Cisco Cloud APIC and Intersight Device Connector

Revised: July 10, 2022

New and Changed Information

The following table provides an overview of the significant changes to this guide up to this current release. The table does not provide an exhaustive list of all changes made to the guide or of the new features up to this release.

Table 1: New Features and Changed Behavior

Cisco APIC Release	Feature	Description
25.0(4)	Initial release of this feature	Initial release of this feature.

About Device Connector

Devices are connected to the Intersight portal through a Device Connector that is embedded in the management controller of each system. Device Connector provides a secure way for the connected devices to send information and receive control instructions from the Cisco Intersight portal, using a secure Internet connection.

When an Intersight-enabled device or application starts, the Device Connector starts at boot by default, and attempts to connect to the cloud service. If the **Auto Update** option is enabled, the Device Connector is automatically updated to the latest version through a refresh by the Cisco Intersight service when you connect to Cisco Intersight. For more information on the **Auto Update** option, see About the Auto Update Option, on page 2.

About the Auto Update Option

This **Auto Update** option is enabled by default. We recommend that you leave the **Auto Update** option enabled.

When the **Auto Update** option is enabled, the Device Connector automatically initiates an upgrade after receiving an Upgrade message from the Cisco Intersight Cloud. During this time, the Device Connector checks if a Cisco Cloud APIC is being upgraded. If a Cisco Cloud APIC is being upgraded, then the Device Connector upgrade will be postponed to maximum of 24 hours, after which the Device Connector is upgraded regardless if a Cisco Cloud APIC is being upgraded. If there are no Cisco Cloud APICs being upgraded, then the Device Connector initiates its upgrade immediately. Likewise, the Cisco Cloud APIC upgrade pre-validation process verifies if the Device Connector is being upgraded when you initiate a Cisco Cloud APIC upgrade. In such a case, the upgrade page displays a corresponding warning message.

If a Device Connector upgrade is in progress, a message is displayed, saying that the DC upgrade is in progress and to wait until the DC upgrade is complete before triggering a Cloud APIC upgrade.

If the Cisco Cloud APIC pre-upgrade validation is unable to check the Device Connector upgrade status, the following message displays:

```
Could not check DC upgrade status
```

In this case, re-initiate the Cisco Cloud APIC upgrade. If the upgrade fails again with the same message, wait 1 or 2 minutes and try again.

If the **Auto Update** option is disabled and there is a new Device Connector software version available, you will be prompted in the Device Connector GUI page to update the software manually when new releases become available. In addition, the Device Connector can become out-of-date, which can affect the ability of the Device Connector to connect to Cisco Intersight.

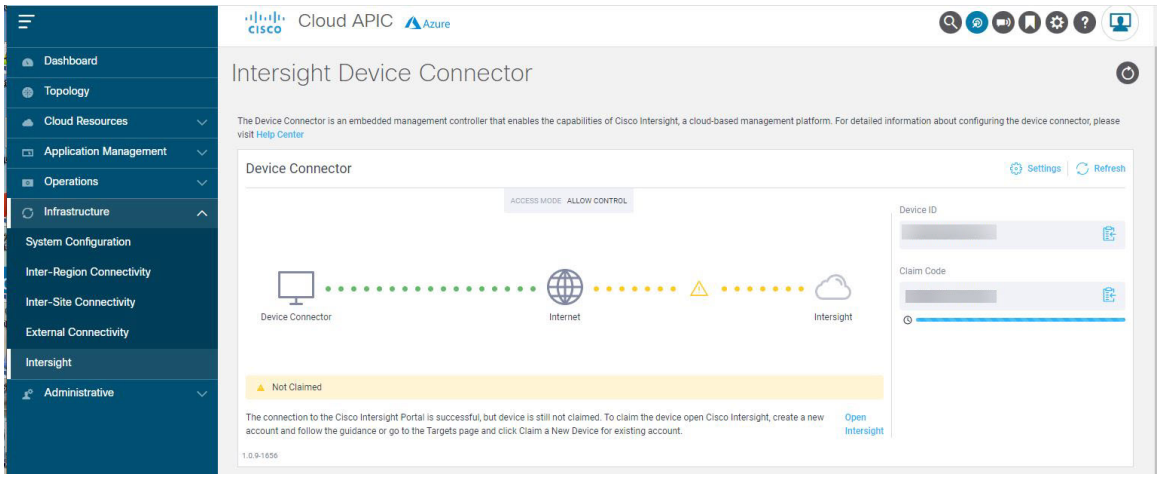
Configuring the Intersight Device Connector

Procedure

Step 1 In the Cisco Cloud APIC GUI, navigate to **Infrastructure** > **Intersight**.

The **Intersight Device Connector** overview page appears.

You should see green dotted lines connecting **Device Connector** to **Internet** in the **Device Connector** graphic in this page.



- If you see green dotted lines connecting **Internet** to **Intersight** in the **Device Connector** graphic, and the text **Claimed** underneath the graphic, then your Intersight Device Connector is already configured and connected to the Intersight service, and the device is claimed.
- If you see yellow dotted lines and a caution icon connecting **Internet** to **Intersight** in the **Device Connector** graphic, and the text **Not Claimed** underneath the graphic, then your Intersight Device Connector is not yet configured and connected to the Intersight service, and the device is not yet claimed. Follow these procedures to configure the Intersight Device Connector and connect to the Intersight service, and claim the device.

Note If you see red dotted lines connecting **Internet** to **Intersight** in the **Device Connector** graphic, go to Step 13, on page 7 to check the connections to troubleshoot the issue.

Step 2 Determine if you would like to update the software at this time, if there is a new Device Connector software version available.

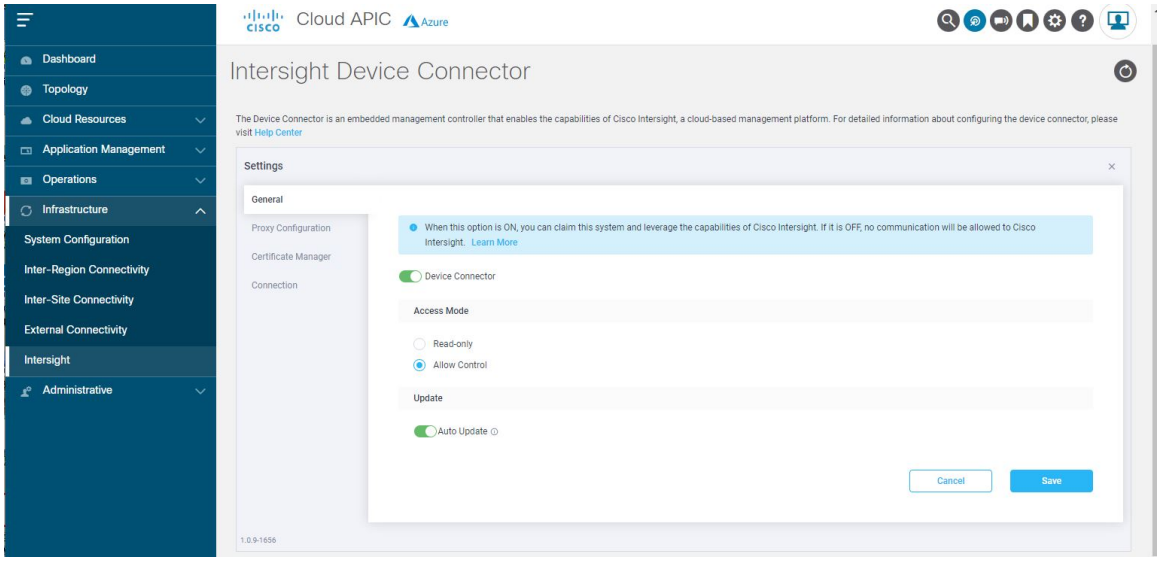
If there is a new Device Connector software version available and you do not have the **Auto Update** option enabled, you will see a message towards the top of the screen telling you that Device Connector has important updates available.

