Firmware Management

This chapter includes the following sections:

Firmware Download from Cisco

You can configure firmware downloads in Cisco UCS Central to communicate with Cisco website at specified intervals and fetch the firmware image list. After configuring Cisco credentials for image download, when you refresh, Cisco UCS Central fetches the available image data from Cisco.com and displays the firmware image in the firmware image library. You can download the actual firmware images when creating a policy using the firmware image version or when downloading the image using the **Store Locally** option.

Important Make sure you do the following to download firmware from Cisco into Cisco UCS Central.

- You must enable Cisco UCS Central to access Cisco.com either directly or using a proxy server.
- You must configure valid Cisco user credentials and enable download state in Cisco UCS Central.

Firmware Library of Images

Image Library in Cisco UCS Central displays a list of all firmware images downloaded into Cisco UCS Central from Cisco.com, local file system and remote file system.

The source for images downloaded from Cisco.com is Cisco and for images downloaded from local or remote file system is local. These firmware images are available for creating firmware policies.

The following are the options to delete firmware images from the library:

- **Deleting the firmware image** — You can delete any downloaded image in the firmware library using the delete option.
- **Purging the firmware image metadata** — You can delete the image metadata using the purge option. Even after you delete the firmware image from the library, the metadata will still exist. You can use the metadata information to download the actual firmware image anytime from Cisco.com even after deleting the image. If you want to completely remove the firmware image and associated metadata from the firmware image library, make sure to delete the actual firmware image and purge the metadata from the library.

Important If you have already downloaded the image corresponding to the metadata into the firmware image library, you cannot purge the metadata without deleting the image.

Configuring Firmware Download from Cisco

When you configure firmware download from Cisco, Cisco UCS Central downloads the firmware metadata from Cisco.com and keeps the information available for you to download and save anytime from Cisco UCS Central.

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Images**.

Step 3 Click **Configure Downloads From Cisco**.

Step 4 In the **Work** pane, **General** tab, fill in the fields with the required information.
Make sure to have the username and password for the Cisco.com account that Cisco UCS Central uses to log in.

Step 5 In the **Proxy** tab, fill in the required information for the proxy account.

Step 6 Click **Save**.

Downloading a Firmware Image from Cisco

When you configure firmware image download from Cisco.com and refresh the library of images, Cisco UCS Central is able to access to all available firmware image metadata. You can download the firmware image in the following ways:

- **Creating a firmware policy** — When you create a firmware policy and select the specific image, Cisco UCS Central automatically downloads the image specified in the firmware policy.
- **Storing the image locally** — When you select the store locally option, the selected firmware image is downloaded from Cisco.com and stored in the image library.

This procedure describes the process to download the image using store locally option.

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Images**.

Step 3 Click **Library**.

Step 4 In the **Work** pane, click **Packages** tab.
The image metadata downloaded from Cisco will have the **Source** as **Cisco** and **State** as **not-downloaded**.

Step 5 Right click on the bundle and from the options, choose **Store Locally**.

Downloading Firmware from a Remote Location

Before You Begin

You must have the remote server configured to support the file transfer protocol that you choose and they must be accessible to Cisco UCS Central.

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Images**.

Step 3 Click **Library**.

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

Step 5 In the **Downloads** tab, click **Download Firmware**.

Step 6 In the **Download Firmware** dialog box, **Location of the Image File**, choose **Remote File System** and fill in the required fields.

Step 7 Click **OK**.

Downloading Firmware from a Local File System

Before You Begin

You must have obtained and saved the firmware image from Cisco in your local file system to configure downloading the firmware from local system into Cisco UCS Central.

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Images**.

Step 3 Click **Library**.

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

Step 5 In the **Downloads** tab, click **Download Firmware**.

Step 6 In the **Download Firmware** dialog box, **Location of the Image File**, choose **Local File System**.

Step 7 Click **Download Image into Image Library**.
A dialog box opens with an option to select the file.

Step 8 Click **Browse** to browse to the firmware file location in your local system and select the file.

Step 9 Click **Submit**.
If the image download is successful, **Firmware Image Download** dialog box opens with a confirmation message.

