Using Cisco Network Insights Base

This chapter contains the following sections:

About Cisco Network Insights Base Application

The Cisco Network Insights Base (Cisco NI Base) application provides TAC Assist functionalities which are useful when working with Cisco TAC. It provides a way for Cisco Customers to collect tech support across multiple devices and upload those tech supports to Cisco Cloud. These tech support are accessible to our TAC teams when helping customers through a resolution of a Service Request. Additionally, it enables capability for our TAC teams to collect tech support on demand for a particular device.

The Cisco NI Base app consists of the following components:

- Devices
- TAC Assist
    - Log Collection
    - Technical Support to Cloud
    - Enhanced TAC Assist

The Cisco NI Base app collects the CPU, device name, device pid, serial number, version, memory, device type, and disk usage information for the nodes in the fabric.

Cisco NI Base Initial Setup

This section contains the steps required to set up the Cisco NI Base app in the Cisco APIC. This set up is required for the Cisco NI Base app to show important information and gather relevant data.

Step 1 Once Cisco NI Base app is installed and after your first log in, a welcome dialog appears. Click **Begin Setup**.

A **Setup** dialog appears.

Step 2 In **Data Collection Setup**, click **Configure**.

The **Data Collection Setup** dialog appears. In the **Fabrics** list are pods that were discovered during the Cisco NI Base application installation.

Step 3 Check only the pods you want visible to the Cisco NI Base application.

Step 4 Click **Ok**.

The **Setup** dialog appears with the selected fabrics appearing in **Data Collection Setup**. You can edit the selected fabric(s) by clicking **Edit configuration**. You can return to the setup utility anytime by clicking the settings icon ⚙ and choose **Rerun Setup**.

Cisco NI Base Settings

Settings

Displayed across the top of the work pane is a group of icons and a list menu comprising the Cisco NI Base app settings. The following table describes each:

Property	Description
Fabric	Choose a fabric containing the pods you want visible to the Cisco NI Base application.
☁	**Device Connector Status**: Identifies the current connection status of the Cisco NI Base application to the Cisco Intersight cloud and the device connector claim condition. Possible connection statuses are: • **Not Connected**: The Cisco NI Base application is not connected to the Cisco Intersight cloud. • **Connected / Not Claimed**: The Cisco NI Base application is connected to the Cisco Intersight cloud but the device connector has not been claimed by the customer. • **Connected / Claimed**: The Cisco NI Base application is connected to the Cisco Intersight cloud and the device connector has been claimed by the customer. For more information, see Configuring the Intersight Device Connector, on page 3.

Property	Description
⚙	Clicking on this icon invokes a list menu allowing you to make changes to the following: • **About Network Insights**—Displays an information dialog identifying the version number of the Cisco NI Base application. Click **Update to Latest** to fetch the latest published version. This requires that the using of the Cisco Intersight Device Connecter is connected and claimed. See Configuring the Intersight Device Connector, on page 3 for details. • **Rerun Setup**—Allows you to edit the Data Collection Setup by adding or removing fabrics.
?	Displays the online help for Cisco Network Insights Base application on Cisco APIC.

Setting Up the Device Connector

This secion describes setting up the device connector for Cisco NI Base on Cisco APIC.