- If you do not want to update the software at this time, go to Step 3, on page 4 to begin configuring the Intersight Device Connector.
- If you would like to update the software at this time, click one of the two links in the yellow bar toward the top of the page, depending on how you would like to update the software:
  - **Update Now**: Click this link to update the Device Connector software immediately.

- **Enable Auto Update**: Click this link to go to the **General** page, where you can toggle the **Auto Update** field to ON, which allows the system to automatically update the Device Connector software. See About the Auto Update Option, on page 2 for more information.

Step 3 Locate the **Settings** link to the right of the **Device Connector** heading and click the **Settings** link.

The **Settings** page appears, with the **General** tab selected by default.



Step 4 In the **General** page, configure the following settings.

a) In the **Device Connector** field, determine if you want to allow communication between the device and Cisco Intersight.

The **Device Connector** option (enabled by default) allows you to claim the device and leverage the capabilities of Intersight. If it is disabled, no communication will be allowed to Intersight.

b) In the **Access Mode** field, determine if you want to allow Intersight the capability to make changes to this device.

Access Mode enables you to allow full read/write operations from the cloud or restrict changes made to this device from Intersight.

- The **Read-only** option ensures that no changes are made to this device from Intersight. For example, actions such as upgrading firmware or a profile deployment will not be allowed in the Read-Only mode. However, the actions depend on the features available for a particular system.
- The **Allow Control** option (selected by default) enables you to perform full read/write operations from the cloud, based on the features available in Cisco Intersight.

c) In the **Auto Update** field, determine if you want to allow the system to automatically update the software.

- Toggle ON to allow the system to automatically update the software.
- Toggle OFF so that you manually update the software when necessary. You will be asked to manually update the software when new releases become available in this case.

See About the Auto Update Option, on page 2 for more information.

Step 5 When you have completed the configurations in the **General** page, click **Save**.

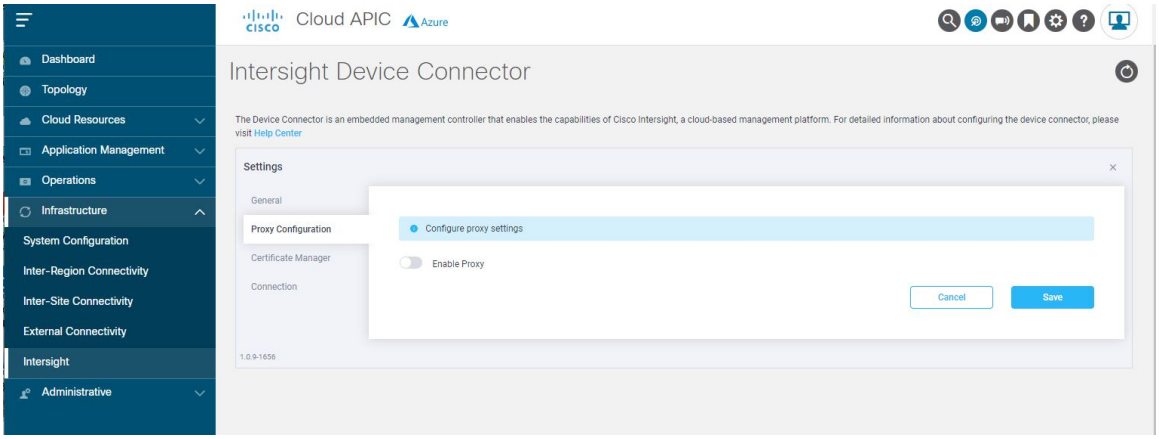
The **Intersight Device Connector** overview page appears again.

Step 6 Continue with the next steps of the configuration process, if necessary.

- If you want to configure the proxy that the Device Connector will use to communicate with the Intersight cloud, go to Step 7, on page 5.
- If you want to manage certificates with the Device Connector, go to Step 10, on page 6.
- If you want to check the connections, go to Step 13, on page 7.

Step 7 If you want to configure the proxy that the Device Connector will use to communicate with the Intersight cloud, click **Settings**, then click **Proxy Configuration**.

The **Proxy Configuration** page appears.



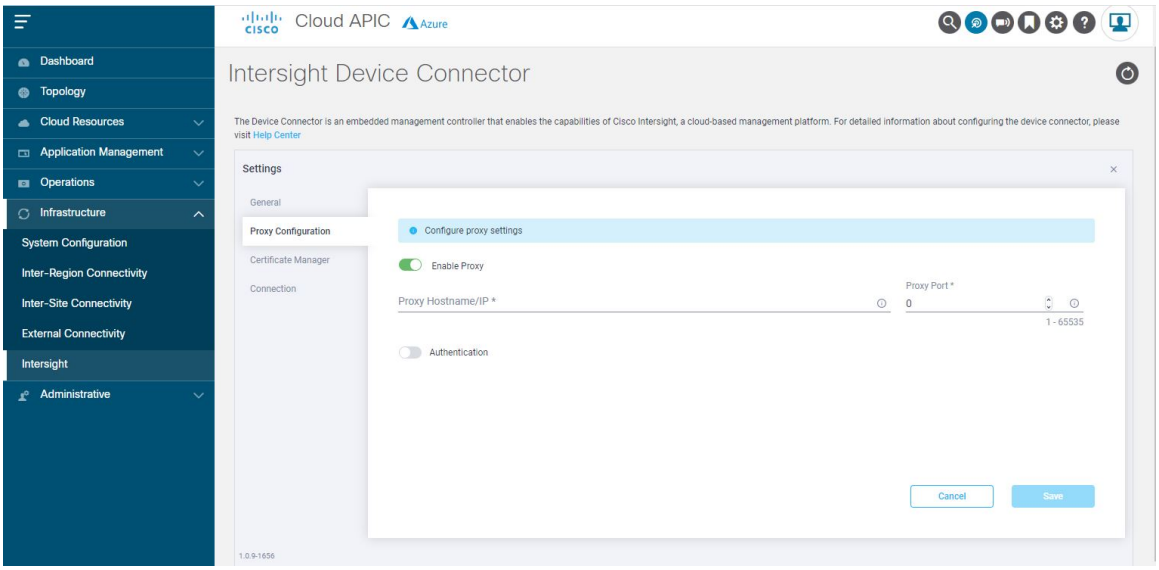
Step 8 In the **Proxy Configuration** page, configure the following settings.

