Upgrading Cisco UCS from Release 1.3 to Release 2.1

Firmware Upgrade to Cisco UCS, Release 2.1 2

Cautions, Guidelines, and Limitations for Firmware Upgrades 2

Downloading the Cisco UCS, Release 2.1 Firmware 9

Upgrading the Firmware to Cisco UCS, Release 2.1 13

Revised: October 17, 2016,

Firmware Upgrade to Cisco UCS, Release 2.1

The firmware upgrade to Cisco UCS, Release 2.1 needs to be planned with scheduled maintenance windows for standalone fabric interconnects and for servers.

With this firmware upgrade, you should expect the following data traffic interruptions:

- For fabric interconnects in a cluster configuration, minimal data traffic disruption if the correct sequence of steps is followed. Failover between the fabric interconnects prevents the longer disruption required for the fabric interconnects and I/O modules to reboot.
- For a standalone fabric interconnect, data traffic disruption of up to one minute for the servers to reboot and approximately ten minutes for the fabric interconnect and I/O module to reboot.
- For servers, if you decide to upgrade them, data disruption while the servers reboot.

Cisco maintains a set of best practices for managing and updating firmware in the Cisco UCS B-Series Firmware Management Guides and in the following technical note: Unified Computing System Firmware Management Best Practices.

Note For information on how to upgrade a Cisco UCS 6100 series fabric interconnect to a Cisco UCS 6200 series fabric interconnect, see Upgrading Cisco UCS B-Series Hardware.

Cautions, Guidelines, and Limitations for Firmware Upgrades

Before you upgrade the firmware for any endpoint in a Cisco UCS domain, consider the following cautions, guidelines, and limitations:

Note The Cisco UCS Manager GUI does not allow you to choose options that a release does not support. If a Cisco UCS domain includes hardware that is not supported in the release to which you are upgrading, Cisco UCS Manager GUI does not display the firmware as an option for that hardware or allow you to upgrade to it.

Configuration Changes and Settings that Can Impact Upgrades

Depending upon the configuration of your Cisco UCS domain, the following changes may require you to make configuration changes after you upgrade. To avoid faults and other issues, we recommend that you make any required changes before you upgrade.

Impact of Upgrade to Cisco UCS, Release 2.1(2) and Higher on Initiator IQNs Defined at the Service Profile Level

If there are two iSCSI vNICs and both use the same initiator IQN (which is supported in Cisco UCS Release 2.0(1)), upgrading creates a single service profile level initiator IQN and resets the initiator IQNs on the iSCSI vNICs to have no value.

If the same initiator IQNs are used in iSCSI vNICs across service profiles in Cisco UCS Release 2.0(1), the upgrade creates duplicate initiator IQNs at the service profile level. This configuration generates faults for each iSCSI vNIC that has a duplicate initiator IQN

defined at the service profile level. Changing the duplicate initiator IQNs at the service profile level clears these faults. You must clear these faults before you perform any service profile related operations, such as updating a host firmware package.

Default Maintenance Policy Should be Configured for User Acknowledgment

The default maintenance policy is configured to immediately reboot the server when disruptive changes are made to the service profile, such as server firmware upgrades through a host maintenance policy. We recommend that you change the reboot policy setting in the default maintenance policy to user acknowledgment to avoid unexpected disruption of server traffic.

When you configure the reboot policy in the default maintenance policy to User Ack, the list of disruptive changes are listed with the pending activities. You can then control when the servers are rebooted.

Overlapping FCoE VLAN IDs and Ethernet VLAN IDs Are No Longer Allowed with Cisco UCS Release 2.0 and Higher

Caution In Cisco UCS 1.4 and earlier releases, Ethernet VLANs and FCoE VLANs could have overlapping VLAN IDs. However, starting with Cisco UCS release 2.0, overlapping VLAN IDs are not allowed. If Cisco UCS Manager detects overlapping VLAN IDs during an upgrade, it raises a critical fault. If you do not reconfigure your VLAN IDs, Cisco UCS Manager raises a critical fault and drops Ethernet traffic on the overlapped VLANs. Therefore, we recommend that you ensure there are no overlapping Ethernet and FCoE VLAN IDs before you upgrade to Cisco UCS Release 2.2.

