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.

Important You must accept the EULA and K9 agreements when creating a Cisco.com account. However, EULA and K9 are not supported through the CLI. You must go to the GUI and accept them.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a sub-domain group under the domain group root. To enter the domain group root mode, type **/** as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope connection-policy cisco**	Enters the connection policy mode for cisco.com.
Step 4	UCSC(policy-mgr) /domain-group/connection-policy # **set username** *username*	Enters the username for your cisco.com account
Step 5	UCSC(policy-mgr) /domain-group/connection-policy # **set password**	Enters the password for your cisco.com account. Password:
Step 6	Enter your cisco.com password.	
Step 7	(Optional) UCSC(policy-mgr) /domain-group/connection-policy # **set http-proxy** *IP address of proxy server| proxy URL*	Enables your system to access Cisco.com through an HTTP proxy server. **Note** This functionality requires that Cisco UCS Central has network access to Cisco.com.
Step 8	(Optional) UCSC(policy-mgr) /domain-group/connection-policy # **set proxy-username** *proxy username*	Enters your username for the HTTP proxy server.
Step 9	(Optional) UCSC(policy-mgr) /domain-group/connection-policy # **set proxy-password**	Enters your password for the HTTP proxy server. Password:
Step 10	(Optional) Enter your proxy server password.	
Step 11	UCSC(policy-mgr) /domain-group/fw-autosync-policy # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example shows how to create a cisco.com account:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope domain-group BayArea
UCSC(policy-mgr) /domain-group # scope connection-policy cisco
UCSC(policy-mgr) /domain-group/connection-policy # set username mdixon
UCSC(policy-mgr) /domain-group/connection-policy # set password
Password: password
UCSC(policy-mgr) /domain-group/connection-policy* # set http-proxy 10.193.200.100
UCSC(policy-mgr) /domain-group/connection-policy* # set proxy-username mdixon
UCSC(policy-mgr) /domain-group/connection-policy* # set proxy-password
HTTP Proxy Password: proxy password
UCSC(policy-mgr) /domain-group/connection-policy* # commit-buffer
UCSC(policy-mgr) /domain-group/connection-policy #
```

Configuring Firmware Image Download from Cisco

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect operation-mgr**	Enters operations manager mode.
Step 2	UCSC(ops-mgr)# **connect policy-mgr**	Enters policy manager mode from operations manager mode.
Step 3	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a sub-domain group under the domain group root. To enter the domain group root mode, type **/** as the *domain-group*.
Step 4	UCSC(policy-mgr) /domain-group # **scope download-policy cisco**	Enters the configuration mode.
Step 5	UCSC(policy-mgr) /domain-group/download-policy # **set**	**a.** **set admin-state** enabled | disabled **Note** Admin state is mandatory. **b.** **set downloadinterval** day | week | on-demand **Note** Download interval is mandatory. **c.** **set eula-status** *yes* | *no* **Note** EULA status is mandatory. **d.** **set http-proxy** *server:port* **e.** **username** *username* **Note** Username is mandatory. **f.** **set password** *password* **Note** Password is mandatory.

	Command or Action	Purpose
		g. **set proxy-password** *password* **h.** **set proxy-username** *username* Enters the configuration details to the system.
Step 6	UCSC(policy-mgr) /domain-group/download-policy/set # **commit-buffer**	Commits the transaction to the system.

Example

The following example shows how to configure firmware download to Cisco UCS Central from Cisco:

```
UCSC# connect operation-mgr
UCSC# (ops-mgr)# connect policy-mgr
UCSC(policy-mgr)# scope domain-group /
UCSC(policy-mgr) /domain-group # scope download-policy cisco
UCSC(policy-mgr) /domain-group/download-policy # set
admin-state  enable
downloadinterval 1 day
http-proxy  Server[:Port]
username          Username
password          Password
proxy-password    HTTP Proxy Password
proxy-username    HTTP Proxy Username
UCSC(policy-mgr) /domain-group/download-policy # commit-buffer
UCSC(policy-mgr) /domain-group/download-policy* #
```

Downloading Firmware Image from Cisco

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# **download list**	Downloads the available firmware image metadata from Cisco.com.

Example

The following example shows how to download a firmware image from Cisco.com to Cisco UCS Central:

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

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.

Viewing Image Download Status

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# **show download-task detail**	Displays the details of the download task.

Example

The following example shows how to view the download task details in Cisco UCS Central:

```
UCSC# connect operation-mgr
UCSC(ops-mgr)# scope firmware
```

```
UCSC(ops-mgr) /firmware # show download-task detail
Download task:
File Name: ucs-catalog.2.1.0.475.T.bin
Protocol: Ftp
Server:
Userid: User
Path: /automation/delmar/catalog
Downloaded Image Size (KB): 0
Image Url:
Image Url:
Proxy Userid:
State: Downloaded
Owner: Management
Current Task:
```

Viewing Downloaded Firmware Image Bundles

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 # **show package**	Displays the downloaded firmware image bundles. You can view the Cisco UCS Manager and Cisco UCS Central bundles. **Note** The classic UCS Infra bundle is not provided as an option for auto-install.

Example

The following example shows how to view the downloaded firmware image bundles in Cisco UCS Central:

```
UCSC# connect operation-mgr
UCSC(ops-mgr)# scope firmware
UCSC(ops-mgr) /firmware # show package

Name                                       Version    Download Status
------------------------------------------ ---------- ---------------
ucs-catalog.2.1.0.489.T.gbin               2.1(0.489)T Downloaded
ucs-k9-bundle-b-series.2.1.0.489.B.gbin    2.1(0.489)B Downloaded
ucs-k9-bundle-infra.2.1.0.489.A.gbin       2.1(0.489)A Downloaded
ucsCENTRAL-bundle.1.0.0.361.bin            1.0(0.361)  Downloaded
update.bin                                 1.0(0.376)  Downloaded


UCSC(ops-mgr) /firmware #
```

Downloading a Firmware Image

You can download firmware image from one of the following remote file systems:

- ftp
- scp
- sftp
- tftp

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# **download image** ftp | scp | sftp | tftp | *image file location*	Enters firmware image download configuration and mode and specifies the remote location for firmware image.
Step 4	UCSC(ops-mgr) /firmware # download image ftp: image file location /**Password:**	Authenticates access to the remote file system.

Example

The following example shows how to configure firmware download to Cisco UCS Central from a remote file system:

```
UCSC# connect operation-mgr
UCSC(ops-mgr)# scope firmware
UCSC(ops-mgr) /firmware # download image ftp:  Enter URL ftp:[//[username@]server][/path]
UCSC(ops-mgr) /firmware # download image ftp://image download path/Password:
UCSC(ops-mgr) /firmware #
```

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.

	Command or Action	Purpose
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
```

Periodic Firmware Synchronization

You can use the firmware auto-sync policy to determine whether firmware versions on recently discovered servers must be upgraded or not. With this policy, you can upgrade the firmware versions of recently discovered unassociated servers to match the firmware version defined in the default host firmware pack. In addition, you can determine if the firmware upgrade process should run immediately after the server is discovered or run at a later time.

Important The firmware automatic synchronization is dependent on the default host firmware pack. If you delete the default host firmware pack, it triggers a major fault. If you have configured a default host firmware pack, but not specified or configured a blade or rack server firmware in it, then it triggers a minor fault. Irrespective of the severity of the fault raised, you must resolve these faults prior to setting the **Firmware Auto Sync Server policy**.

Following are the values for the **Firmware Auto Sync Server policy**:

- **No Action**—No firmware upgrade is initiated on the server.

  This value is selected by default.

- **User Acknowledge**—Firmware on the server is not synchronized until the administrator acknowledges the upgrade in the **Pending Activities** dialog box.

The firmware for a server is automatically triggered when the following conditions occur:

- The firmware version on a server, or the endpoint on a server, differs from the firmware version configured in the default host firmware pack.
- The value for the firmware auto-sync policy has been modified.

Setting the Firmware Auto-Sync Policy

Use this policy to determine when and how you must update the firmware version of a recently discovered, unassociated server so that it matches with the firmware version of the default host firmware pack.

If the firmware version of a specific endpoint of a server differs from the version in the default host firmware pack, the FSM state displays the update status for that specific endpoint only. The firmware version of the server is not updated.