In this page, you can configure the proxy that the Device Connector will use to communicate with the Intersight cloud.

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 depends on the configuration of the HTTP proxy server.

a) In the **Enable Proxy** field, toggle the option to ON to configure the proxy settings.

The **Proxy Hostname/IP** and **Proxy Port** fields appear.

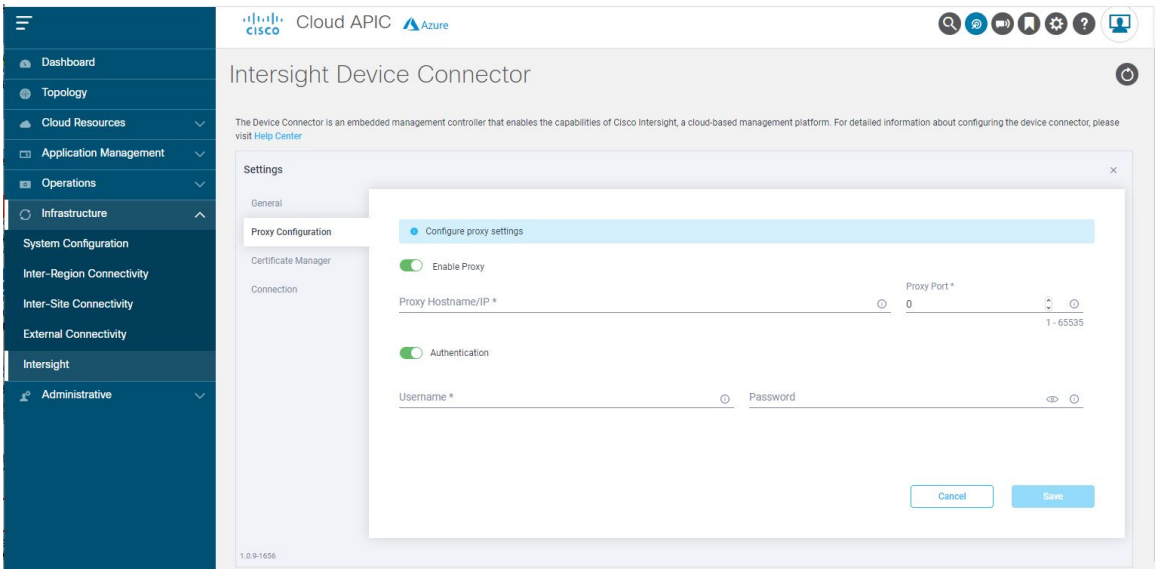


b) In the **Proxy Hostname/IP** field, enter a Proxy Hostname and IP Address.

c) In the **Proxy Port** field, enter a Proxy Port.

d) In the **Authentication** field, toggle the **Authentication** option to ON to configure the proxy authentication settings.

The **Username** and **Password** fields appear.



e) Enter a proxy username and password for authentication.

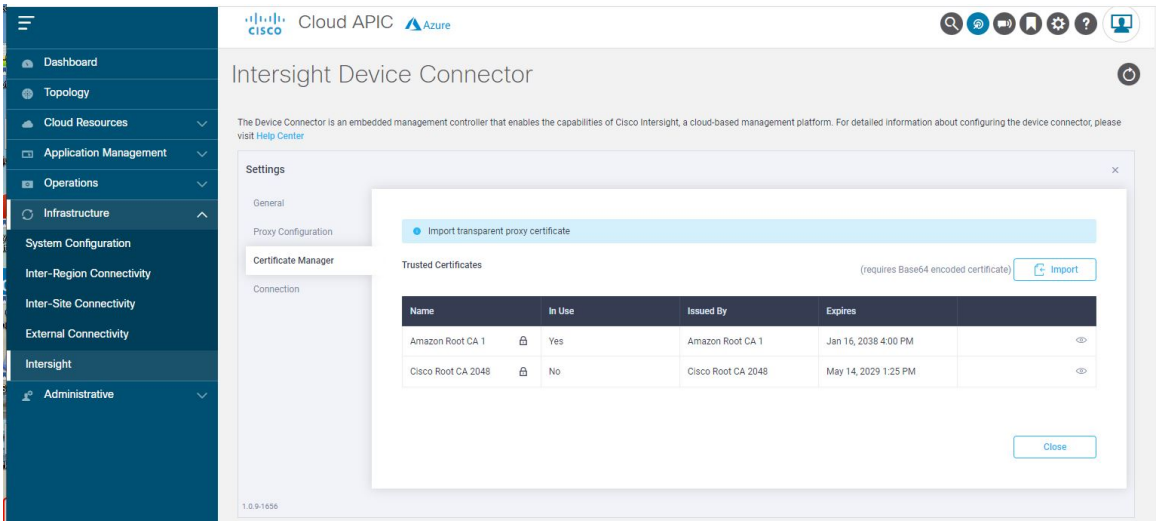
Step 9 When you have completed the configurations in the **Proxy Configuration** page, click **Save**.

The **Intersight Device Connector** overview pages appears again.

If you want to make manage certificates with the Device Connector, go to the next step.

Step 10 If you want to manage certificates with the Device Connector, click **Settings**, then click **Certificate Manager**.

The **Certificate Manager** page appears.



Step 11 In the **Certificate Manager** page, configure the following settings.

By default, the device connector trusts only the built-in svc.ucs-connect.com certificate. If the device connector establishes a TLS connection and a server sends a certificate that does not match the built-in svc.ucs-connect.com certificate, the device connector terminates TLS connections because it cannot determine if the server is a trusted device or not.

Click **Import** to import a CA signed certificate. The imported certificates must be in the *.pem (base64 encoded) format. After a certificate is successfully imported, it is listed in the list of Trusted Certificates and if the certificate is correct, it is shown in the In-Use column.

View these details for a list of certificates that are used to connect to svc.ucs-connect.com (intersight.com):

- **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.

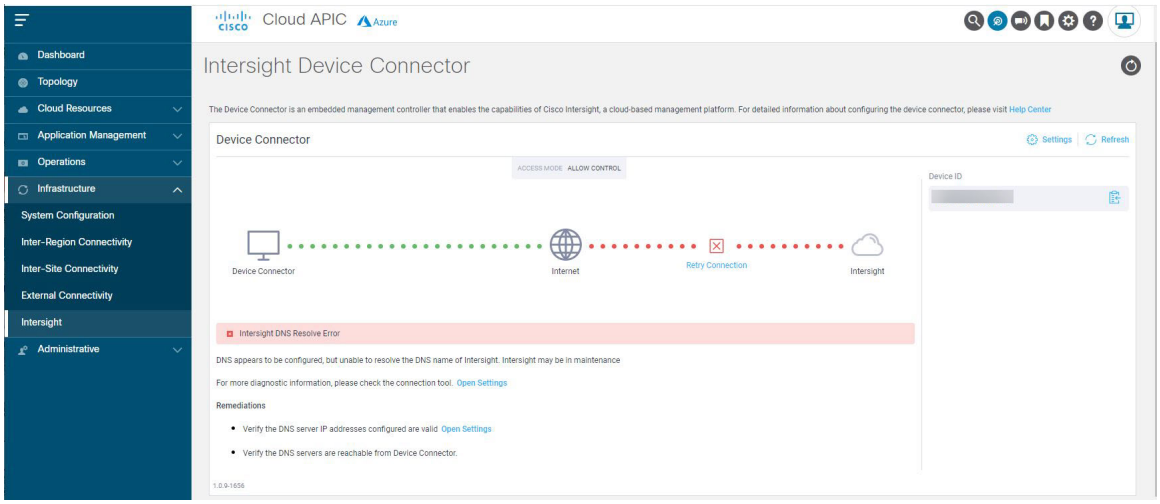
Delete a certificate from the list of Trusted certificates. However, you cannot delete bundled certificates (root+intermediate certificates) from the list. The lock icon represents the Bundled certificates.