Be aware that when an uplink trunk is configured with VLAN ID 1 defined and set as the native VLAN, changing the Ethernet VLAN 1 ID to another value can cause network disruption and flapping on the fabric interconnects, resulting in an HA event that introduces a large amount of traffic and makes services temporarily unavailable.

If you did not explicitly configure the FCoE VLAN ID for a VSAN in Cisco UCS 1.4 and earlier releases, Cisco UCS Manager assigned VLAN 1 as the default FCoE VLAN for the default VSAN (with default VSAN ID 1). In those releases, VLAN 1 was also used as the default VLAN for Ethernet traffic. Therefore, if you accepted the default VLAN ID for the FCoE VLAN and one or more Ethernet VLANs, you must reconfigure the VLAN IDs for either the FCoE VLAN(s) on the VSAN(s) or the Ethernet VLAN(s).

For a new installation of Cisco UCS Release 2.2, the default VLAN IDs are as follows:

- The default Ethernet VLAN ID is 1.
- The default FCoE VLAN ID is 4048.

After an upgrade from Cisco UCS Release 1.4, where VLAN ID 4048 was used for FCoE storage port native VLAN, to release 2.0, the default VLAN IDs are as follows:

- The default Ethernet VLAN ID is 1.
- The current default FCoE VLAN ID is preserved. Cisco UCS Manager raises a critical fault on the conflicting Ethernet VLAN, if any. You must change one of the VLAN IDs to a VLAN ID that is not used or reserved.

Note If a Cisco UCS domain uses one of the default VLAN IDs, which results in overlapping VLANs, you can change one or more of the default VLAN IDs to any VLAN ID that is not used or reserved. From release 2.0 and higher, VLANs with IDs from 4030 to 4047 are reserved.

VSANs with IDs in the Reserved Range are not Operational

A VSAN with an ID in the reserved range is not operational after an upgrade. Make sure that none of the VSANs configured in Cisco UCS Manager are in these reserved ranges:

- If you plan to use FC switch mode in a Cisco UCS domain, do not configure VSANs with an ID in the range from 3040 to 4078.
- If you plan to use FC end-host mode in a Cisco UCS domain, do not configure VSANs with an ID in the range from 3840 to 4079.

If a VSAN has an ID in the reserved range, change that VSAN ID to any VSAN ID that is not used or reserved.

Organization Name Limitations for Upgrade from Release 1.3

If you created an organization with a space in its name in a release of Cisco UCS Manager prior to 1.3 and then later upgraded Cisco UCS Manager to a 1.3.x release, the space was automatically replaced with an underscore. However, if you subsequently upgrade Cisco UCS Manager to a 1.4.x or later release, the old organization name with a space reappears without the space to underscore conversion. All of the objects in the organization which has a space in its name, including service profiles, policies, and templates, are deleted.

To avoid this problem, do the following before upgrading from a 1.3.x release to a 1.4.x or a later release:

1. Change the description field of the organizations that have underscores in their names, by removing the underscores and any spaces to help keep the organizations in the database.
2. Create a backup using the All Configuration option before upgrading. If a problem occurs after the upgrade, restore the configuration using the backup file. After importing the configuration file, reacknowledge all blades to restore their VIF status.

All Connectivity May Be Lost During Upgrades if vNIC Failover and NIC Teaming Are Both Enabled

All connectivity may be lost during firmware upgrades if you have configured both **Enable Failover** on one or more vNICs and you have also configured NIC teaming/bonding at the host operating system level. Please design for availability by using one or the other method, but never both.

To determine whether you have enabled failover for one or more vNICs in a Cisco UCS domain, verify the configuration of the vNICs within each service profile associated with a server. For more information, see the Cisco UCS Manager configuration guide for the release that you are running.

Hardware-Related Guidelines and Limitations for Firmware Upgrades

The hardware in a Cisco UCS domain can impact how you upgrade. Before you upgrade any endpoint, consider the following guidelines and limitations:

No Server or Chassis Maintenance

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

Avoid Replacing RAID-Configured Hard Disks During or Prior to Upgrade

During or prior to Cisco UCS infrastructure and server firmware upgrades:

- Do not remove, insert or replace any local storage hard disks or SSDs in the servers.
- Ensure that no storage operations are running, including Rebuild, Association, Copyback, BGI, and so on.