About Device Connector

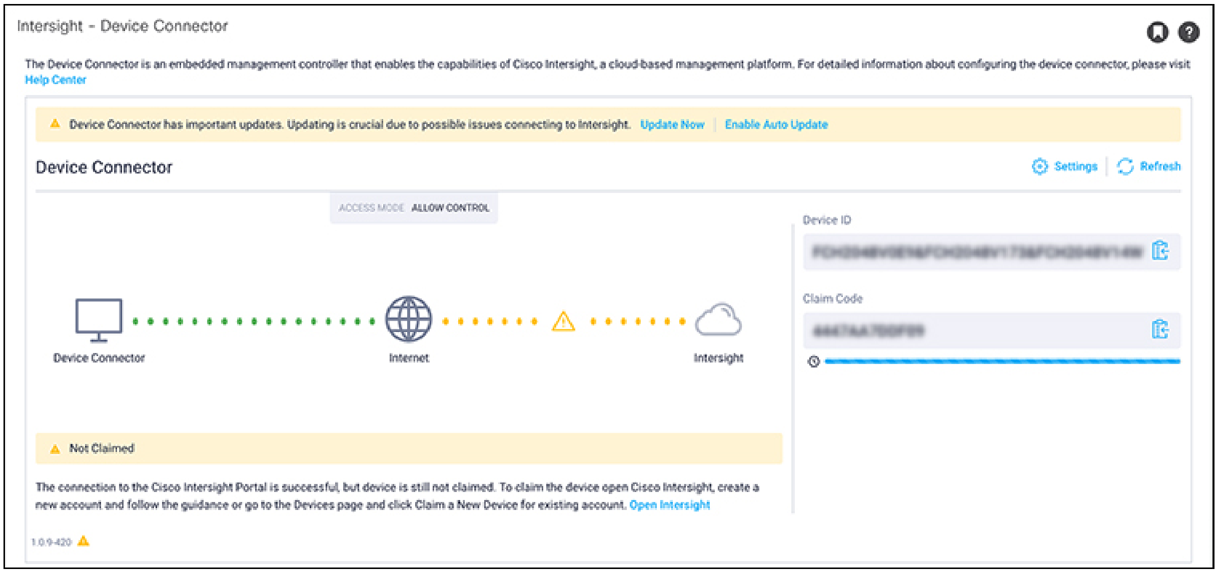
Devices are connected to the Intersight portal through a Device Connector that is embedded in the management controller of each system. Device Connector provides a secure way for the connected devices to send information and receive control instructions from the Cisco Intersight portal, using a secure 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 Intersight service when you connect to Intersight. For more information on the **Auto Update** option, see Configuring the Intersight Device Connector, on page 3.

Configuring the Intersight Device Connector

Step 1 In the Cisco APIC GUI, click **System** > **System Settings** > **Intersight**.

The Device Connector work pane appears:



Intersight - Device Connector

The Device Connector is an embedded management controller that enables the capabilities of Cisco Intersight, a cloud-based management platform. For detailed information about configuring the device connector, please visit Help Center

⚠ Device Connector has important updates. Updating is crucial due to possible issues connecting to Intersight. Update Now | Enable Auto Update

Device Connector

Device ID: [redacted]

Claim Code: [redacted]

⚠ Not Claimed

The connection to the Cisco Intersight Portal is successful, but device is still not claimed. To claim the device open Cisco Intersight, create a new account and follow the guidance or go to the Devices page and click Claim a New Device for existing account. Open Intersight

1.0.9-420 ⚠

307486

- 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, that means that you configured the proxy incorrectly in Step 6.

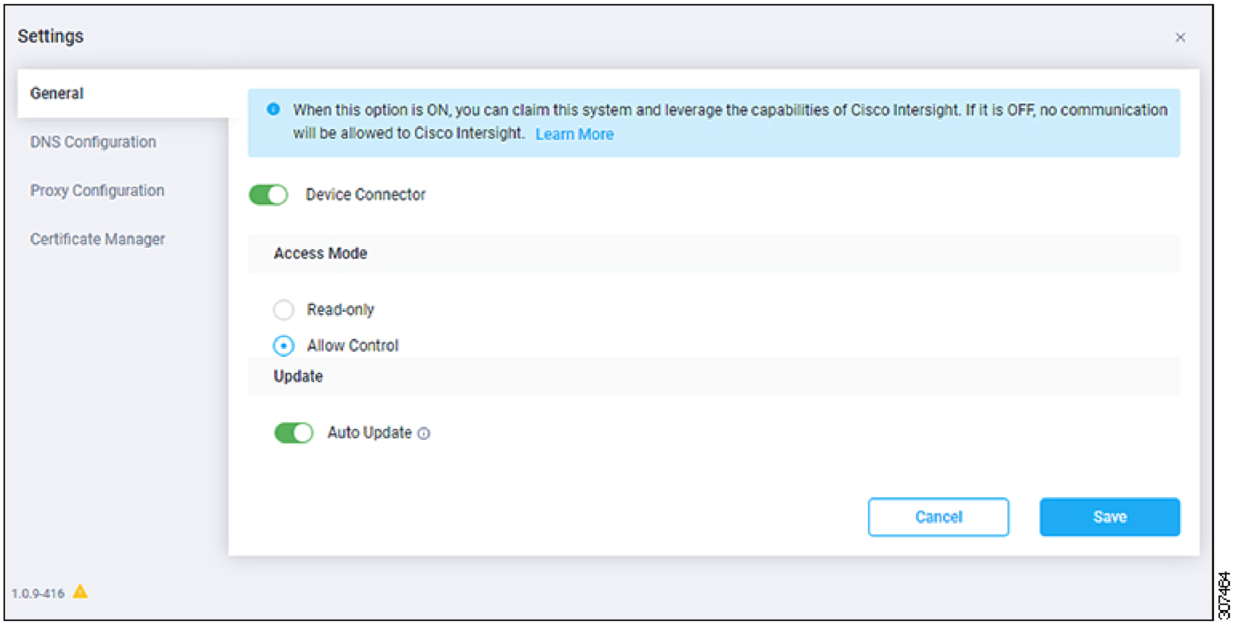
Step 2 Determine if you would like to update the software at this time, if there is a new Device Connector software version available.