Step 12 When you have completed the configurations in the **Certificate Manager** page, click **Close**.

The **Intersight Device Connector** overview pages appears again.

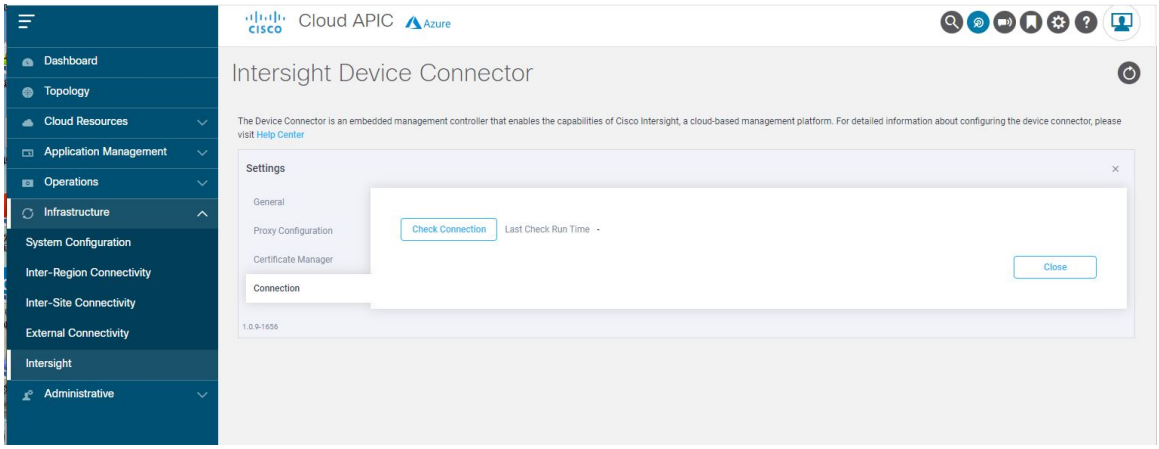
Step 13 Determine if you want to check the connection.

You might want to navigate to the **Connection** page to troubleshoot connection issues, such as if you see red dotted lines connecting **Internet** to **Intersight** in the **Device Connector** graphic, as shown in the following figure:

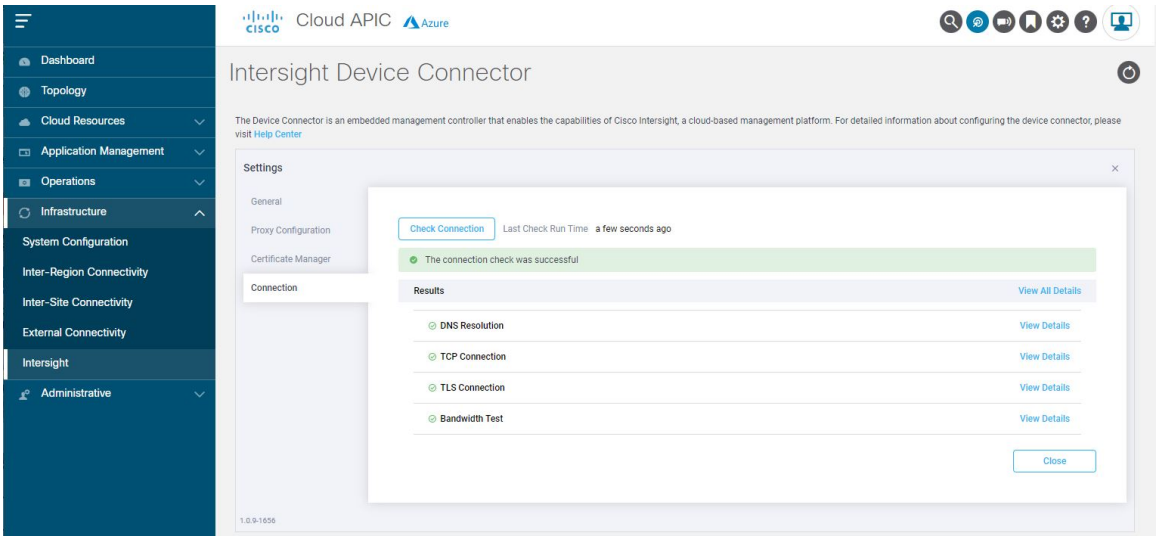


In that case, navigate to the **Connections** page by clicking on **Open Settings** in the **Device Connector** graphic, or by clicking **Settings**, then clicking **Connections**.

The **Connections** page appears.



Click **Check Connection** to check the connections, then use the information provided in the page to address any connection issue that you might have.



Click **Close** when you're finished with this page.

What to do next

Claim the device using the instructions provided in Claiming a Device Using the GUI, on page 9.

Claiming a Device Using the GUI

Before you begin

Configure the Cisco Intersight Device Connector information from the Cisco Cloud APIC site using the instructions provided in Configuring the Intersight Device Connector, on page 3.

Procedure

Step 1 Navigate to the Cisco Intersight cloud site:

https://www.intersight.com

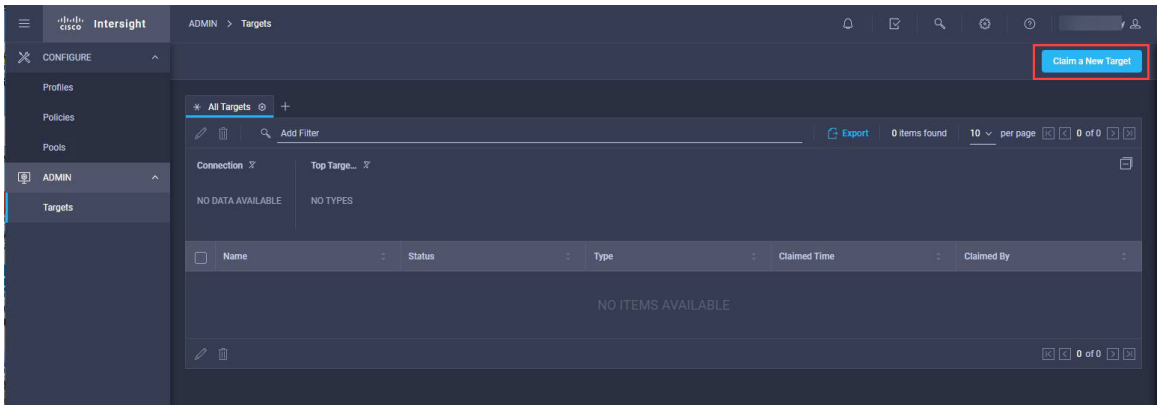
Step 2 Enter the necessary information to log into the Cisco Intersight cloud site.