Step 10 In the **Firmware Image Download** dialog box, click **OK**.

Viewing Image Download Faults

You can view the faults in firmware image download process from the same **Library of Images** panel.

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Images**.

Step 3 Click **Library**.

Step 4 In the **Work** pane, click **Faults** tab.
The faults table displays all download faults with details.

Viewing Firmware Images in the Library

You can view the downloaded firmware images and image metadata in the **Library of Images** panel.

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Images**.

Step 3 Click **Library**.

Step 4 The **Work** pane click the **Packages** tab.
The available packages are displayed. You can select a package and click **Properties** to view details on specific packages.

Deleting Image Metadata from the Library of Images

You can delete the firmware image metadata from the **Library of Images** using the purge option. The purge option clears only the metadata of already downloaded images.

Note If you want to delete any of the firmware packages such as the capability catalog, infrastructure and host firmware packages, you can do so from the firmware management section under each domain groups or from the domain group root.

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Images**.

Step 3 Click **Library**.

Step 4 In the **Work** pane, choose the firmware image metadata you want to delete from **Library of Images** and click **Purge**.

Step 5 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

Firmware Upgrades for Cisco UCS Domains

You can deploy infrastructure and server firmware upgrades for registered Cisco UCS domains from Cisco UCS Central.

If desired, you can upgrade the Cisco UCS domains in each domain group with different versions of firmware. Cisco UCS Central also provides you the option to acknowledge the fabric interconnect reboot globally from Cisco UCS Central or individually from each Cisco UCS domain.

Scheduling Infrastructure Firmware Updates for Cisco UCS Domains

You can schedule an infrastructure firmware upgrade or downgrade for either a classic or mini Cisco UCS Domain from **Infrastructure Firmware** panel. For more information on managing firmware in Cisco UCS domains, see Cisco UCS Manager Firmware Management Guides.

Note You must create a separate infrastructure firmware policy for modular domains in Cisco UCS Central. The infrastructure firmware policies must be unique to modular servers. This will prevent any firmware policy resolution issues with other domain groups.

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Groups Root** > **Firmware Management**.

Step 3 Click **Infrastructure Firmware**.

Step 4 In the **Firmware Version** section, click the drop down for **UCS** or **UCS Mini**, and select the firmware version for these domains.
You can select either one, or both at the same time. The **Scheduler** options are enabled after you select the firmware version. If you remove the firmware version in both **UCS** and **UCS Mini**, the **Scheduler** is reset to disabled.

Step 5 In the **Scheduler** section, specify the schedule.
If you check mark **User Acknowledged**, the upgrade is listed on the pending activities panel. Actual upgrade is triggered only after you manually acknowledge this activity.

Step 6 Click **Save** to save the infrastructure firmware upgrade schedule.

Acknowledging a Pending Activity

if the service profiles in Cisco UCS domains use a global maintenance policy and global host firmware package, Cisco UCS Central provides you an option to enable user acknowledgment before deploying the firmware upgrade.

If you have created a maintenance policy with **User Ack** reboot policy, you must acknowledge the actual firmware upgrade in Cisco UCS Manager. If you have created a maintenance policy with a global schedule and enabled **User Ack**, you must acknowledge the actual upgrade for all Cisco UCS domains in Cisco UCS Central.

Note You can view and acknowledge pending activities from **Infrastructure Firmware** and **Host Firmware** sections. This procedure describes the process to acknowledge a pending activity from the host firmware section.

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Groups Root** > **Firmware Management**.

Step 3 In the **Work** pane, click **Pending Activities** tab.

Step 4 Choose the pending activity from the displayed list, right click and click **Acknowledge**.

Deleting an Infrastructure Firmware Package

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Groups Root** > **Firmware Management**.

Step 3 The **Work** pane displays a list of all created infrastructure firmware packages.

Step 4 Click **Delete**.

Step 5 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

Creating a Host Firmware Package

Procedure

Step 1 On the menu bar, click **Servers**.

Step 2 In the **Navigation** pane, expand **Servers** > **Policies** > **root**.

Step 3 Click **Host Firmware Packages**.

Step 4 In the **Work** pane, click **Create a Host FW Pack**.