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 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 towards 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 Step 4c 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.



Settings

General

DNS Configuration

Proxy Configuration

Certificate Manager

When this option is ON, you can claim this system and leverage the capabilities of Cisco Intersight. If it is OFF, no communication will be allowed to Cisco Intersight. Learn More

Device Connector: ON

Access Mode

○ Read-only

● Allow Control

Update

Auto Update: ON

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) enables you to claim the device and leverage the capabilities of Intersight. If it is turned OFF, 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 **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. This function is not used for changes from Cisco Cloud to the customer network.

- 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.

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.

Note If the **Auto Update** option is turned OFF, that may periodically cause the Device Connector to be out-of-date, which could affect the ability of the Device Connector to connect to Intersight.

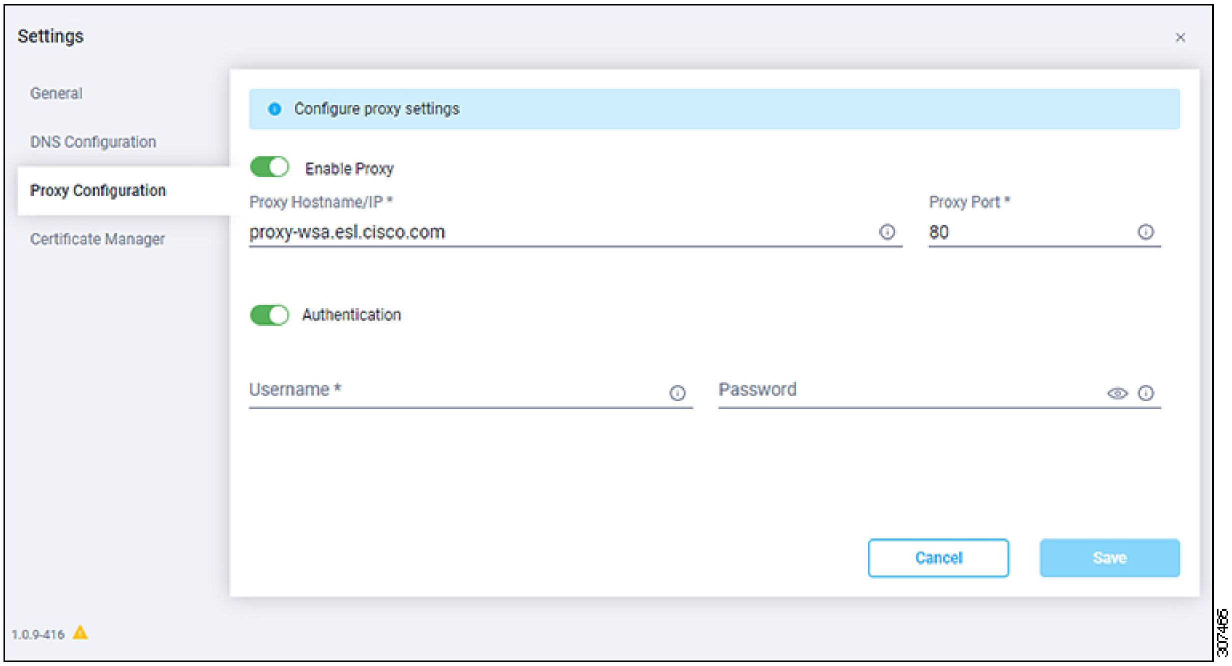
Step 5 When you have completed the configurations in the **General** page, click **Save**.