Always Upgrade Cisco UCS Gen-2 Adapters through a Host Firmware Package

You cannot upgrade Cisco UCS Gen-2 adapters directly at the endpoints. You must upgrade the firmware on those adapters through a host firmware package.

Cannot Upgrade Cisco UCS 82598KR-CI 10-Gigabit Ethernet Adapter

The firmware on the Cisco UCS 82598KR-CI 10-Gigabit Ethernet Adapter (N20-AI0002), Intel-based adapter card, is burned into the hardware at manufacture. You cannot upgrade the firmware on this adapter.

Number of Fabric Interconnects

For a cluster configuration with two fabric interconnects, you can take advantage of the failover between the fabric interconnects and perform a direct firmware upgrade of the endpoints without disrupting data traffic. However, you cannot avoid disrupting data traffic for those endpoints which must be upgraded through a host or management firmware package.

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.

Note If the internal power sequencer firmware for NX-OS is updated as part of the Cisco UCS upgrade process, then the fabric interconnect will boot to the loader prompt. Power-cycle the fabric interconnect in order to continue.

Unsupported Hardware Leads to Discovery Failure

When you add new servers or adapters to an existing Cisco UCS system with a Cisco UCS Manager release that does not support these servers and adapters, discovery of the system fails. The FSM displays an error message that the server or adapter is not supported on the current UCS firmware version. To resolve this issue, do one of the following:

- Update the Capability Catalog to the latest compatible release
- Upgrade the Cisco UCS Manager infrastructure firmware to the version required by the new hardware. The hardware support matrix in the Release Notes provides compatibility details.

Appliance Ports

If you are using appliance ports for direct attached storage, you must add VLANs to the ethernet uplinks. This will ensure that vNICS can properly pin on boot.

Firmware- and Software-Related Guidelines and Limitations for Upgrades

Before you upgrade any endpoint, consider the following guidelines and limitations:

Determine the Appropriate Type of Firmware Upgrade for Each Endpoint

Some endpoints, such as adapters and the server CIMC, can be upgraded through either a direct firmware upgrade or a firmware package included in a service profile. The configuration of a Cisco UCS domain determines how you upgrade these endpoints. If the service profiles associated with the servers include a host firmware package, upgrade the adapters for those servers through the firmware package. In the same way, if the service profiles associated with the servers include a management firmware package, upgrade the CIMC for those servers through the firmware package.

Upgrades of a CIMC through a management firmware package or an adapter through a firmware package in the service profile associated with the server take precedence over direct firmware upgrades. You cannot directly upgrade an endpoint if the service profile associated with the server includes a firmware package. To perform a direct upgrade, you must remove the firmware package from the service profile.

Do Not Activate All Endpoints Simultaneously in Cisco UCS Manager GUI

If you use Cisco UCS Manager GUI to update the firmware, 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 and 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.

Determine Available Bootflash and Workspace Partition

The bootflash partition is dedicated solely to firmware images managed by Cisco UCS Manager. To initiate upgrade or downgrade, at least 20 percent of the bootflash partition must be available. Faults are raised when the bootflash partition exceeds 70 percent and 90 percent capacity.

The workspace partition on the fabric interconnect stores tech support files, core files, and the debug plugin. To initiate upgrade or downgrade, at least 20 percent of the workspace partition must be available.

Impact of Activation for Adapters and I/O Modules

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.

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.

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.

Disable Call Home before Upgrading to Avoid Unnecessary Alerts (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.

Cautions, Guidelines, and Limitations for Upgrading with Auto Install

Before you use Auto Install to upgrade the firmware for any endpoint in a Cisco UCS domain, consider the following cautions, guidelines, and limitations:

Note These guidelines are specific to Auto Install and are in addition to those listed in Cautions, Guidelines, and Limitations for Firmware Upgrades, on page 2.

State of the Endpoints

Before you begin an upgrade, all affected endpoints must be in the following state:

- 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.
- For all endpoints to be upgraded, verify that they are in an Operable state.
- For all servers to be upgraded, verify that all the servers have been discovered and that discovery did not fail. Install Server Firmware will fail if any server endpoints cannot be upgraded.