Step 3 Select the appropriate account and role, if necessary.

The **Profiles** page appears.

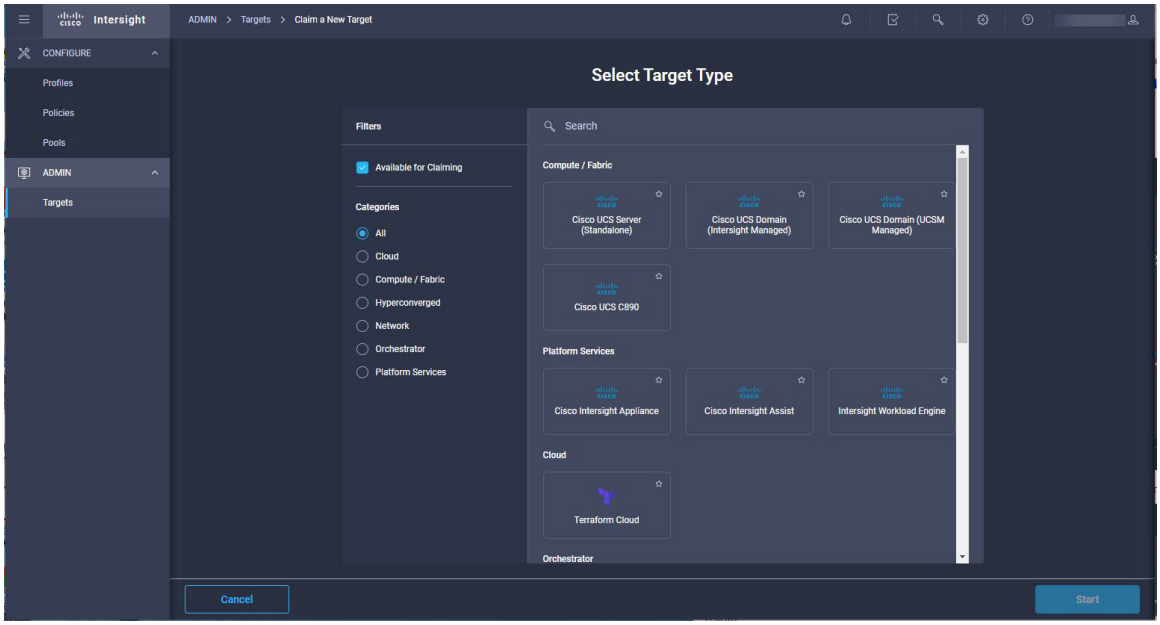
Step 4 Navigate to **Admin** > **Targets**.

The **Targets** page appears.

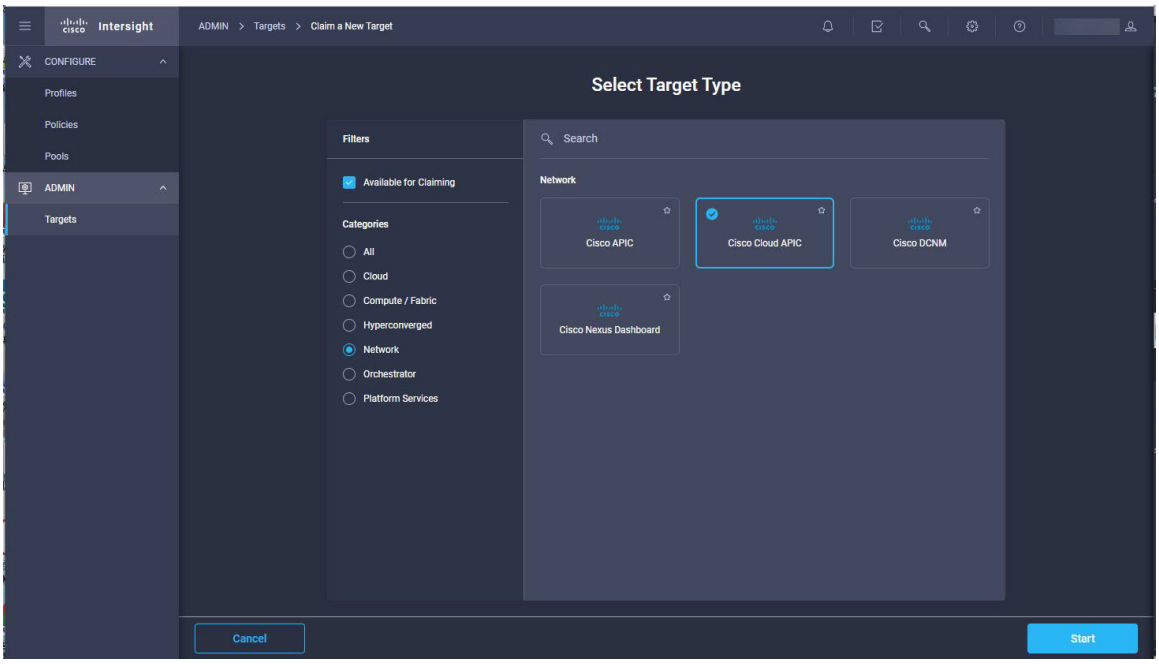


Step 5 Click **Claim a New Target**.

The **Select Target Type** page appears.

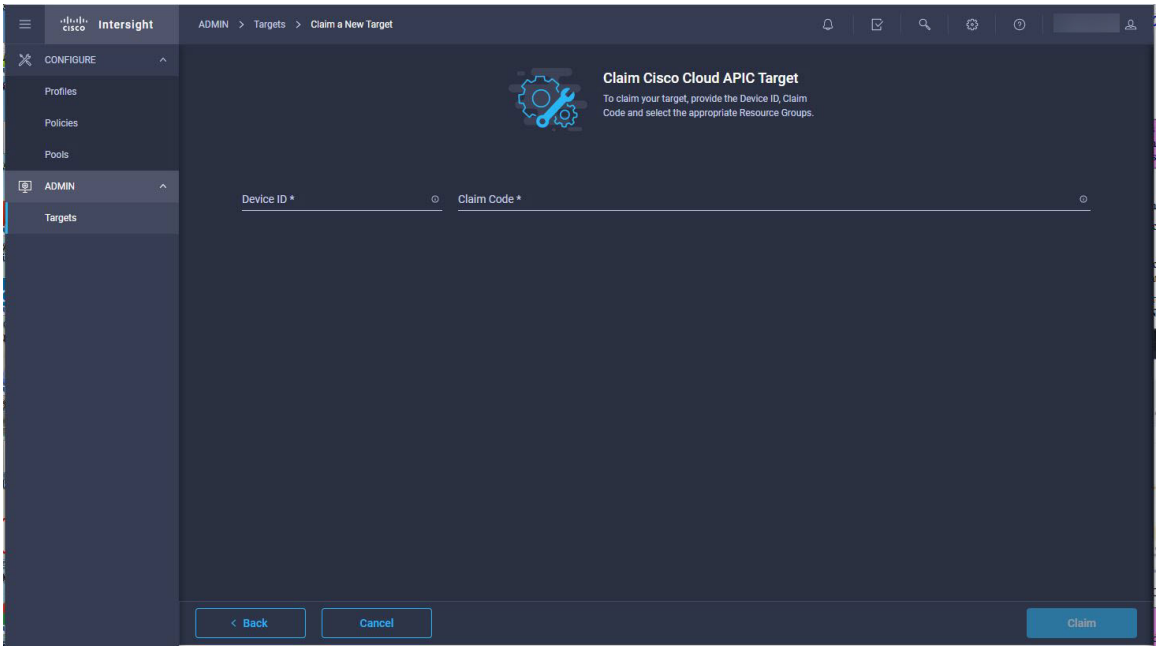


Step 6 Under the **Categories** area in the left side, click **Network** to filter the target types.