The **Intersight - Device Connector** overview pages appears again. At this point, you can make or verify several configure settings for the Intersight Device Connnector:

- If you want to configure the proxy that the Device Connector will use to communicate with the Intersight cloud, go to Step 6.
- If you want to manage certificates with the Device Connector, go to Step 9.

Step 6 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.



Enable Proxy: ON

Proxy Hostname/IP *: proxy-wsa.esl.cisco.com

Proxy Port *: 80

Authentication: ON

Username *

Password

Step 7 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.

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, then enter a Proxy Username and Password for authentication.

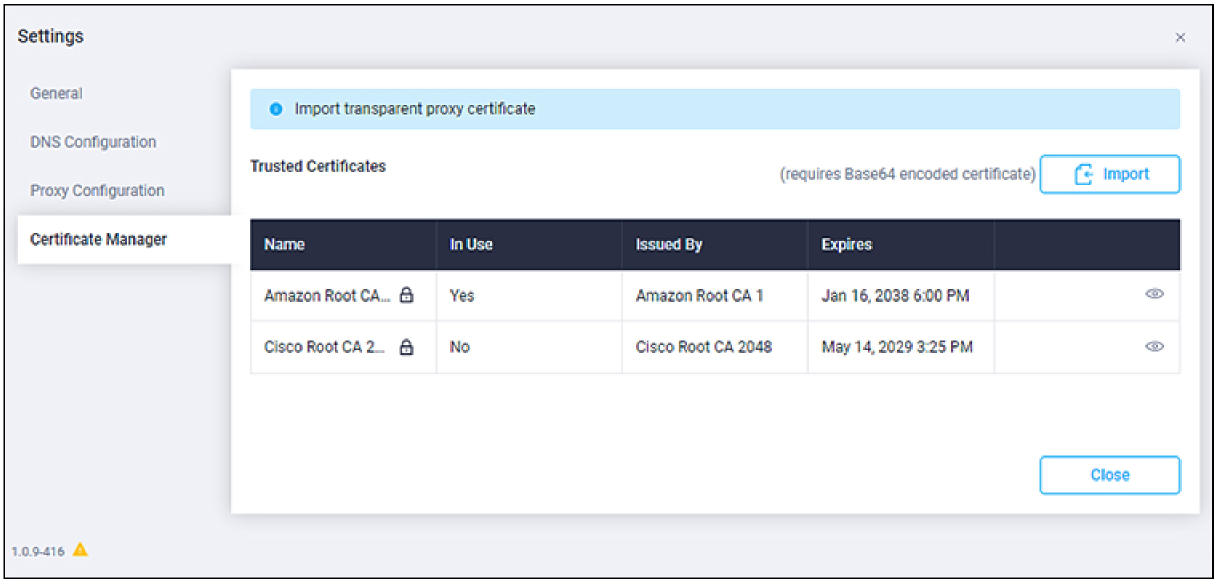
Step 8 When you have completed the configurations in the **Proxy Configuration** page, click **Save**.

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

The **Certificate Manager** page appears.



Trusted Certificates

(requires Base64 encoded certificate)

Name	In Use	Issued By	Expires
Amazon Root CA... 🔒	Yes	Amazon Root CA 1	Jan 16, 2038 6:00 PM
Cisco Root CA 2... 🔒	No	Cisco Root CA 2048	May 14, 2029 3:25 PM

Step 10 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 11 When you have completed the configurations in the **Certificate Manager** page, click **Close**.

You can claim the device using the instructions provided in Claiming a Device, on page 8.