Before you begin

- You must create a default host firmware pack before setting this policy.
- You must log in as an administrator to complete this task.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a sub-domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope fw-autosync-policy**	Enters the firmware auto synchronization policy mode.
Step 4	UCSC(policy-mgr) /domain-group/fw-autosync-policy # **set auto-sync** {**no-actions** | **user-acknowledge**}	Choose one of the following values: • **user-acknowledge**—Firmware on the server is not synchronized until the administrator acknowledges the discovered server in the server command mode. • **no-actions**—No firmware upgrade is initiated on the server.
Step 5	UCSC(policy-mgr) /domain-group/fw-autosync-policy # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example shows how to set the firmware autosync policy:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope domain-group
UCSC(policy-mgr) /domain-group # scope fw-autosync-policy
UCSC(policy-mgr) /domain-group/fw-autosync-policy # set auto-sync user-acknowledge
UCSC(policy-mgr) /domain-group/fw-autosync-policy* # commit-buffer
UCSC(policy-mgr) /domain-group/fw-autosync-policy #
```

What to do next

If you set the value to User Acknowledge, then you must acknowledge the pending activity for the server for the firmware synchronization to occur.

Creating a Host Firmware Package

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope org** *org-name*	Enters the organizations mode for the specified organization. To enter the root mode type/ as the *org-name*.
Step 3	UCSC(policy-mgr) /org # **create fw-host-pack***policy name*	Creates the specified host firmware pack.
Step 4	UCSC(policy-mgr) /org/fw-host-pack # **set descr** *description*	Specifies the description for the host firmware policy.
Step 5	UCSC(policy-mgr) /org/fw-host-pack # **set bladebundleversion** *version number*	Specifies the blade server bundle version for the host firmware policy.
Step 6	UCSC(policy-mgr) /org/fw-host-pack # **set rackbundleversion** *version number*	Specifies the rack server bundle version for the host firmware policy.
Step 7	UCSC(policy-mgr) /org/fw-host-pack #**create exclude-server-component** {**adapter** | **board-controller** | **cimc** | **flexflash-controller** | **graphics-card** | **host-hba** | **host-hba-optionrom** | **host-nic** | **host-nic-optionrom** | **local-disk** | **psu** | **raid-controller** | **sas-expander** | **server-bios**}	Creates an excluded component and enters exclude server component mode. **Note** You must repeat the **exclude-server-component** command for each component that you want to exclude from the host firmware package.
Step 8	UCSC(policy-mgr) /org/fw-host-pack/exclude-server-component #**exit**	Returns to host firmware pack mode.
Step 9	UCSC(policy-mgr) /org/fw-host-pack # **commit-buffer**	Commits the transaction to the system.

Example

The following example shows how to:

- Create a host firmware pack called FWPack1
- Add a blade server bundle version

- Exclude the psu and server-bios

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org
UCSC(policy-mgr) /org # create fw-host-pack FWPack1
UCSC(policy-mgr) /org/fw-host-pack* # create exclude-server-component psu
UCSC(policy-mgr) /org/fw-host-pack/exclude-server-component* # exit
UCSC(policy-mgr) /org/fw-host-pack* # create exclude-server-component server-bios
UCSC(policy-mgr) /org/fw-host-pack/exclude-server-component* # commit-buffer
UCSC(policy-mgr) /org/fw-host-pack/exclude-server-component #
```

Viewing Host Firmware Packages

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope org**	Enters into the organization.
Step 3	UCSC(policy-mgr) /org # **show fw-host-pack detail**	Displays a list of host firmware packages.

Example

The following example shows how to display available host infrastructure firmware packages:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org
UCSC(policy-mgr) /org # show fw-host-pack detail
Compute Host Pack:

Name: root/Default
Mode: Staged
Blade Bundle Version: 2.1(0.469)B
Rack Bundle Version: 2.1(0.469)C
Description: UCSC

Name: root/default
Mode: Staged
Blade Bundle Version: 2.1(0.474)B
Rack Bundle Version: 2.1(0.474)C
Description: default from UCSC

Name: root/latest
Mode: Staged
Blade Bundle Version: 2.1(0.469)B
Rack Bundle Version: 2.1(0.469)C
Description: latest

Name: root/Marketing/mytest
```

```
Mode: Staged
Blade Bundle Version: 2.1(0.469)B
Rack Bundle Version: 2.1(0.469)C
Description: Test
UCSC(policy-mgr) /domain-group #
```

Acknowledging a Pending Activity

This procedure describes the process to acknowledge the start of a host firmware update from the Cisco UCS Central CLI.

Procedure

	Command or Action	Purpose
Step 1	UCSC # **connect resource-mgr**	Enters resource manager mode.
Step 2	UCSC(resource-mgr) # **scope org**	Enters into the organization.
Step 3	UCSC(resource-mgr) /org # **show ucs-service-profile**	Displays the existing service profiles.
Step 4	UCSC(resource-mgr) /org # **scope ucs-service-profile***service-profile-name*	Enters the UCS service profile.
Step 5	UCSC(resource-mgr) /org/ucs-service-profile # **show instance**	Displays the instances in the service profile.
Step 6	UCSC(resource-mgr) /org/ucs-service-profile # **scope instance***instance-ID*	Scopes into the instance.
Step 7	UCSC(resource-mgr) /org/ucs-service-profile/instance # **show pending-changes**	Displays all pending activities for that service profile.
Step 8	UCSC(resource-mgr) /org/ucs-service-profile/instance # **apply pending-changes immediate**	Acknowledges all of pending activities.
Step 9	UCSC(resource-mgr) /org/ucs-service-profile/instance * # **commit-buffer**	Commits the transaction to the system.

Example

The following example shows how to acknowledge a pending activity:

```
UCSC# connect resource-mgr
UCSC(resource-mgr)# scope org
UCSC(resource-mgr) /org # show ucs-service-profile
Service Profiles deployed on UCS domain:
    Name                 Status               Ref Count Instantiation State
    -------------------- -------------------- --------- -------------------
    SP-1                 Ok                           1 Instantiated
```

```
    SPCSCuz56952         Ok                            1 Instantiated

UCSC(resource-mgr) /org # scope ucs-service-profile SP-1
UCSC(resource-mgr) /org/ucs-service-profile # show instance
Compute Instance:
    ID    Name            Status          Assoc State  Config State Physical Ref
    ----- --------------- --------------- ------------ ------------ ------------
     1008 Dhana           Ok              Associated   Applied      SP-1/1008

UCSC(resource-mgr) /org/ucs-service-profile/ # scope instance 1008
UCSC(resource-mgr) /org/ucs-service-profile/instance # show pending-changes
Pending Changes:
    State                    Pending Changes       Pending Disruptions
    ------------------------ --------------------- -------------------
    Untriggered              0                     0

UCSC(resource-mgr) /org/ucs-service-profile/instance # apply pending-changes immediate
UCSC(resource-mgr) /org/ucs-service-profile/instance* # commit-buffer
```

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.

Configuring a Capability Catalog Upgrade

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) #**scope org**	Scopes into the organization.
Step 3	UCSC(policy-mgr) /org # **scope domain-infra-profile** *job-name*.	Enters the infrastructure firmware policy job that you created previously.
Step 4	UCSC(policy-mgr)/org # **scope fw-catalog-pack-config** <*config-name*>	Enters the capability catalog packages mode.
Step 5	UCSC(policy-mgr) /org/fw-catalog-pack # **set catalogversion** <*catalogversion*>	Specifies the capability catalog version for this update.
Step 6	UCSC(policy-mgr) /org/fw-catalog-pack* # **commit-buffer**	Commits the transaction to the system.

Example

The following example shows how to configure a capability catalog update:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)* # scope org
UCSC policy-mgr) /org* # scope domain-infra-profile job1
UCSC(policy-mgr) /org/domain-infra-profile/ # scope fw-catalog-pack-config job50
UCSC(policy-mgr) /org/domain-infra-profile/fw-catalog-pack-config # set catalogversion 1.5
UCSC(policy-mgr) /org/domain-infra-profile/fw-catalog-pack-config* # commit-buffer
UCSC(policy-mgr) /org/domain-infra-profile/fw-catalog-pack-config #
```

Viewing a Capability Catalog in a Domain Group

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) #**scope org**	Scopes into the organization.
Step 3	UCSC(policy-mgr) /org # **scope domain-infra-profile** *job-name*.	Enters the infrastructure firmware policy job that you created previously.
Step 4	UCSC(policy-mgr)/org/domain-infra-profile # **scope fw-catalog-pack-config** *default*	Enters the capability catalog packages mode.
Step 5	UCSC(policy-mgr) /org/domain-infra-profile/fw-catalog-pack # **show detail**	Specifies the capability catalog version for this update.

Example

The following example shows how to view the capability catalog:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)* # scope org
UCSC policy-mgr) /org* # scope domain-infra-profile job1
UCSC(policy-mgr) /org/domain-infra-profile # scope fw-catalog-pack-config default
UCSC(policy-mgr) /org/domain-infra-profile/fw-catalog-pack-config # show detail
UCSC(policy-mgr) /org/domain-infra-profile/fw-catalog-pack-config * #
```

Deleting a Capability Catalog Policy

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.

	Command or Action	Purpose
Step 2	UCSC(policy-mgr) #**scope org**	Scopes into the organization.
Step 3	UCSC(policy-mgr) /org # **scope domain-infra-profile** *job-name*.	Enters the infrastructure firmware policy job that you created previously.
Step 4	UCSC(policy-mgr) /domain-group # **delete fw-catalog-pack-config***name*	Deletes the specified catalog policy from the domain group.
Step 5	UCSC(policy-mgr) /domain-group* # **commit-buffer**	Commits the transaction to the system.

Example

The following example shows how to delete a capability catalog policy from a domain group:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)* # scope org
UCSC policy-mgr) /org* # scope domain-infra-profile job1
UCSC(policy-mgr) /org/domain-infra-profile # scope fw-catalog-pack-config config1
UCSC(policy-mgr) /org/domain-infra-profile/fw-catalog-pack-config # delete
fw-catalog-pack-config config1
UCSC(policy-mgr) /org/domain-infra-profile/fw-catalog-pack-config* # commit-buffer
UCSC(policy-mgr) /org/domain-infra-profile/fw-catalog-pack-config* #
```