Step 7 Click the **Cisco Cloud APIC** button, then click **Start**.

The **Claim Cisco Cloud APIC Target** page appears.

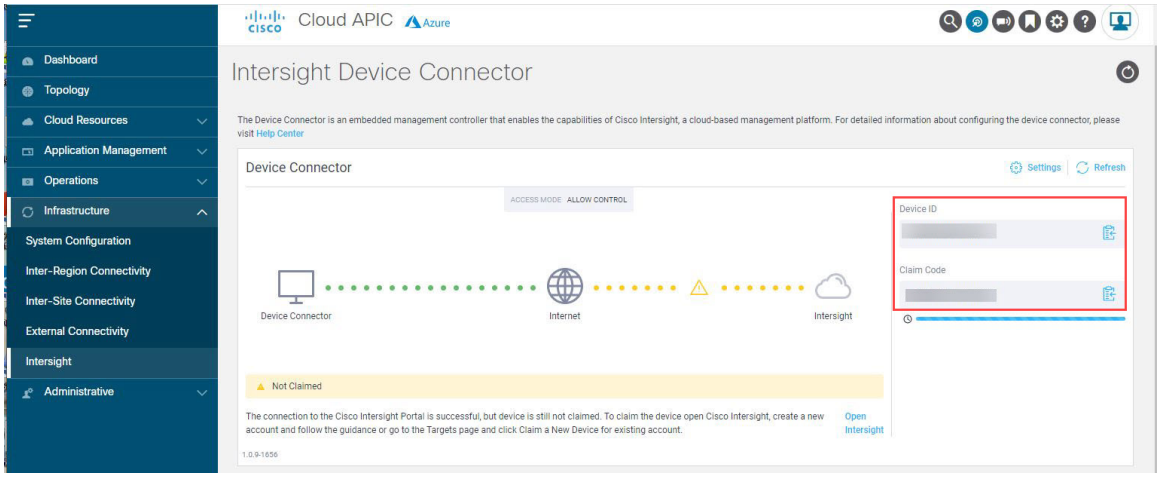


Step 8 In the Cisco Cloud APIC site, navigate back to **Infrastructure** > **Intersight**.

The **Intersight Device Connector** overview page appears.

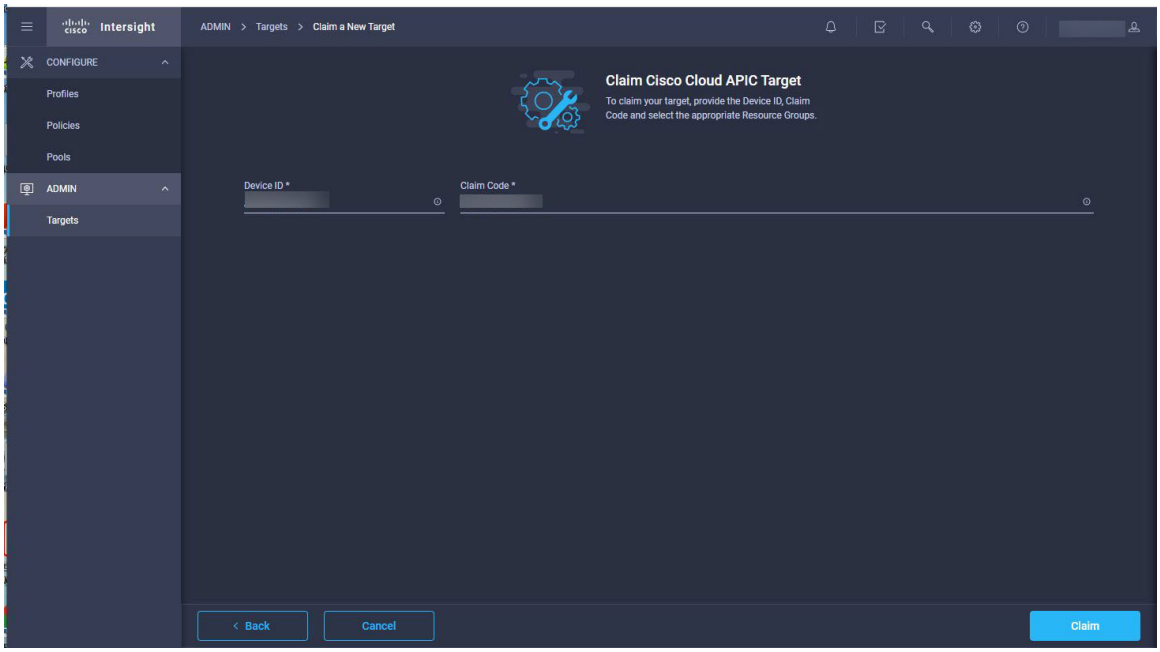
Step 9 From the Cisco Cloud APIC site, copy the values in the **Device ID** and **Claim Code** fields, then paste them into the proper fields in the **Claim a New Device** page in the Cisco Intersight cloud site.

For each area in the Cisco Cloud APIC site, click the clipboard next to that field to copy the information into the clipboard, then paste it into the proper fields in the **Claim a New Device** page in the Cisco Intersight cloud site.

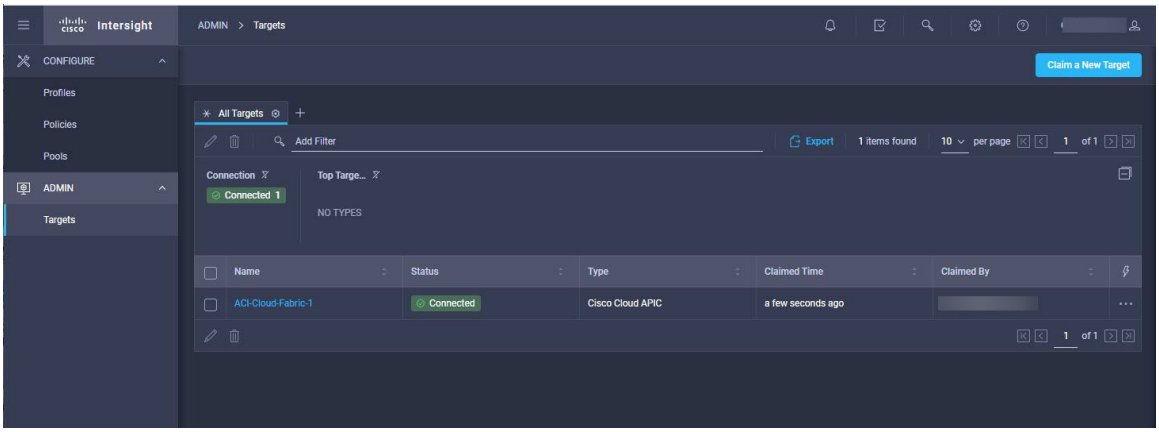


Step 10 In the Cisco Intersight cloud site, claim the Cisco Cloud APIC target.