Claiming a Device

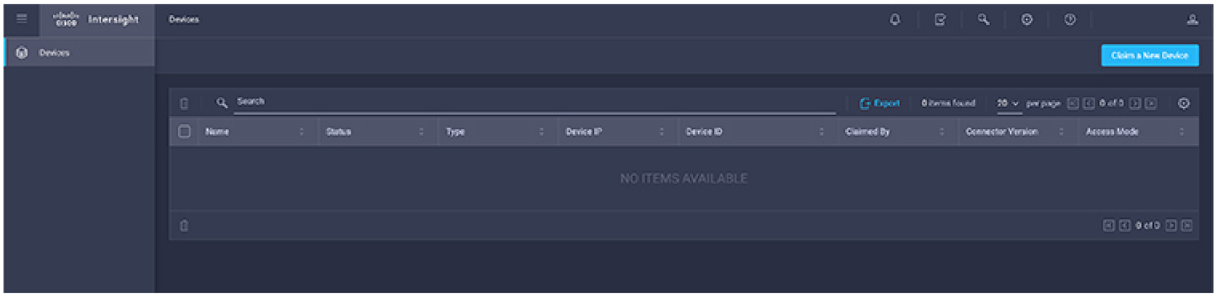
Before you begin

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

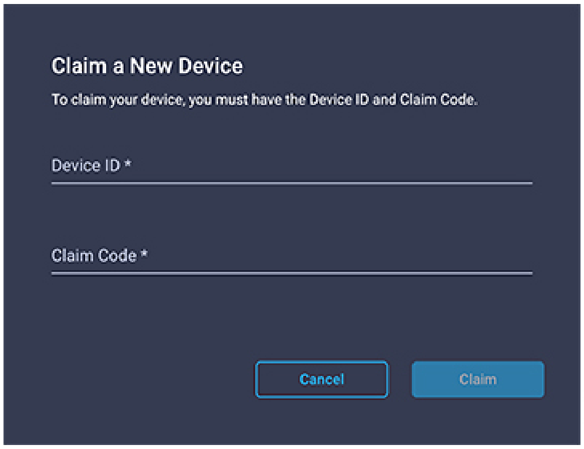
Step 1 Log into the Cisco Intersight cloud site:

https://www.intersight.com

Step 2 In the Cisco Intersight cloud site, under the **Devices** tab, click **Claim a New Device**.



The **Claim a New Device** page appears.



Claim a New Device

To claim your device, you must have the Device ID and Claim Code.

Device ID *

Claim Code *

Step 3 Go back to the Cisco APIC site and navigate back to the **Intersight - Device Connector** page.

a) On the menu bar, choose **System** > **System Settings**.

b) In the **Navigation** pane, click **Intersight**.

Step 4 Copy the **Device ID** and **Claim Code** from the Cisco APIC site and paste them into the proper fields in the **Claim a New Device** page in the Intersight cloud site.

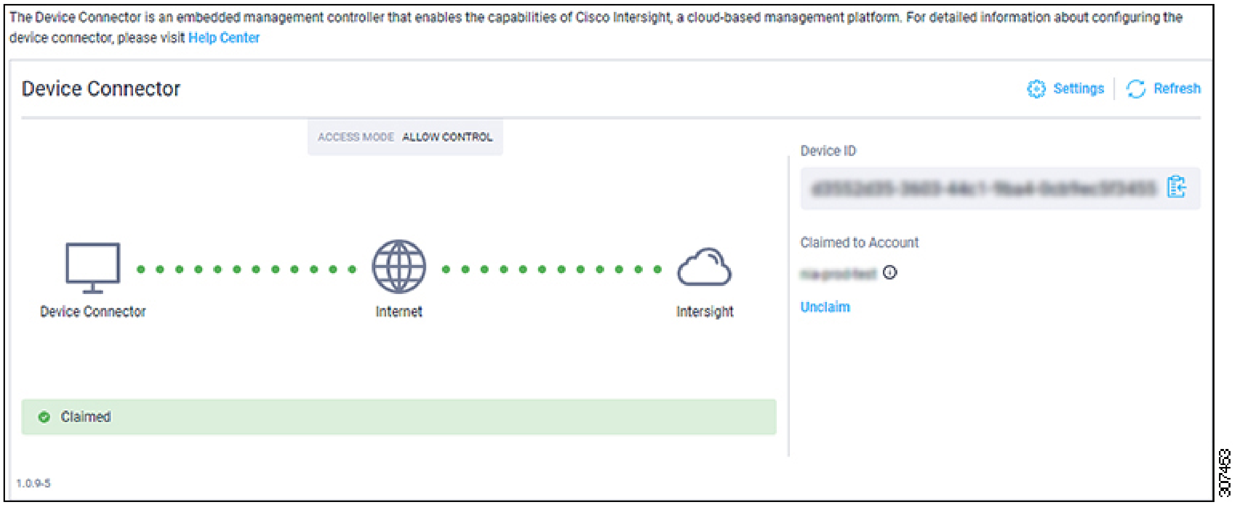
Click on the clipboard next to the fields in the Cisco APIC site to copy the field information into the clipboard.

Step 5 In the **Claim a New Device** page in the Intersight cloud site, click **Claim**.

You should see the message "Your device has been successfully claimed" in the **Claim a New Device** page. Also, in the main page, you should see your Cisco APIC system, with Connected shown in the Status column.

Step 6 Go back to the **Intersight - Device Connector** page in the Cisco APIC GUI and verify that the system was claimed successfully.

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



The Device Connector is an embedded management controller that enables the capabilities of Cisco Intersight, a cloud-based management platform. For detailed information about configuring the device connector, please visit Help Center

Device Connector

ACCESS MODE ALLOW CONTROL

Device ID

[redacted]

Claimed to Account

[redacted]

Claimed

1.0.9-5

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

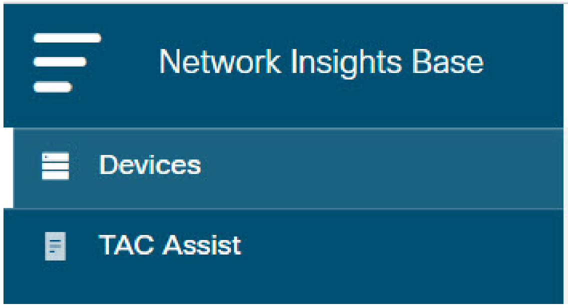
If you decide to unclaim this device for some reason, locate the **Unclaim** link in the **Intersight - Device Connector** page and click that link.

Navigating Cisco NI Base

The Cisco NI Base application window is divided into two parts: the Navigation pane and the Work pane.

Navigation Pane

The Cisco NI Base app navigation pane divides the collected data into the following categories:



1 Devices: Sorts devices by device name, serial number, IP address, version, and platform.

2 TAC Assist: Collects logs for specified devices that can be attached to service requests using the Cisco Intersight Cloud.

Devices

The Devices page displays the devices by device name, serial number, IP address, version, and platform.

TAC Assist

The TAC Assist work pane lets you collect logs for specified devices that can be attached to service requests using the Cisco Intersight Cloud. It lets you check the device(s) for which you can collect logs to assist TAC.

The **Log Collection** section displays the new job triggered for TAC Assist. The **Job Details** page lists the TAC Assist logs.

All information about TAC Assist job including, status, devices, fabric, start time, job id, device name, log location, and cloud upload appear in the work pane.

Using the Cisco Network Insights Base Application

Main Dashboard

The Cisco NI Base application main dashboard provides immediate access to a high-level view of Devices and access to TAC Assist logs in your network.

Property	Description
Devices	Displays devices by device name, serial number, IP address, version, and platform in your network.
TAC Assist	Displays the total number of TAC assist logs currently being collected or finished being collected.

Devices

The Devices dashboard displays devices by serial numbers, software versions, and hardware platforms. You can sort devices by device name, serial number, IP address, software version, and hardware platform.

TAC Assist

The TAC Assist dashboard allows you to collect logs for devices in your network. These logs can be attached to Service Requests (SRs) for further analysis.

1. Click **Begin** to initiate the log collection process.
2. To display specific devices in the list, use the filter utility:
    - Operators - display devices using an operator. Valid operators are:
        - = = - display devices with an exact match. This operator must be followed by text and/or symbols that are the exact software version, product ID, device name, or assigned IP address of the device.

    - contains - display device names or platform identifiers containing entered text or symbols. This operator must be followed by text and/or symbols.

  - Version - display devices that are running a specific software version.
  - Platform - display devices that are a specific type defined by the platform ID.
  - Device Name - display devices that are specifically named.
  - Serial Number - display devices that are running a specific serial number.
  - IP Address - display devices that are assigned a specific IP address.

3. Place a check in the checkbox next to the device for which you want to collect logs. If you want to choose all of the devices in the list, place a check in the checkbox next to the **Device Name** column title.
4. Click **Collect Logs**.

   The **Collect Logs** dialog appears on the TAC Assist dashboard. Once the logs are collected, Cisco NI Base app lets you view the collected log details. The TAC Assist detailed page displays the location where the logs are collected and lets you upload to the Cisco Intersight Cloud.

The following table describes the status messages for TAC Assist.

Property	Description
Pending	Displays when connecting to Intersight Device Connector is pending.
Collection in Progress	Displays when collecting the logs locally to Intersight Device Connector is in progress.
Collection Complete	Displays when collecting the logs locally to Intersight Device Connector is complete.
Retry Upload	Displays when there is a failure to collect logs.
Upload Pending	Displays when uploading the logs from Intersight Device Connector to Cisco Intersight Cloud is pending.
Upload in Progress	Displays when uploading the logs from Intersight Device Connector to Cisco Intersight Cloud is in progress.
Complete	Displays when upload to Cisco Intersight Cloud is complete.

TAC Assist

This section contains the steps required for you to trigger a TAC Assist job to collect logs for specified devices and upload the logs to cloud. The collected logs for specified devices then can be attached to the service requests (SRs).

Before you begin

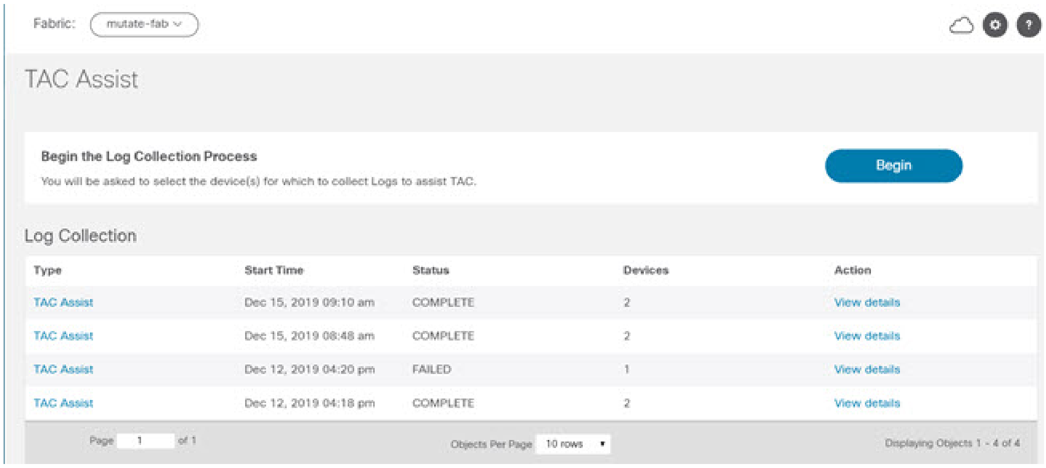
Before you upload the collected logs to cloud, make sure the fabric is conneced to Cisco Intersight cloud. See Configuring the Intersight Device Connector, on page 3 for details.

Step 1 Click **TAC Assist** from the Cisco APIC navigation pane.

Step 2 Click **Begin** to choose the fabric device(s).

Step 3 From the **Collect Logs** page check the device(s) for which to collect logs to assist TAC.

The **Log Collection** section displays the new job triggered for TAC Assist.



Fabric: mutate-fab

TAC Assist

Begin the Log Collection Process

You will be asked to select the device(s) for which to collect Logs to assist TAC.

Begin

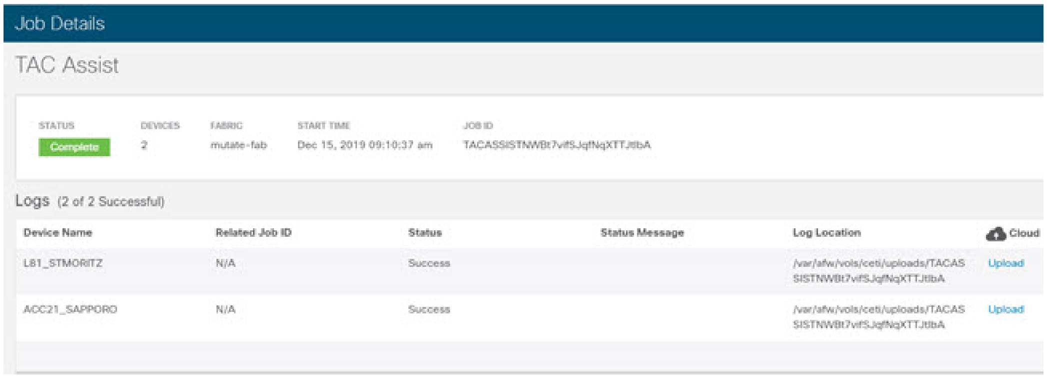
Log Collection

Type	Start Time	Status	Devices	Action
TAC Assist	Dec 15, 2019 09:10 am	COMPLETE	2	View details
TAC Assist	Dec 15, 2019 08:48 am	COMPLETE	2	View details
TAC Assist	Dec 12, 2019 04:20 pm	FAILED	1	View details
TAC Assist	Dec 12, 2019 04:18 pm	COMPLETE	2	View details

Page 1 of 1 Objects Per Page 10 rows Displaying Objects 1 - 4 of 4

Step 4 Click **View Details** from the list of logs to display the **Job Details** page.

All information about TAC Assist job including, status, devices, fabric, start time, job id, device name, log location, and cloud upload appear in the work pane.



Job Details

TAC Assist

STATUS	DEVICES	FABRIC	START TIME	JOB ID
Complete	2	mutate-fab	Dec 15, 2019 09:10:37 am	TACASSISTNWBt7vifSJqfNqXTTJtlbA

Logs (2 of 2 Successful)

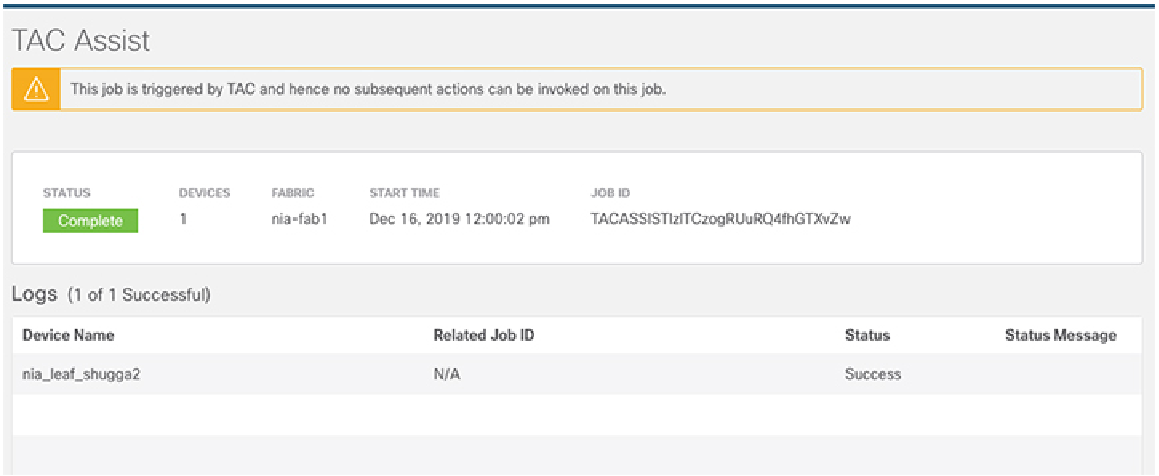
Device Name	Related Job ID	Status	Status Message	Log Location	Cloud
L81_STMORITZ	N/A	Success		/var/afw/vols/ceti/uploads/TACASSISTNWBt7vifSJqfNqXTTJtlbA	Upload
ACC21_SAPPORO	N/A	Success		/var/afw/vols/ceti/uploads/TACASSISTNWBt7vifSJqfNqXTTJtlbA	Upload

Step 5 Click **Upload** to upload the collected logs to Cisco Intersight cloud.

The **Cloud** status shows **Complete** when the upload of collected logs to Cisco Intersight cloud is complete.

Enhanced TAC Assist

The Enhanced TAC Assist feature triggered by TAC enables collection of logs for specified devices and uploads the logs to Cisco Intersight Cloud. Click **View Details** from list of logs to display the job details page.



TAC Assist

⚠ This job is triggered by TAC and hence no subsequent actions can be invoked on this job.

STATUS	DEVICES	FABRIC	START TIME	JOB ID
Complete	1	nia-fab1	Dec 16, 2019 12:00:02 pm	TACASSISTIzITCzogRUuRQ4fhGTXvZw

Logs (1 of 1 Successful)

Device Name	Related Job ID	Status	Status Message
nia_leaf_shugga2	N/A	Success	

The **View Details** page shows a message that the job is triggered by TAC and hence no subsequent actions can be invoked on this job.