Recommendations for the Default Host Firmware Policy

After you upgrade Cisco UCS Manager, a new host firmware policy named "default" is created, and assigned to all service profiles that did not already include a host firmware policy. The default host firmware policy is blank. It does not contain any firmware entries for any components. This default policy is also configured for an immediate reboot rather than waiting for user acknowledgment before rebooting the servers.

During the upgrade of server firmware, you can add firmware for the blade and rack mount servers in the Cisco UCS domain to the default host firmware policy. To complete the upgrade, all servers must be rebooted.

Every service profile that is assigned the default host firmware policy reboots the associated server according to the maintenance policy included in the service profile. If the maintenance policy is set to immediate reboot, you cannot cancel the upgrade or prevent the servers from rebooting after you complete the configuration in the **Install Server Firmware** wizard. We recommend that you verify the maintenance policy associated with these service profiles to ensure that they are set for a timed reboot or for user acknowledgment.

Note If you are upgrading from a release prior to 2.1(2a), you may be impacted by CSCup57496. After manually upgrading the CIMC and associating a service profile, remove the Management Firmware pack to activate the firmware of CIMC. For more information, please refer to https://tools.cisco.com/bugsearch/bug/CSCup57496.

Available Bootflash Partition

The bootflash partition is dedicated solely to firmware images managed by Cisco UCS Manager. To initiate Auto Install, at least 20 percent of the bootflash partition must be available. Faults are raised when the bootflash partition exceeds 70 percent and 90 percent capacity.

Available Workspace Partition

The workspace partition on the fabric interconnect stores tech support files, core files, and the debug plugin. To initiate upgrade or downgrade, at least 20 percent of the workspace partition must be available.

Time, Date, and Time Zone on Fabric Interconnects Must Be Identical

To ensure that the fabric interconnects in a cluster configuration are in sync, you must ensure that they are configured for the same date, time, and time zone. We recommend that you configure an NTP server and the correct time zone in both fabric interconnects. If the date, time or time zone in the fabric interconnects are out of sync, the Auto Install might fail.

Cannot Upgrade Infrastructure and Server Firmware Simultaneously

You cannot upgrade the infrastructure firmware at the same time as you upgrade server firmware. We recommend that you upgrade the infrastructure firmware first and then upgrade the server firmware. Do not begin the server firmware upgrade until the infrastructure firmware upgrade is completed.

Required Privileges

Users must have the following privileges to upgrade endpoints with Auto Install:

Privileges	Upgrade Tasks User Can Perform
admin	• Run Install Infrastructure Firmware • Run Install Server Firmware • Add, delete, and modify host firmware packages
Service profile compute (ls-compute)	Run Install Server Firmware
Service profile server policy (ls-server-policy)	Add, delete, and modify host firmware packages
Service profile config policy (ls-config-policy)	Add, delete, and modify host firmware packages

Impact of Host Firmware Packages and Management Firmware Packages on Install Server Firmware

Because Install Server Firmware uses host firmware packages to upgrade the servers, you do not have to upgrade all servers in a Cisco UCS domain to the same firmware versions. However, all servers which have associated service profiles that include the host firmware packages you selected when you configured Install Server Firmware are upgraded to the firmware versions in the specified software bundles.

If the service profiles associated with servers include a management firmware package as well as a host firmware package, Install Server Firmware uses the firmware version in the management firmware package to upgrade the CIMC on the servers. The CIMC is not upgraded to the firmware version in the host firmware package, even if it is a more recent version of the CIMC than the one in the management firmware package. If you want to use the host firmware packages to upgrade the CIMC in the servers, you must remove the management firmware packages from the associated service profiles.

Effect of Using Install Server Firmware on Servers Whose Service Profiles Do Not Include a Host Firmware Package

If you use Install Server Firmware to upgrade server endpoints on servers that have associated service profiles without host firmware packages, Install Server Firmware uses the default host firmware package to upgrade the servers. You can only update the default host firmware package through Install Server Firmware.

If you want to upgrade the CIMC or adapters in a server with an associated service profile that has previously been updated through the default host firmware package in Install Server Firmware, you must use one of the following methods:

- Use Install Server Firmware to modify the default host firmware package and then upgrade the server through Install Server Firmware.
- Create a new host firmware package policy, assign it to the service profile associated with the server, and then upgrade the server through that host firmware package policy.
- Disassociate the service profile from the server and then directly upgrade the server endpoints.