After you paste the Cisco Cloud APIC values in the **Device ID** and **Claim Code** fields in the Cisco Intersight cloud site, click **Claim** in the bottom right area of the page.

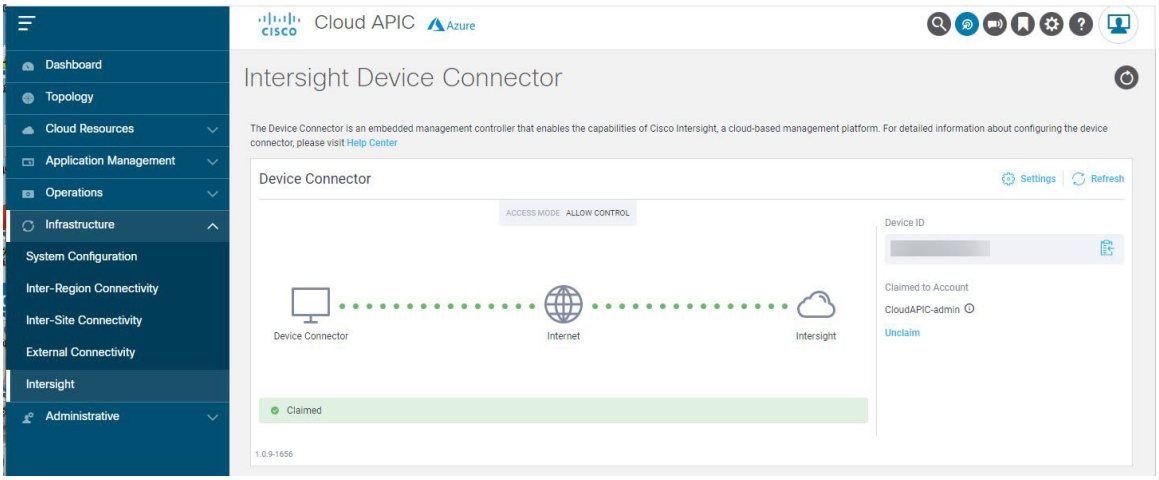


The **Targets** page appears again, with the Cisco Cloud APIC shown in the table and **Connected** in the Status column.



Step 11 Go back to the **Intersight Device Connector** page in the Cisco Cloud APIC GUI and verify that Cisco Intersight successfully claimed the system.

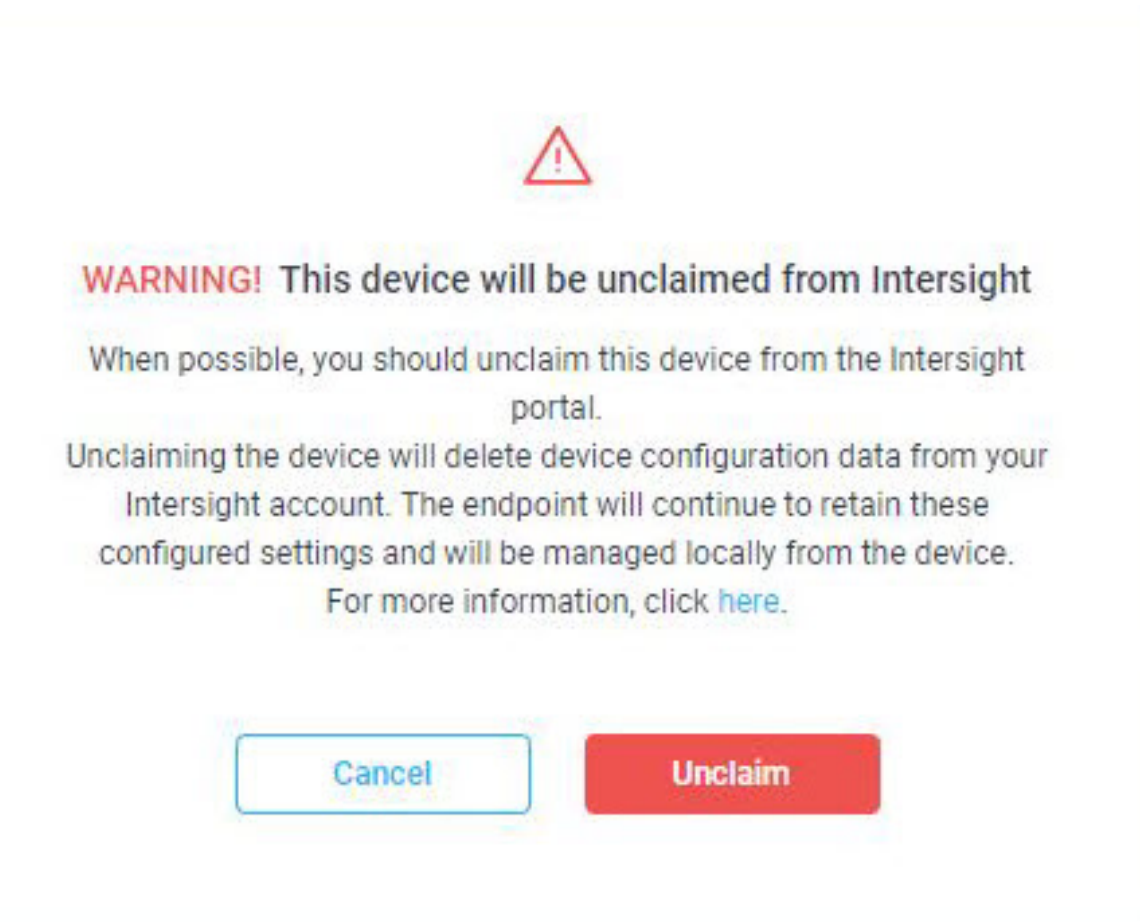
You will see green-dotted lines connecting **Internet** to **Intersight** in the **Device Connector** graphic, and the text **Claimed** underneath the graphic.



Note You may have to click **Refresh** in the **Intersight Device Connector** page in the Cloud APIC GUI to update the information in the page to the current state.

