connect local-mgmt
Cisco Nexus Operating System (NX-OS) Software
```

```
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2011, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php

UCS-A(local-mgmt)# cluster lead b
UCS-A(local-mgmt)#
```

Verifying that the Data Path is Ready

This chapter includes the following sections:

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 –l**	Returns the number of active Ethernet interfaces. Verify that this number matches the number of Ethernet interfaces that were up prior to the upgrade.

	Command or Action	Purpose
Step 3	UCS-A(nxos)# **show platform fwm info hw-stm | grep '1.' | wc –l**	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 domain, 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 -l**	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 domain, 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

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

Note If you have followed the entire procedure to activate the fabric interconnects in a cluster configuration, the former primary fabric interconnect is now the subordinate fabric interconnect.

Before You Begin

Activate the subordinate fabric interconnect, force a fabric interconnect switchover, and verify that the data path is up and running.

Procedure

Step 1 On the **Installed Firmware** tab, click **Activate Firmware**.
Cisco UCS Manager GUI opens the **Activate Firmware** dialog box and verifies the firmware versions for all endpoints in the Cisco UCS domain. 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 (former) primary fabric interconnect, do the following:

a) In the **Kernel** row, choose the version for the current 2.0 release from the drop-down list in the **Startup Version** column.

b) In the **System** row, choose the version for the current 2.0 release 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 domain 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

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** tab, click **Activate Firmware**.
Cisco UCS Manager GUI opens the **Activate Firmware** dialog box and verifies the firmware versions for all endpoints in the Cisco UCS domain. 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 version for the current 2.0 release from the drop-down list in the **Startup Version** column.

b) In the **System** row, choose the version for the current 2.0 release 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 domain.

Updating Host and Management Firmware Packages

Effect of Updates to Firmware Packages in Service Profiles

To update firmware through a firmware package in a service profile, you need to update the firmware in the package. What happens after you save the changes to a firmware package depends upon how the Cisco UCS domain is configured.

The following table describes the most common options for upgrading servers with a firmware package in a service profile.

Service Profile	Maintenance Policy	Upgrade Actions
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, 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, disassociating a service profile may result in data loss when the disk or the BIOS is scrubbed upon association with the new service profile.
The firmware package is included in one or more service profiles, and the service profiles are associated with one or more servers. OR The 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 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 reboots the servers and updates the firmware. All servers associated with service profiles that include the firmware package are rebooted at the same time.

Service Profile	Maintenance Policy	Upgrade Actions
The firmware package is included in one or more service profiles, and the service profiles are associated with one or more servers. OR The 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 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 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 reboots the server and updates the firmware. A manual reboot of the servers does not cause Cisco UCS 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.
The firmware package is included in one or more service profiles, and the service profiles are associated with one or more servers. OR The 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 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 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 reboots the server and updates the firmware. A manual reboot of the servers does not cause Cisco UCS 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 unless you have configured and scheduled a maintenance window.

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 firmware table, do the following:

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 to which you want to update the firmware.

Step 7 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 2.0. 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 unless you have configured and scheduled a maintenance window.

This procedure assumes that the host firmware package already exists and that you have upgraded Cisco UCS Manager to the current 2.0 release. 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.

The information in the **Present** column lets you know whether that firmware exists in the Cisco UCS domain.

c) In the **Version** column, choose the version for the current 2.0 release.

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.

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**.

What to Do Next

Ensure that Call Home is fully configured.