Upgrading Server Firmware on Newly Added Servers

If you add a server to a Cisco UCS domain after you run Install Server Firmware, the firmware on the new server is not automatically upgraded by Install Server Firmware. If you want to upgrade the firmware on a newly added server to the firmware version used when you last ran Install Server Firmware, you must manually upgrade the endpoints to upgrade the firmware on that server. Install Server Firmware requires a change in firmware version each time. You cannot rerun Install Server Firmware to upgrade servers to the same firmware version.

Downloading the Cisco UCS, Release 2.1 Firmware

This section contains information about how to obtain the Cisco UCS, Release 2.1 firmware and download it to a fabric interconnect.

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.

Obtaining Software Bundles from Cisco

Before You Begin

Determine which of the following software bundles you need to update the Cisco UCS domain:

- 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.

Procedure

Step 1 In a web browser, navigate to Cisco.com.

Step 2 Under **Support**, click **All Downloads**.

Step 3 In the center pane, click **Servers - Unified Computing**.

Step 4 If prompted, enter your Cisco.com username and password to log in.

Step 5 In the right pane, click the link for the software bundles you require, as follows:

Bundle	Navigation Path
Cisco UCS Infrastructure Software Bundle	Click **Cisco UCS Infrastructure and UCS Manager Software** > **Unified Computing System (UCS) Infrastructure Software Bundle**.
Cisco UCS B-Series Blade Server Software Bundle	Click **Cisco UCS B-Series Blade Server Software** > **Unified Computing System (UCS) Server Software Bundle**.
Cisco UCS C-Series Rack-Mount UCS-Managed Server Software Bundle	Click **Cisco UCS C-Series Rack-Mount UCS-Managed Server Software** > **Unified Computing System (UCS) Server Software Bundle**.

Tip The Unified Computing System (UCS) Documentation Roadmap Bundle, which is accessible through these paths, is a downloadable ISO image of all Cisco UCS documentation.

Step 6 On the first page from which you download a software bundle, click the **Release Notes** link to download the latest version of the Release Notes.

Step 7 For each software bundle that you want to download, do the following:

a) Click the link for the latest software bundle for the release you want to download.
The release number is followed by a number and a letter in parentheses. The number identifies the maintenance release level, and the letter differentiates between patches of that maintenance release. For more information about what is in each maintenance release and patch, see the latest version of the Release Notes.

b) Click one of the following buttons and follow the instructions provided:

- **Download Now—**Allows you to download the software bundle immediately.
- **Add to Cart—**Adds the software bundle to your cart to be downloaded at a later time.

c) Follow the prompts to complete your download of the software bundle(s).

Step 8 Read the Release Notes before upgrading your Cisco UCS domain.

What to Do Next

Download the software bundles to the fabric interconnect.

Downloading Firmware Packages to the Fabric Interconnect

You can use the same procedure to download a single firmware image to the fabric interconnect.

Note In a cluster setup, the image file for the firmware bundle is downloaded to both fabric interconnects, regardless of which fabric interconnect is used to initiate the download. Cisco UCS Manager maintains all firmware packages and images in both fabric interconnects in sync. If one fabric interconnect is down, the download finishes successfully. The images are synced to the other fabric interconnect when it comes back online.

Before You Begin

Obtain the required firmware bundles from Cisco.

Procedure

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

Step 2 Click the **Equipment** node.

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

Step 4 Click the **Installed Firmware** tab.

Step 5 Click **Download Firmware**.

Step 6 In the **Download Firmware** dialog box, complete the following fields:

Name	Description
Protocol field	The protocol to use when communicating with the remote server. This can be one of the following: • **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. **Note** The TFTP file size limitation is 32 MB. Because firmware bundles can be much larger, Cisco recommends that you do not choose TFTP for firmware downloads. If your system supports Cisco USB drives, it may take up to one minute for the Cisco USB drive to be detected by Cisco UCS Manager during insertion and removal. No other type of USB drive is supported.
Server field	If the file came from a remote server, this is the IP address or hostname of the remote server on which the files resides. If the file came from a local source, this field displays "local". **Note** If you use a hostname rather than an IPv4 or IPv6 address, you must configure a DNS server. If the Cisco UCS domain is not registered with Cisco UCS Central or DNS management is set to **local**, configure a DNS server in Cisco UCS Manager. If the Cisco UCS domain is registered with Cisco UCS Central and DNS management is set to **global**, configure a DNS server in Cisco UCS Central.
Filename field	The name of the firmware file.
Path field	The absolute path to the file on the remote server. If you use SCP, the absolute path is always required. If you use any other protocol, you may not need to specify a remote path if the file resides in the default download folder. For details about how your file server is configured, contact your system administrator.
User field	The username the system should use to log in to the remote server. This field does not apply if the protocol is TFTP or USB.
Password field	The password for the remote server username. This field does not apply if the protocol is TFTP or USB.

Cisco UCS Manager GUI begins downloading the firmware bundle to the fabric interconnect.

Step 7 Click **OK**.

Step 8 (Optional) Monitor the status of the image download on the **Download Tasks** tab.

Note If Cisco UCS Manager reports that the bootflash is out of space, delete obsolete images to free up space. To view the available space in bootflash, navigate to the fabric interconnect on the **Equipment** tab and expand the **Local Storage Information** area on the **General** tab.

What to Do Next

After the image file for the firmware bundles download completes, update the firmware on the endpoints.

Upgrading the Firmware to Cisco UCS, Release 2.1

This section contains information about the steps you need to follow to upgrade a Cisco UCS domain to Cisco UCS, Release 2.1.

Options for Firmware Upgrades to Cisco UCS, Release 2.1

With Cisco UCS, Release 2.1, you have the following options for upgrading the firmware in a Cisco UCS domain:

- Upgrade with Auto Install—This upgrade path requires that the pre-upgrade level of firmware in the Cisco UCS domain be at the latest firmware version for that release. To use this upgrade option, you must first upgrade Cisco UCS Manager to the latest version of Cisco UCS, Release 2.1 and then use Auto Install to upgrade the remaining infrastructure components. This option uses host firmware packages to upgrade all server endpoints.
- Upgrade manually—This upgrade path does not require that the pre-upgrade level of firmware be at a specific level for that release. You can choose to upgrade some server endpoints, such as adapters, manually.

Summary of Steps for Upgrading from Release 1.3 with Partial Use of Auto Install

Note The following set of steps assumes that you have included host firmware packages in the service profiles of all servers. See the Cisco UCS B-Series Firmware Management Guides for details of the appropriate procedures.

The order of steps is designed to minimize the disruption to data traffic. If you do not follow this order, the firmware upgrade may fail and the servers may experience communication issues with Cisco UCS Manager.

Important If you are upgrading from a release prior to 2.1(3a), you may be impacted by CSCuh61202. This defect affects FC traffic on the Cisco 1240, Cisco 1280, and Cisco M81KR adapters. To avoid this situation and reduce the number of server reboots, you must first upgrade the adapter and server firmware using a host firmware package, and then proceed with the corresponding infrastructure upgrade. This is an exception to the normal upgrade procedure. For more details, refer to https://tools.cisco.com/bugsearch/bug/CSCuh61202.

1 Complete all prerequisite steps, as described in Prerequisites for Upgrading and Downgrading Firmware, on page 9.

2 Obtain the following firmware image from Cisco.com and download it to the fabric interconnect: Cisco UCS Infrastructure Software Bundle.You must download this firmware image a second time, in Step 5, to complete the infrastructure upgrade. This additional download is required because Cisco UCS, Release 1.3 does not support separate server and infrastructure bundles.

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. For more information, see Disabling Call Home.

4 Activate Cisco UCS Manager—Choose **Skip Validation** when performing this step. For more information, see Activating the Cisco UCS Manager Software.

5 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, on page 9.

- 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.

6 Upgrade the infrastructure firmware—In Cisco UCS Manager, choose **Equipment** > **Firmware Management** > **Firmware Auto Install**, click **Install Infrastructure Firmware** and complete the fields to upgrade the infrastructure. For more information, see Upgrading the Infrastructure Firmware with Auto Install.

