Cisco Intersight Management

- Device Connector, on page 1
- Enabling or Disabling Cisco Intersight Management, on page 1
- Viewing Intersight Device Connector Properties, on page 2
- Updating Device Connector, on page 5

Device Connector

Device connector connects Cisco UCS Manager to Cisco Intersight, the cloud-hosted server management system. It enables Cisco UCS Manager to be managed and monitored through Cisco Intersight.

To register a device with Cisco Intersight in the cloud, you must do the following:

1. Connect Cisco UCS Manager with Cisco Intersight by configuring the device connector proxy settings, if they are required.
2. Use the device serial number and security code to validate your access to the device from Cisco Intersight and claim the device.

Enabling or Disabling Cisco Intersight Management

When you enable Cisco Intersight management, it establishes a bidirectional communication between the Intersight Cloud application and the device.

Before you begin

You must be an administrator to configure the device connector.

Procedure

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

Step 2 Expand **All** > **Device Connector**.

Step 3 In the **Intersight Management** area, click **On** to enable Intersight management or **Off** to disable Intersight management.

By default, the Cisco Intersight Management state is **Enabled**.

The **Connection** area displays the connection status of Intersight management. If the device connector has not been able to establish a connection to Intersight management, review the recommendations provided in the **Details & Recommendations** drop-down list to fix the connection issues.

Step 4 Select the **Access Mode** as **Read-only** or **Allow Control**.

You cannot configure the device through Cisco Intersight when the **Read-only** access mode is selected. Therefore, any configuration that comes to the device connector through the cloud is rejected with an error code.

You have full control to configure the device through Cisco Intersight when the **Allow Control** mode is selected.

Step 5 To disable the Intersight management, click **Off**.

When you disable the Intersight management, the **Connection** area displays the connection status as **Administratively Disabled**.

Viewing Intersight Device Connector Properties

Procedure

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

Step 2 Expand **All** > **Device Connector**.

Step 3 In the **Intersight Management** area, review the following information:

Name	Description
Enabled radio button	The state of the connection between Cisco UCS Manager and Cisco Intersight. Allows you to enable or disable the Cisco Intersight management. This can be one of the following: • **On**—Enables Cisco Intersight management. You can claim this system and leverage the capabilities of Cisco Intersight. This is the default connection status. • **Off**—Disables Cisco Intersight management. No communication will be allowed with Cisco Intersight.

Step 4 In the **Connection** area, review the following information:

Table 1:

Name	Description
Status field	Displays the status of the connection to Cisco Intersight. This can be one of the following: • **Administratively Disabled**—Indicates that the Intersight management has been disabled. • **DNS Misconfigured**—DNS has been configured incorrectly in Cisco UCS Manager. • **UCS Connect Network Error**—Indicates the invalid network configurations. • **Certificate Validation Error**—Cisco UCS Manager is refusing to establish a connection to the Cisco Intersight platform because the certificate presented by the Cisco Intersight platform is invalid. Ensure that you allow https traffic from URL `svc.ucs-connect.com` to the devices that are in the path by making necessary changes to their SSL proxy, Web filtering, or transparent Web proxy. • **Claimed**—The connection to the Cisco Intersight platform is successful and you have claimed the connection. • **Not Claimed**—The connection to the Cisco Intersight platform is successful, but still not claimed. You can claim an unclaimed connection through Cisco Intersight.
Details & Recommendations drop-down list	Lists the details and recommendations to fix the connection issues based on the status.
Access Mode field	Whether access permissions are set to **Read-Only** or **Allow Control**. The mode will be **Allow Control** by default.
Device ID field	The unique serial number of the device.
Claim Code	The security code provided to the device. Provide this security code to claim the device from Cisco Intersight. **Note** This code is available only when **Connection** status is **Not Claimed**.

