Firmware Management

Firmware Management

In Cisco UCS Central, you can manage all firmware components for all registered Cisco UCS domains. The status of all firmware updates displays under the **Domains** section:

- **Firmware Ready—**The firmware has been successfully updated.
- **In Progress—**The firmware update is currently in progress.
- **Pending User Ack—**Requires user acknowledgment on the **Alerts** > **Pending Activities** page before it updates the firmware.

Note To manage Cisco UCS domains firmware from Cisco UCS Central, enable the global firmware management option in Cisco UCS Manager. You can enable the global firmware management option when you register Cisco UCS Manager with Cisco UCS Central. You can also turn global management option on or off based on your management requirements.

The Cisco UCS domains are categorized into domain groups in Cisco UCS Central for management purposes. You can manage firmware for each domain group separately, at the domain group level, or for all domain groups from the domain group root. Cisco UCS Central provides the option to manage the following Cisco UCS domain firmware packages:

- **Capability Catalog—**One capability catalog per domain group. All Cisco UCS domains registered to a particular domain group use the capability catalog defined in the domain group.
- **Infrastructure Firmware—**One infrastructure firmware policy per domain group. All Cisco UCS domains registered to a particular domain group use the same Infrastructure firmware version defined in the domain group.

Image Library

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

- The **Packages** tab displays all firmware packages.
- The **Downloads**tab allows you to monitor the status of your downloads.

These firmware images are available for creating firmware policies.

From here you can:

- Delete any downloaded image from the image library by selecting the image and clicking the Delete icon.

  Note If the firmware image you are trying to delete is referenced in a scheduled policy, the delete operation fails. You cannot delete this policy from the image library.

- Sync firmware images with images on Cisco.com by clicking the [flash] icon.

Importing Firmware Bundle

Make sure you have downloaded the firmware bundle from Cisco.com and saved it either in your local desktop or in a supported remote file system.

Step 1 On the menu bar, click the **Operations** icon and select **Firmware**.

Step 2 On the Firmware page, click the **Operations** icon and select **Import Firmware Bundle**.
This launches the **Import Firmware Bundle** dialog box.

Step 3 If you have a BIN file containing the firmware bundle in your local system,

a) In **FW Bundle Location** click **Local**.
b) In the **File Name** field, click the file icon to open your local browser.
c) From the file location, select the BIN file and click **Import**.

Step 4 If you have the firmware bundle in a remote file system,

Note Make sure you have the Hostname, User name and Password for the remote file system.

a) In **FW Bundle Location** click **Remote**.
This displays supported file transfer protocols.

b) Select one of the options from where you want to import files, enter the required information in the fields, and click **Import**.
For example, if you want to use the BIN file `ucs-k9-bundle-infra.2.2.3a.A.bin` on the remote server, you would enter the absolute path /home/cisco-ucs-central/firmware/ucs-k9-bundle-infra.2.2.3a.A.bin

What to Do Next

Add the firmware bundle to the appropriate policies and perform the upgrade.

Once the upgrade has been completed, you can delete the firmware bundle from Cisco UCS Central, but you must remove it from all associated policies first.

Enabling Automatic Firmware Update Sync-ups from Cisco.com

You must have a valid Cisco.com username and password to access the updated firmware bundles on Cisco.com.

Step 1 In the Task bar, type **Sync Firmware Updates from Cisco.com** and press Enter.
This launches the **Sync Firmware Updates from Cisco.com** dialog box.

Step 2 Enter your Cisco.com username and password in the appropriate fields.

Step 3 If you want Cisco UCS Central to automatically download new firmware updates:

a) Click **Enable** in the **Sync FW Updates Periodically** field.

b) Select the desired frequency in the **Frequency** field.

Note If you select **On Demand** in this field, Cisco UCS Central does not automatically download new firmware updates. Instead, you must download them manually using the **Sync** button in this dialog box.

Step 4 If you want your system to be able to access Cisco.com via HTTP, select **Enabled** in the **HTTP Proxy To Access Cisco.com** field and enter the HTTP connection information in the appropriate fields.

Note This functionality requires that Cisco UCS Central has network access to Cisco.com. Please enable and apply the proxy server configuration as appropriate.

Step 5 Click **Sync**.

Scheduling Infrastructure Firmware Update for a Cisco UCS Domain Group

You can schedule an infrastructure firmware update for all domains in a domain group.

Step 1 In the Task bar, type **Schedule Infra Firmware Update - Classic** and press Enter.
This launches the **Schedule Infra Firmware Update - Classic** dialog box.

Step 2 Select the domain group in the **Domain Group for UCS Infra Update** drop-down list.
Cisco UCS Central displays the number of domains that will be impacted by the firmware upgrade, and the Cisco UCS Manager version(s) on those domains.

Step 3 Select the firmware version you want to use in the **UCS Infra Update Version** drop-down list.

Step 4 (Optional) Select the catalog version in the **Catalog Version** drop-down list.

Step 5 Select the maintenance window in the **FW Update Maintenance Window** field.

Step 6 Select whether any server reboots require user acknowledgment in the **User Acknowledgement Required To Install** field.

- **Enabled—**A user must manually acknowledge the reboot request before any domain in the selected domain group is rebooted.
- **Disabled—**The domains in the selected domain group will be automatically rebooted as needed during the update.

Step 7 Click **Schedule**.
You can monitor the firmware update on the **Firmware** page. See Firmware Management, on page 1.

Removing an Infrastructure Firmware Schedule for a Cisco UCS Domain Group

Step 1 In the Task bar, type **Remove Infra Firmware Schedule - Classic** and press Enter.
This launches the **Remove Infra Firmware Schedule - Classic** dialog box.

Step 2 Select the domain group in the **Domain Group for UCS Infra Update** drop-down list.
Cisco UCS Central automatically populates the **UCS Infra Update Version**, **Catalog Version**, and **FW Update Maintenance Window** fields.

Step 3 Click **Remove**.

Creating or Editing a Host Firmware Package Policy

Step 1 In the Task bar, type **Create Host Firmware Package Policy** and press Enter.
This launches the **Create Host Firmware Package Policy** dialog box.

Step 2 On the **Basic** tab, click **Organization** and select the location in which you want to create the policy.

Step 3 Enter a **Name** and optional **Description**.
The policy name is case sensitive.

Step 4 Select the **Blade Version**, **Rack Version**, and/or **Modular Version** of the firmware, as required for your environment.

Step 5 In the **Components** tab, click the **Plus** icon to select any components that you would like to exclude from the firmware update.
The included and excluded components are displayed.

Note Excluding components is not supported for registered domains on Cisco UCS Manager release 2.2.6 or earlier.

Step 6 To remove an excluded component, select the check box for the component and click the **Trash** icon.

Step 7 Click **Create**.