Step 5 In **Create a Host FW Pack** dialog box, fill in the following fields:

a) Fill in **Name** and **Description**.
b) In the **Blade Version** area, choose the blade server version.
c) In the **Rack Version** area, choose the rack server version.
d) In the **Modular Version** area, choose the modular server version.

Step 6 The **Impacted Endpoints** dialog box displays the list of end points that will be affected by this host firmware policy.
During a firmware upgrade, these endpoints will be rebooted and will therefore be unavailable during part of the upgrade process

Step 7 Click **OK**.

What to Do Next

The host firmware policy you create in Cisco UCS Central will be available for association to a service profile in a Cisco UCS Domain registered to a domain group.

Deploying a Host Firmware Upgrade

You can update all host firmware policies defined in Cisco UCS Central to specific B, C, and M bundles using the **Install Servers**.

Before You Begin

You must have created a host firmware package.

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Groups Root** > **Firmware Management**.

Step 3 Click **Host Firmware**.

Step 4 In the **Work** pane, from the displayed list of host firmware packages, choose the firmware version you want to deploy.

Step 5 Click **Install Servers** on the table header.

Step 6 In the **Install Servers** dialog box, select **Blade Version**, **Rack Version**, **Modular Version** and **Impacted Endpoints**.

Step 7 In **Upgrade host Firmware Warning** message dialog box, click **Yes**.
If the servers in the selected endpoints use the global host firmware upgrade policy, they will be upgraded with the host firmware package.

Deleting a Host Firmware Package

Procedure

Step 1 On the menu bar, click **Servers**.

Step 2 In the **Navigation** pane, expand **Servers** > **Policies** > **root**.

Step 3 Click **Host Firmware Packages**.

Step 4 The **Work** pane displays a list of all created host firmware packages.

Step 5 Click and choose the host firmware package name you want to delete.
The table header area shows action icons.

Step 6 Click **Delete**.

Step 7 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

Firmware Upgrade Schedules

To upgrade firmware by domain groups in registered Cisco UCS domains, you can schedule upgrades from Cisco UCS Central in the following ways:

- As a one time occurrence
- As a recurring occurrence that recurs at designated intervals

If you configure the schedules for user acknowledgment, the fabric interconnect will not reboot without explicit acknowledgment.

Creating a Maintenance Policy

You can create the following types of maintenance policies for host firmware update in Cisco UCS Central:

- **Immediate —** The immediate option reboots the servers immediately without any user acknowledgment.
- **Timer-automatic —** In timer-automatic option, the server reboot will happen based on the schedule you select for this maintenance policy.

  Important If you use the timer automatic option, you must create a schedule in Cisco UCS Central to specify in the maintenance policy. When you create a schedule in Cisco UCS Central, you can acknowledge this scheduled maintenance policy only in Cisco UCS Central.Servers using this maintenance policy will reboot only during the maintenance window defined in the schedule. If user-ack is enabled in the schedule, then you must acknowledge the server reboot.

- **User-acknowledgment —** The user-ack option sends a pending activity notification in each Cisco UCS Domain before rebooting servers.

  Important The user-ack option provides Cisco UCS domains administrators the option to decide on rebooting servers in individual Cisco UCS domains at different times.

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** Pane, expand **Domain Groups** > **Domain Group Root** > **Maintenance**.

Step 3 In the **Work** pane, click **Create Maintenance Policy**.

Step 4 In the **Create Maintenance Policy** dialog box, do fill in the required fields.

Step 5 Click **OK**.

What to Do Next

Associate the maintenance policy to a service profile in Cisco UCS Manager.

Creating a One Time Occurrence Schedule

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Groups Root** > **Schedules**.

Step 3 In the **Work** pane, click **Create Schedule**.

Step 4 In the **Create Schedule** dialog box, enter the details in the **Properties** area.

Step 5 Choose **One Time Occurrences** tab and click **Create One Time Occurrence**.

Step 6 In the **Create One Time Occurrence** dialog box, fill in the details.

Step 7 Click **OK**.

Step 8 Click OK in the **Create Schedule** dialog box.
The one time schedule you created is added to the **Schedules** table.

