Image Library

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. Access the Image Library through the **System Tools** icon.

- **Packages**—Displays all firmware packages.
- **Downloads**—Allows you to monitor the status of your downloads.

Use the firmware images when creating firmware policies.

In the Image Library, you can:

- Delete any downloaded image by selecting the image and clicking **Delete**.

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.

- Schedule Periodic Firmware Image Synchronizations
- Sync firmware images with images on Cisco.com
- Import Firmware Bundles (or Service Packs)

- For more information on downloading images, see Downloading Firmware from Cisco.com , on page 2.

Downloading Firmware from Cisco.com

You can configure Cisco UCS Central to communicate with the Cisco website at specified intervals to 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.

To download the Firmware image from cisco.com, you must:

1. Setup the cisco.com account with user credentials.
2. Accept EULA and K9 through the GUI.
3. Set the frequency of the sync (on-demand, daily, weekly, and bi-weekly).
4. Download the metadata.

Note This process runs in the background and takes approximately 15 minutes to complete. The download time varies based on the number of images.

5. Select an image from the metadata and download the image.

Important Make sure that you create a Cisco.com account to download firmware from Cisco.com to Cisco UCS Central.

Note If you change users in the Cisco.com account, this causes a full synchronization of the Image Library. Download operations are unavailable while it is synchronizing. This can take up to 15 minutes, depending on the size of the library.

Setting Up the Cisco.Com Account

Both the firmware management and hardware compatibility list credentials are managed through your cisco.com account.

Procedure

Step 1 Click the **System Configuration** icon and choose **Cisco.com Account**.

Step 2 Enter your user name and password.

Step 3 If you want your system to access Cisco.com through HTTP, choose **Enabled** in the **HTTP Proxy To Access Cisco.com** field. Enter the HTTP connection information in the appropriate fields.

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

Step 4 Select the Cisco Services that you want to use:

- Firmware Image Downloads—Select if you want to download Infrastructure Firmware updates and Firmware Image downloads from Cisco.com.
- Hardware Compatibility Catalog—Select if you want to synchronize your local list with Cisco.com, and to verify that the hardware you are using is compatible.

Step 5 Click **Save**.

Downloading Infrastructure Firmware Images from Cisco

Procedure

Step 1 Click the **System Tools** icon and choose **Image Library**.

Step 2 Click **Packages** to view the available packages.

Step 3 Select a package, or packages, and click the **Import Selected Image** icon.

Step 4 Click **Downloads**.

You can view information about the status of the download in the table.

Step 5 In the Transfer State column, click **Launch** to view the status dialog.

View detailed information about the download status in this dialog.

Deleting Images from the Firmware Library

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 by selecting it and clicking delete.
- **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.

Deleting Image Metadata from the Library of Images

You can only purge metadata through the CLI.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect operation-mgr**	Enters operations manager mode.
Step 2	UCSC(ops-mgr)# **scope firmware**	Enters the firmware management mode.
Step 3	UCSC(ops-mgr) /firmware# **scope download-source cisco**	Accesses the image metadata downloaded from Cisco website.
Step 4	UCSC(ops-mgr) /firmware/download-source# **purge list**	Deletes the firmware images metadata from the library of images.

Example

The following example shows how to delete the image metadata from the library of images:

```
UCSC# connect operation-mgr
UCSC(ops-mgr)# scope firmware
UCSC(ops-mgr) /firmware # scope download-source cisco
UCSC(ops-mgr) /firmware/download-source # purge list
```

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

The Cisco UCS Infrastructure Software Bundle includes Capability Catalog updates. Unless otherwise instructed by Cisco Technical Assistance Center, 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 3.x releases work with any 3.x release of the capability catalog, but not with 2.x releases. 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.

Scheduling Periodic Firmware Image Synchronization

Before you begin

You must have a valid Cisco.com username and password to access the updated firmware bundles on Cisco.com. See Setting Up the Cisco.Com Account

Procedure

Step 1 Click the **System Tools** icon and choose **Image Library**.

Step 2 In the Image Library page, click **Tools** and choose **Schedule Periodic Firmware Image Syncs**.

This launches the **Periodic Firmware Image Sync** dialog box.

Step 3 Select the frequency for infrastructure firmware downloads from www.cisco.com:

- **On Demand**—Downloads the firmware image library list when the user clicks **Schedule**.
- **Daily**—Downloads the firmware image library list once per day.
- **Weekly**—Downloads the firmware image library list once per week.
- **Bi-weekly**—Downloads the firmware image library every other week.

Step 4 Click **Cisco End User License Agreement** and follow the steps to accept the EULA.

Step 5 Click **K9 TM** and follow the steps to accept the agreement.

Step 6 Click **Schedule**.

Note After installing UCS Central, or after upgrading from UCS Central v1.4 to v1.5, and after performing the initial firmware image synchronization, downloading the image catalog from Cisco.com takes 15 minutes.

Importing Firmware Bundle

Before you begin

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

Procedure

Step 1 Click the **System Tools** icon and choose **Image Library**.

Step 2 On the Image Library page, click the **Tools** icon and choose **Import Firmware Bundle**.

This launches the **Firmware Bundle Import** 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 **Open**.
d) In the **Firmware Bundle Import** dialog box, click **Import**.

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

Note Make sure that 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 a transfer protocol.
c) 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 completes, delete the firmware bundle from Cisco UCS Central.

Note Remove the firmware bundle from all associated policies before deleting it.

Creating or Editing a Host Firmware Package Policy

Procedure

Step 1 In the **Actions** bar, type **Create Host Firmware Package Policy** and press Enter.

Step 2 In the **Host Firmware Package Policy** dialog box, click **Basic** and choose the **Organization** where 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** and **Rack Version** of the firmware, as required for your environment.

Step 5 Select the required **Service Pack Version** of the firmware.

A Service pack can be applied only to the base version of a release and it should be compatible with that version. If the service pack is incompatible with the base version, the following error message is displayed:

Package Version of all bundles in the pack must match.

For more information about applicable service packs, see About Service Packs. The service pack version rolls back to the default setting when you remove the selection from the drop-down. For more information on downloading images, see Downloading Firmware from Cisco.com in the *Cisco UCS Central Administration Guide*.

Step 6 In the **Components** tab, click **Add** to select any components that want to exclude from the firmware update.

The included and excluded components display.

Step 7 To exclude all components, click **Excluded Components**.

Step 8 To remove an excluded component, select it and click **Delete**.

Step 9 Click **Create**.

Note To understand the impact of the policy, click **Evaluate**.

After you create a Host Firmware Package policy and associate it with a service profile template, the Service Pack images take precedence and when it is resolved, the firmware image is applied to the components accordingly.