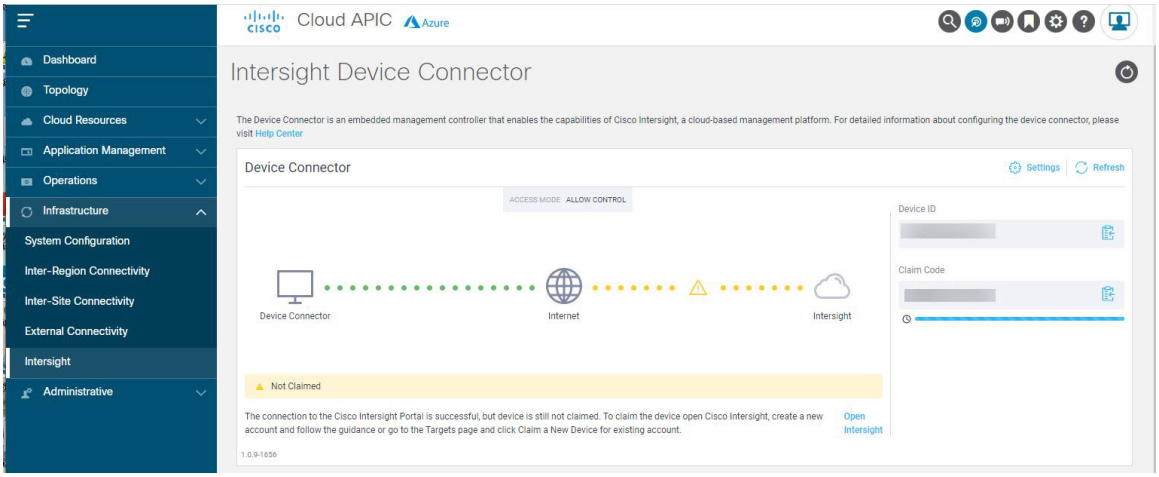
If you decide to unclaim this device for some reason, locate the **Unclaim** link in the **Intersight Device Connector** page in the Cisco Cloud APIC GUI and click that link.

A popup page appears, asking you to confirm that you want to unclaim the device.

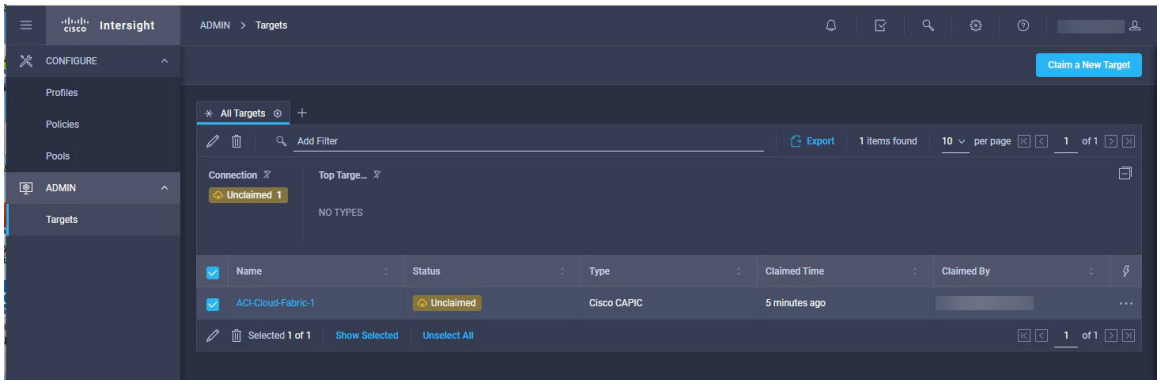


Click **Unclaim** again to confirm that you want to unclaim this device.

- In the **Intersight Device Connector** page in the Cisco Cloud APIC GUI, the status changes to **Not Claimed**.



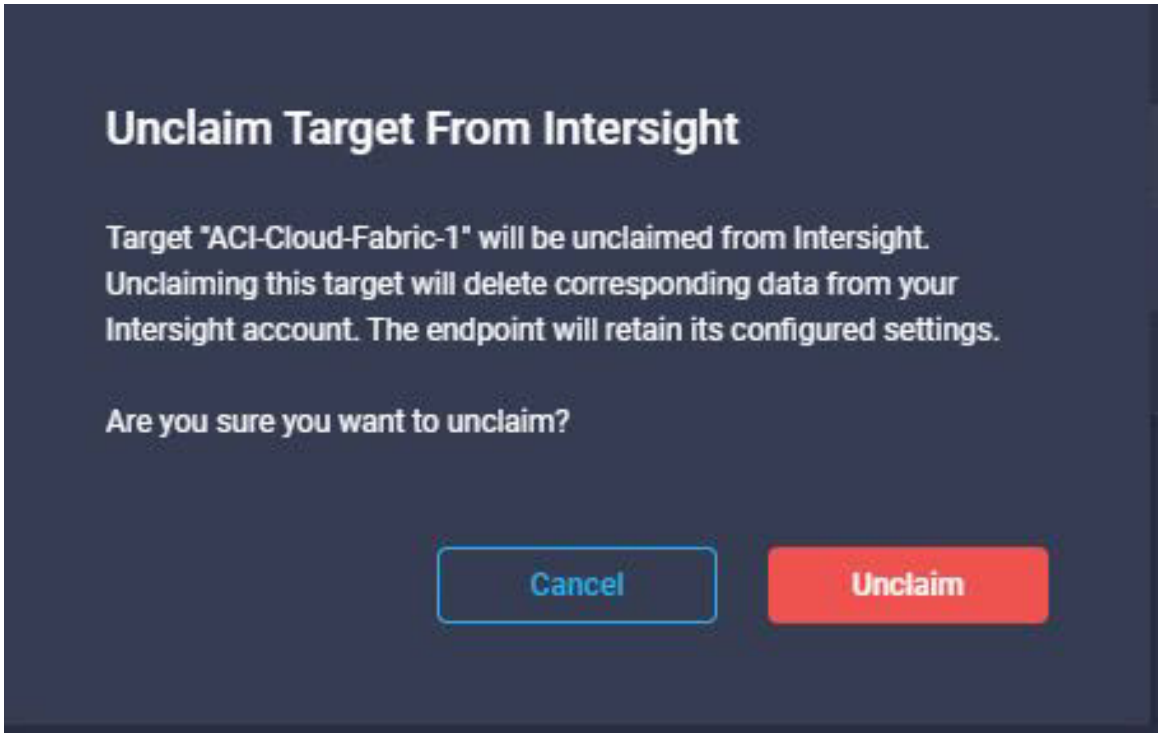
- In the **Targets** page in the Cisco Intersight cloud site, the status changes to **Unclaimed**.



You can then click the box next to the Cisco Cloud APIC in the **Targets** page in the Cisco Intersight cloud site and click the trashcan icon to delete that target, if necessary.

Note You can also unclaim the device and delete the target in a single step, without having to perform any actions in the Cisco Cloud APIC GUI, by clicking the box next to the Cisco Cloud APIC in the **Targets** page in the Cisco Intersight cloud site and then clicking the trashcan icon.

A popup page appears, asking you to confirm that you want to unclaim the device.



Click **Unclaim** again to confirm that you want to unclaim this device.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

Asia Pacific Headquarters
CiscoSystems(USA)Pte.Ltd.
Singapore

Europe Headquarters
CiscoSystemsInternationalBV
Amsterdam,TheNetherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.