Creating a Recurring Occurrence Schedule

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Groups Root** > **Schedules**.

Step 3 In the **Work** pane, click **Create Schedule**.

Step 4 In the **Create Schedule** dialog box, enter the details in the **Properties** area.

Step 5 Choose **Recurring Occurrences** tab and click **Create Recurring Occurrence**.

Step 6 In the **Create Recurring Occurrence** dialog box, fill in the details.

Step 7 Click **OK**.

Step 8 Click OK in the **Create Schedule** dialog box.
The recurring schedule you created is added to the table.

Deleting a Firmware Upgrade Schedule

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Groups Root** > **Schedules**.

Step 3 The **Work** pane displays a list of all scheduled firmware events.

Step 4 Click and choose the schedule name you want to delete.
The table header area shows action icons.

Step 5 Click **Delete**.

Step 6 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

Capability Catalog

The Capability Catalog is a set of tunable parameters, strings, and rules. Cisco UCS uses the catalog to update the display and configurability of components such as newly qualified DIMMs and disk drives for servers.

The catalog is divided by hardware components, such as the chassis, CPU, local disk, and I/O module. You can use the catalog to view the list of providers available for that component. There is one provider per hardware component. Each provider is identified by the vendor, model (PID), and revision. For each provider, you can also view details of the equipment manufacturer and the form factor.

For information about which hardware components are dependent upon a particular catalog release, see the component support tables in the Service Notes for the B- Series servers. For information about which components are introduced in a specific release, see the Cisco UCS Release Notes.

Contents of the Capability Catalog

The contents of the Capability Catalog include the following:

Implementation-Specific Tunable Parameters

- Power and thermal constraints
- Slot ranges and numbering
- Adapter capacities

Hardware-Specific Rules

- Firmware compatibility for components such as the BIOS, CIMC, RAID controller, and adapters
- Diagnostics
- Hardware-specific reboot

User Display Strings

- Part numbers, such as the CPN, PID/VID
- Component descriptions
- Physical layout/dimensions
- OEM information

Updates to the Capability Catalog

Capability Catalog updates are included in each Cisco UCS Infrastructure Software Bundle. Unless otherwise instructed by Cisco TAC, you only need to activate the Capability Catalog update after you've downloaded, updated, and activated a Cisco UCS Infrastructure Software Bundle.

As soon as you activate a Capability Catalog update, Cisco UCS immediately updates to the new baseline catalog. You do not have to perform any further tasks. Updates to the Capability Catalog do not require you to reboot or reinstall any component in a Cisco UCS domain.

Each Cisco UCS Infrastructure Software Bundle contains a baseline catalog. In rare circumstances, Cisco releases an update to the Capability Catalog between Cisco UCS releases and makes it available on the same site where you download firmware images.

Note The Capability Catalog version is determined by the version of Cisco UCS that you are using. For example, Cisco UCS 2.0 releases work with any 2.0 release of the Capability Catalog, but not with 1.0 releases of the Capability Catalog. For information about Capability Catalog releases supported by specific Cisco UCS releases, see the *Release Notes for Cisco UCS Software* accessible through the *Cisco UCS B-Series Servers Documentation Roadmap* available at the following URL: http://www.cisco.com/go/unifiedcomputing/b-series-doc.

Configuring a Capability Catalog Update for a Cisco UCS Domain

You can create only one capability catalog per each Cisco UCS Domain group in Cisco UCS Central. All the member Cisco UCS domains of a group will run the same firmware version.

Note You can configure capability catalog update from domain group root or at the domain group level. When you update the capability catalog at the domain group root level, if the domain groups under the root do not have a capability catalog defined, will get the same capability catalog version.

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Groups Root** > **Firmware Management**.

Step 3 Click **Capability Catalog**.

Step 4 In the **Work** pane, click **Create**.

Step 5 In the **Version** table, select the version of the capability catalog you want to associate with the Cisco UCS domains included in the selected Cisco UCS Central domain group.
The capability catalog version selected here overrides the version inherited from any parent groups, if an inherited version exists.

Step 6 Click **Save**.

Cisco UCS Central triggers the capability catalog update in the specified Cisco UCS domains.