Claiming a Target

Device Connector Requirements

You can claim a target in Cisco Intersight Virtual Appliance through the embedded device connector. Before you claim a target, ensure that the device connector requirements are met. The following table lists the software compatibility and the supported device connector versions for Intersight Virtual Appliance:

Table 1: Device Connector Requirements

Component	Minimum software version for Connected Virtual Appliance	Minimum software version for Private Virtual Appliance	Supported Device Connector version	Minimum supported versions that include supported Device Connectors
Cisco UCS Manager	3.2(1)	4.0(2a)	1.0.9-2290	4.0(2a)
Cisco IMC Software	For M5 Servers: 3.1(3a) For M4 Servers: 3.0(4)	4.0(2d)	1.0.9-335	4.0(2d)
HyperFlex Connect and Data Platform	2.6	3.5(2a)	1.0.9-1335	3.5(2a)
CIsco UCS Director	6.7.2.0	6.7.2.0	1.0.9-911	6.7.2.0

Device Connector Upgrade

When the Device Connector on an endpoint is not at the compatible version, you can upgrade it in the following ways:

- Perform a complete firmware upgrade to the version that has the supported Device Connector. This process could involve updating your configuration settings.

- Manually upgrade the Device Connector. This option is supported only on Cisco UCS Manager. For more information, See Manual Upgrade of Device Connector (applicable only to Cisco UCS Fabric Interconnect).

- Cisco Intersight Virtual Appliance supports upgrading the device connector from the cloud. When the target claim process detects that the device connector at the endpoint is not at the compatible version, it triggers an upgrade of the device connector from Intersight cloud. To facilitate this upgrade, port 80 must be open between the appliance and the endpoint target. The HTTPS proxy running on port 80 requires that your firewall settings allow communication through port 80.

  Device Connector upgrade from Intersight cloud is optional. During the upgrade from the cloud, some target data (server inventory) from the appliance leaves your premise. When you choose this option the following data leaves your premises:

  - The endpoint target type - Cisco UCS Fabric Interconnect, Integrated Management Controller, Cisco HyperFlex System, Cisco UCS Director

  - The firmware version(s) of the endpoint

  - The serial number(s) of the endpoint target

  - The IP address of the endpoint target

  - The hostname of the endpoint target

  - The endpoint device connector version and the public key

Attention Target claim could fail if the device connector is at an older version that does not support the appliance, and you have disabled the data collection option during the initial setup. This failure is caused due to details about the endpoint being required to leave the premises for the one time upgrade to work. To avoid a target claim failure, select the Enable Data Collection option temporarily or upgrade the device connector in the other methods mentioned above.

Manual Upgrade of Device Connector (applicable only to Cisco UCS Fabric Interconnect)

If you do not want to share the target data as part of the automatic device connector upgrade, you can choose to manually upgrade the device connector on a Cisco UCS Fabric Interconnect. Use these instructions to upgrade the device connector:

```
Log in to your UCS Fabric Interconnect as an admin user and run the following command:
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 local Fabric interconnect
Successfully updated device connector on local Fabric interconnect
UCS-A(local-mgmt)#
```

Data Collected from Intersight Virtual Appliance

Cisco Intersight Virtual Appliance works on a connected mode and requires connectivity to hosted Intersight services. You must register the appliance with Intersight to manage your UCS or HyperFlex infrastructure.

If you enable the option to allow collecting additional information, Intersight may collect other details about the managed systems, beyond what is listed in the table **Minimum Data Collected**. If the data collection option is enabled, Cisco reserves the right to collect more data for diagnosis and proactive troubleshooting purposes.

The tables below list the details of data collected by Intersight:

Table 2: Minimum Data Collected

Component	Details of Data Collected
From Intersight Virtual Appliance	• The appliance ID (Serial Number) • The IP address of the appliance • The hostname of the appliance • The device connector version and public key on the appliance
Appliance Software Auto-Upgrade	Version of software components or the services running on the appliance
Appliance Health	• CPU usage • Memory usage • Disk usage • Service statistics
Licensing	Server count
Information about the endpoint target	• Serial number and PID (to support Connected TAC) • UCS Domain ID • Platform Type

Table 3: Data Collected During One time Device Connector Upgrade

Component	Details of Data Collected
From the endpoint target, only if the one time device connector upgrade is used	• The endpoint target type - Cisco UCS Fabric Interconnect, Integrated Management Controller, Cisco HyperFlex System • One or more firmware versions of the endpoint • The serial number of the endpoint target • The IP address of the endpoint target • The hostname of the endpoint target • The endpoint device connector version and the public key

TechSupport Diagnostic File Collection (Open a TAC Case)

When you open a case with Cisco TAC, Intersight collects Tech Support diagnostic files to assist with an open support case. The data collected could include (but is not limited to) hardware telemetry, system configuration, and any other details which aid in active troubleshooting of the TAC case. TechSupport collection is allowed to occur regardless of data collection options you specify. However, this information is not collected arbitrarily, but only when you open a case against a system, requiring assistance with the system support.

Claiming a Target in Intersight Virtual Appliance

Log in to the appliance as a user with account administrator privileges. Use the following procedure to claim a target in Cisco Intersight Virtual Appliance:

Before you begin

- Ensure that you have completed the Cisco Intersight Virtual Appliance OVA installation and set up the appliance.
- You have an account on the target being claimed that has administrative privileges.
- You can claim a target or multiple targets in bulk.

Step 1 Navigate to **Admin** > **Targets** > **Claim a New Target**.

You can either use the wizard to set the configuration or use a file to set the configuration.

Step 2 To use the wizard to set the configuration, select the **Use Wizard to Set the Configuration** tab and click **Start**.

a) Select **Available for Claiming**.
b) Select the target type.
c) Enter the IP/Hostname of the target you want to claim, the Username for the target, and the Password for the user. This user must have administrative privileges.
d) Click **Claim** to initiate the target claim.

Step 3 To use a file to set the configuration, select the **Use a File to Set the Configuration** tab and click **Start**.

a) Click **Browse** to select the .csv file containing the target details.

For each target, add a line containing Target Type, Hostname or IP Address, User Name, and Password. Use the CIDR notation to specify the IP Range. You can add as many lines with these details in the .csv file. The following example shows the format to add target details in a .csv file:

```
UCSFI,10.1.1.3,user-1,password1
IMC,10.1.1.5/26,user-2,password2
HX,10.1.2.1/30,user-3,password3
UCSD,1.1.1.1,user-4,password4
```

b) Click **Next**.

c) Review the details on the Summary page and click **Claim**.

Important The target claim process could take a few minutes. If required, the Device Connector will be automatically upgraded as part of the process.

You can unclaim a target by selecting a target from **Targets** > **Table view**, and clicking **Delete** (trash can representation). You can reclaim the target later, as required by using the steps listed above for a target claim.

Renewing Target Certificates

In the event that the target certificate expires for an endpoint, the status reflects as **Not Connected** on the Target Table View page and the badge for this endpoint indicates that the target certificate has expired.

Step 1 In the appliance UI, navigate to **Admin** > **Targets** and locate the target with the **Not Connected** status.

Step 2 Hover on the badge to find out if the target certificate has expired.

Step 3 Click the **Actions** menu for this target, and select **Renew Certificate**.

Note The **Renew Certificate** option is available only if the certificate needs to be renewed for the selected endpoint.

Step 4 In the **Renew Certificate** pop-up window, enter the username and password and click **Renew**.

After the certificate renewal process completes, the status for the endpoint indicates as **Connected**.