Step 5 In the **Settings** area, review the following information:

Name	Description
General tab	Configures Access mode settings. **Access Mode**—Configure access as **Read-only** or **Allow Control**. • **Read-only**—When the **Read-only** access mode is selected, you cannot configure the device through Intersight. • **Allow Control**—When the**Allow Control** access mode is selected, you have full control to configure the device through Intersight.
Proxy Configuration tab	Whether HTTPS proxy settings are disabled or manually configured. This can be one of the following: • **Off**—Select this option if you want to disable the HTTPS proxy settings configuration. This is the default HTTPS proxy setting. • **On**—Select this option if you want to enable the HTTPS proxy settings configuration. • **Proxy Hostname/IP**—Enter the proxy hostname or IP address. • **Proxy Port**— Enter the proxy port number. • **Authentication**—Enable this option to authenticate access to the proxy server. Enter the **Username** and **Password** to authenticate access. **Note** The device connector does not mandate the format of the login credentials, they are passed as-is to the configured HTTP proxy server. Whether or not the username must be qualified with a domain name will depend on the configuration of the HTTP proxy server.

Name	Description
Certificate Manager tab	Allows you to view a list of trusted certificates and import a valid trusted certificate. • **Import**—Allows you to select and import a CA signed certificate. **Important** The imported certificate must be in the *.pem (base64 encoded) format. • You can view the list of certificates with the following information: • **Name**—Common name of the CA certificate • **In Use**—Whether the certificate in the trust store was used to successfully verify the remote server • **Issued By**—The issuing authority for the certificate • **Expires**—The expiry date of the certificate **Note** You cannot delete bundled certificates.

Updating Device Connector

When you upgrade Cisco UCS Manager, the device connector is automatically updated to the image integrated with the Cisco UCS Manager version. The device connector does not get downgraded when you downgrade the Cisco UCS Manager version.

You can update the device connector through the Cisco Intersight GUI. You can also update the device connector through the local management shell in Cisco UCS Manager CLI.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **connect local-mgmt**	Enters local management mode.
Step 2	UCS-A(local-mgmt)# **copy** [*from-filesystem*:] [*from-path*] *filename to-path* [*dest-filename*]	Copies the device connector image file from a remote server to a local destination by using the specified file transfer protocol. You need to copy the file to one fabric interconnect only. • *from-filesystem*—The remote file system containing the file to be copied. This file system can be specified by using one of the following options: • **ftp:** [// [*username@*] *server*]

	Command or Action	Purpose
		• **scp:** [// [*username@*] *server*] • **sftp:** [// [*username@*] *server*] • **tftp:** [//*server* [:*port*]] If the file system is not specified, the current working file system is assumed. If a remote protocol is specified with no server name, you are prompted to enter the server name. • *from-path*—Absolute or relative path to the file to be copied. If no path is specified, the current working directory is assumed. • *filename*—The name of the source file to be copied. • *to-path*—Absolute or relative path to the copied file. If no path is specified, the current working directory is assumed. The path includes the local file system to contain the copied file. This file system can be specified from one of the following options: • **volatile:** • **workspace:** • *dest-filename*—The new name for the copied file. If a dest-filename is specified, the copied file is renamed at the destination location. **Note** You cannot download the device connector image file through Cisco UCS Manager GUI.
Step 3	UCS-A(local-mgmt)# **update-device-connector workspace:** | **volatile:**/*filename* [**skip-upgrade-on-peer**]	Updates the device connector image on the peer fabric interconnect and then the local fabric interconnect. Using the **skip-upgrade-on-peer** option skips update on the peer fabric interconnect.

Example

The following example updates the device connector on both fabric interconnects:

```
UCS-A# connect local-mgmt
UCS-A(local-mgmt)# copy scp://username@10.100.100.100/filepath/filename.bin workspace:/
UCS-A(local-mgmt)# update-device-connector workspace:/filename.bin
Update Started
Updating Device Connector on peer Fabric interconnect
Successfully updated device connector on peer Fabric interconnect
Updating Device Connector on local Fabric interconnect
Successfully updated device connector on local Fabric interconnect
UCS-A(local-mgmt)#
```

The following example updates the device connector on the local fabric interconnect only:

```
UCS-A# connect local-mgmt
UCS-A(local-mgmt)# copy scp://username@10.100.100.100/filepath/filename.bin workspace:/
UCS-A(local-mgmt)# update-device-connector workspace:/filename.bin skip-upgrade-on-peer
Update Started
Updating Device Connector on local Fabric interconnect
Successfully updated device connector on local Fabric interconnect
UCS-A(local-mgmt)#
```