7 Verify that the data path has been restored. For more information, see Verifying that the Data Path is Ready.

Caution To upgrade with minimal disruption, you must confirm the following:

- Ensure that both of the fabric interconnects and the service profiles are configured for failover.
- Verify that the data path has been successfully restored from the secondary fabric interconnect before you acknowledge the reboot of the primary fabric interconnect.

8 Acknowledge the reboot of the primary fabric interconnect on the **User Acknowledged Activities** tab of the **Pending Activities** dialog box. Click the **Pending Activities** icon to open the dialog box. For more information, see Acknowledging the Reboot of the Primary Fabric Interconnect.

9 Upgrade the server firmware—Complete the following steps in the **Install Servers Firmware** wizard. For more information, see Upgrading the Server Firmware with Auto Install.

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

b Choose the firmware bundles that you have just downloaded to the fabric interconnects.

c Click on the root for the host firmware packages to upgrade all servers, including those that do not have an associated service profile.

d On the **Impacted Endpoints Summary** page, review the list of servers that will be reset by this upgrade.

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

10 (Optional) Enable Call Home—If you disabled Call Home before the upgrading the firmware, enable Call Home. For more information, see Enabling Call Home.

Summary of Steps for Manually Upgrading from Release 1.3

Note The following set of steps assumes that you have included host firmware packages in the service profiles of all servers. See the Cisco UCS B-Series Firmware Management Guides for details of the appropriate procedures.

The order of steps is designed to minimize the disruption to data traffic. If you do not follow this order, the firmware upgrade may fail and the servers may experience communication issues with Cisco UCS Manager.

Important If you are upgrading from a release prior to 2.1(3a), you may be impacted by CSCuh61202. This defect affects FC traffic on the Cisco 1240, Cisco 1280, and Cisco M81KR adapters. To avoid this situation and reduce the number of server reboots, you must first upgrade the adapter and server firmware using a host firmware package, and then proceed with the corresponding infrastructure upgrade. This is an exception to the normal upgrade procedure. For more details, refer to https://tools.cisco.com/bugsearch/bug/CSCuh61202.

1. Complete all prerequisite steps, as described in Prerequisites for Upgrading and Downgrading Firmware, on page 9.
2. Obtain the following firmware image from Cisco.com and download it to the fabric interconnect: Cisco UCS Infrastructure Software Bundle.You must download this firmware image a second time, in Step 5, to complete the infrastructure upgrade. This additional download is required because Cisco UCS, Release 1.3 does not support separate server and infrastructure bundles.
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. For more information, see Disabling Call Home.
4. Update the I/O modules. For more information, see Updating the Firmware on an IOM or Updating the Firmware on Multiple Endpoints.
5. Activate the I/O modules—Choose **Ignore Compatibility Check** and **Set Startup Version Only** when performing this step. For more information, see Activating the Firmware on an IOM.
6. Activate Cisco UCS Manager—Choose **Skip Validation** when performing this step. For more information, see Activating the Cisco UCS Manager Software.
7. 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, on page 9.
   - 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.
8. Activate the subordinate fabric interconnect. For more information, see Activating the Firmware on a Subordinate Fabric Interconnect.
9. To avoid control plane disruption, manually failover the primary fabric interconnect to the fabric interconnect that has already been upgraded. For more information, see Forcing a Fabric Interconnect Failover.

10 Verify that the data path has been restored. For more information, see Verifying that the Data Path is Ready.

Caution To upgrade with minimal disruption, you must confirm the following:

- Ensure that both of the fabric interconnects and the service profiles are configured for failover.
- Verify that the data path has been successfully restored from the secondary fabric interconnect before you reboot the primary fabric interconnect.

11 Activate the primary fabric interconnect. For more information, see Activating the Firmware on the Primary Fabric Interconnect.

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. For more information, see Updating a Host Firmware Package. You can upgrade the following firmware in a host firmware package:

- BIOS
- Storage controller
- Adapters
- Cisco Integrated Management Controller (CIMC)

  Cisco UCS no longer supports the creation of new management firmware packages. We recommend that you remove the management firmware packages from all service profiles and use host firmware packages to update the CIMC on the servers.

Note The board controller firmware upgrade requires an AC power-cycle, which you will be prompted to complete when you perform the upgrade.

13 (Optional) Enable Call Home—If you disabled Call Home before the upgrading the firmware, enable Call Home. For more information, see Enabling Call Home.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands