



Cisco Network Insights Base  
Application for Cisco APIC User Guide,  
Release 2.0.24

# Table of Contents

The Cisco Network Insights Base Application for Cisco APIC User Guide .....	3
New and Changed Information .....	4
Cisco Network Insights Base Installation .....	5
About Cisco Network Insights Base on Cisco APIC .....	5
Cisco Network Insights Base Upgrade .....	6
Cisco NI-Base Pre-packaged App on Cisco APIC .....	6
Cisco Network Insights Base Setup and Settings .....	7
About Cisco Network Insights Base Application .....	7
Cisco NI Base Settings .....	7
Setting Up the Device Connector .....	9
About Device Connector .....	9
Configuring Smart Licensing .....	9
Configuring the Intersight Device Connector .....	9
Claiming a Device .....	14
Navigating Cisco Network Insights Base .....	17
Navigation Pane .....	17
Cisco Network Insights Base Dashboard .....	18
Cisco NI-Base Dashboard .....	18
TAC Assist - Upload to Cloud .....	19
Enhanced TAC Assist .....	20
Troubleshooting Cisco NI-Base .....	21
Recovering Deleted Pre-Packaged Cisco NI-Base App .....	21

First Published: 2020-06-30

Last Modified: 2021-03-05

**Americas Headquarters**

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA

<http://www.cisco.com>

Tel: 408 526-4000

800 553-NETS (6387)

Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <http://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2017-2021 Cisco Systems, Inc. All rights reserved.

# The Cisco Network Insights Base Application for Cisco APIC User Guide

# New and Changed Information

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

New Features and Changed Behavior in the Cisco Network Insights Base (Cisco NI-Base) app on Cisco APIC.

<b>Feature</b>	<b>Description</b>	<b>Release</b>	<b>Where Documented</b>
Cisco Network Insights Base, Release 2.0.24	The Cisco NI-Base app gets onboarded and configured automatically when device connector is configured.	2.0.24	<a href="#">About Cisco Network Insights Base on Cisco APIC</a>
Smart license configuration on Cisco APIC	After upgrading Cisco APIC to newer version the Device Connector inherits the smart license configuration that was configured in the older version of Cisco APIC.	2.0.24	<a href="#">Configuring Smart Licensing</a>

# Cisco Network Insights Base Installation

## About Cisco Network Insights Base on Cisco APIC

Cisco Network Insights Base (Cisco NI-Base) application consists of monitoring utilities that can be added to the Cisco Application Policy Infrastructure Controller (Cisco APIC). The Cisco NI-Base application uses the Device Connector available on the platform to communicate with the services running in Cisco Intersight Cloud.

Device Connector provides a secure way for the connected devices to send information and receive control instructions from the Cisco Intersight Cloud, using a secure Internet connection. See [About Device Connector](#).

Cisco Intersight is a management platform delivered as a service. Cisco APIC platform has a Device Connector that is packaged with the software that connects to Cisco Intersight Cloud. Device Connector is used to provide Cisco NI-Base Cloud connectivity feature sets.

Cisco NI-Base 2.0.24 app auto onboards the fabrics so that the application automatically enables telemetry, when Device Connector is configured. Cisco NI-Base functionality is supported by Device Connector plugins that enable communication with the Cisco Intersight Cloud. See [About Cisco Network Insights Base Application](#) for specific telemetry details.

Starting with Cisco APIC Release 4.2(4n), Cisco NI-Base app queries for smart license information on Cisco APIC. If the Proxy details are configured, then Device Connector inherits this configuration and attempts to connect with Cisco Intersight Cloud. If the information is modified in smart license configuration or removed, Device Connector is not updated. However, Cisco NI-Base app UI alerts you that the Device Connector is disconnected and allows you to update the smart license. See [Configuring Smart Licensing](#) for details.

For a more detailed overview on Cisco Licensing, go to [cisco.com/go/licensingguide](https://cisco.com/go/licensingguide).

# Cisco Network Insights Base Upgrade

## Cisco NI-Base Pre-packaged App on Cisco APIC

App Version	1.0.1	2.0.1	2.0.22	2.0.24
Cisco APIC Version	3.2(9)	4.2(1), 4.2(2), 4.2(3)	4.2(4), 5.0(1k)	4.2(4o)
Upgrade Cisco APIC	Yes <ul style="list-style-type: none"><li>• 3.2(9)to 4.2(4o)</li><li>• 3.2(9)to 5.0(1k)</li></ul>	Yes	Yes	Yes
Upgrade Cisco NI-Base App	Yes	Yes	Yes	N/A

### Upgrading Cisco NI-Base Application on Cisco APIC

Cisco APIC Release 4.2(4o) packages Cisco NI-Base 2.0.24 app. Only one instance of Cisco NI-Base app is supported on Cisco APIC.

When Device Connector is connected to the Cisco Intersight Cloud, on upgrading Cisco APIC to the latest release or on installing Cisco APIC, you are prompted to configure the Device Connector. Until you configure the Device Connector there is an alert present on the bell icon.

After upgrading Cisco APIC to newer version the Device Connector inherits the smart license configuration that was configured in the older version of Cisco APIC.

To upgrade Cisco NI-Base 1.0.1 or 2.0.1 pre-packaged app running on Cisco APIC, you will see an option in the application tab to upgrade. The arrow indicates that you have an explicit action to upgrade the app. Cisco APIC can be running while you upgrade Cisco NI-Base. The older version of Cisco NI-Base app shuts down and newer version is enabled.

When you upgrade Cisco APIC, Release 3.2(9) with Cisco NI-Base 1.0.1 app, to either Cisco APIC, Release 4.2(4o) or 5.0(1k) the respective app packaged with Cisco NI-Base 2.0.24 or 2.0.22 app gets enabled.

Pre-package remove-all policy does not remove a pre-packaged Cisco NI-Base app if the Cisco NI-Base app bundled in Cisco APIC release is older than the Cisco NI-Base app version already installed on your setup.

Cisco APIC release 4.2(4o) contains Cisco NI-Base 2.0.24 app, and Cisco APIC release 5.0(1k) contains Cisco NI-Base 2.0.22 app.

If you upgrade from Cisco APIC release 4.2(4o) to Cisco APIC release 5.0(1k), remove-all policy does not remove the Cisco NI-Base app.



# Cisco Network Insights Base Setup and Settings

## About Cisco Network Insights Base Application



The Cisco Network Insights Base application provides TAC Assist functionalities which are useful when working with Cisco TAC.

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 telemetry data. See [Table 2](#) and [Table 3](#) for telemetry data collected.

The Cisco NI-Base app provides a way for Cisco Customers to collect technical support across multiple devices and upload those technical supports to Cisco Intersight Cloud. These technical support are accessible to Cisco TAC teams when helping customers through a resolution of a Service Request. Additionally, it enables capability for Cisco TAC teams to collect technical support on demand for a particular device.

## Cisco NI Base 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
<b>Fabric</b>	Choose a fabric containing the pods you want visible to the Cisco NI-Base application.

Property	Description
	<p><b>Device Connector Status:</b> 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:</p> <ul style="list-style-type: none"> <li>• <b>Not Connected:</b> The Cisco NI-Base application is not connected to the Cisco Intersight Cloud.</li> <li>• <b>Connected / Not Claimed:</b> The Cisco NI-Base application is connected to the Cisco Intersight Cloud but the device connector has not been claimed by the customer. Cisco NI-Base app collects telemetry data.</li> <li>• <b>Connected / Claimed:</b> The Cisco NI-Base application is connected to the Cisco Intersight Cloud and the device connector has been claimed by the customer. Cisco NI-Base app uses TAC Assist functionality.</li> </ul> <p>For more information, see <a href="#">Configuring the Intersight Device Connector</a>.</p>
	<p>Clicking on this icon invokes a list menu allowing you to make changes to the following:</p> <ul style="list-style-type: none"> <li>• <b>About Network Insights</b>—Displays an information dialog identifying the version number of the Cisco NI-Base application.</li> <li>• <b>Rerun Setup</b>—Allows you to edit the Data Collection Setup by adding or removing fabrics.</li> </ul>
	<p>Displays the user guide for Cisco Network Insights Base application on Cisco APIC.</p>

# Setting Up the Device Connector

## 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.

All device connectors must properly resolve `svc.intersight.com` and allow outbound initiated HTTPS connections on port 443. To resolve `svc.intersight.com`, you must configure DNS on the managed devices. If a proxy is required for an HTTPS connection to `svc.intersight.com`, the proxy can be configured in the device connector user interface.

Note: Security appliances that terminate outbound device connector HTTPS connections are not supported at this time.

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](#).

## Configuring Smart Licensing

Configuring the smart licensing on Cisco APIC can be done using the following methods:

- Cisco Smart Software Manager (CSSM).
- Cisco Smart Licensing Satellite.
- Http Proxy.

When you configure Device Connector, Cisco NI-Base app adds the Proxy details for configuring the smart licensing.

Once the Proxy is enabled with the smart license configuration on Cisco APIC, the Device Connector inherits this configuration and attempts to connect with Cisco Intersight Cloud. If the information is modified in smart license configuration or removed, Device Connector is not updated. Additionally, if Device Connector is configured with a new value then it is honored.

Cisco NI-Base app starts collecting telemetry data from your network using the Proxy details while configuring Device Connector.

For a more detailed overview on Cisco Licensing, go to [cisco.com/go/licensingguide](https://cisco.com/go/licensingguide).

## Configuring the Intersight Device Connector

Cisco NI-Base application is connected to the Cisco Intersight Cloud portal through a Device

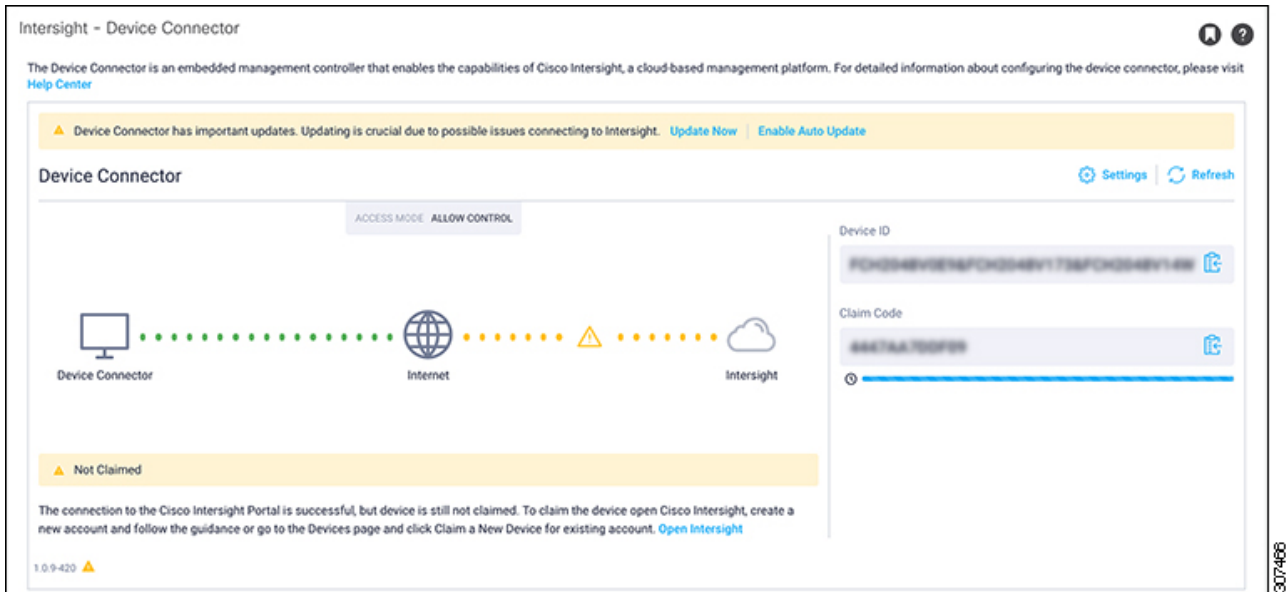
Connector which is embedded in the management controller of the Cisco APIC platform.

Cisco Intersight is a management platform delivered as a service. Cisco APIC platform has a Device Connector that is packaged with the software that connects to Cisco Intersight Cloud. Device Connector is used to provide Cisco NI-Base Cloud connectivity feature sets.

The Device Connector provides a secure way for connected Cisco APIC to send and receive information from the Cisco Intersight portal, using a secure Internet connection.

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

The Device Connector work pane appears:



- 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.



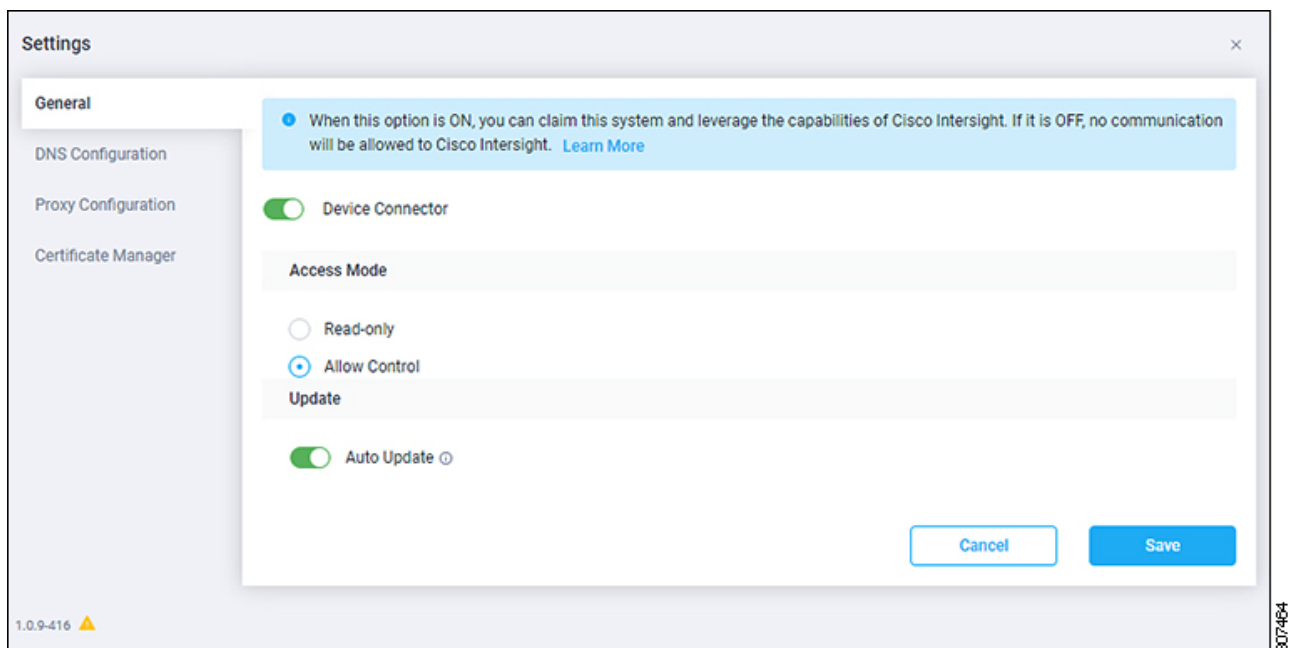
If you see red dotted lines connecting **Internet** to **Intersight** in the **Device Connector** graphic, that means that you configured the proxy incorrectly in Step 6.

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.
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.



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 configuration changes are done by Cisco

Intersight on Cisco APIC. 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.



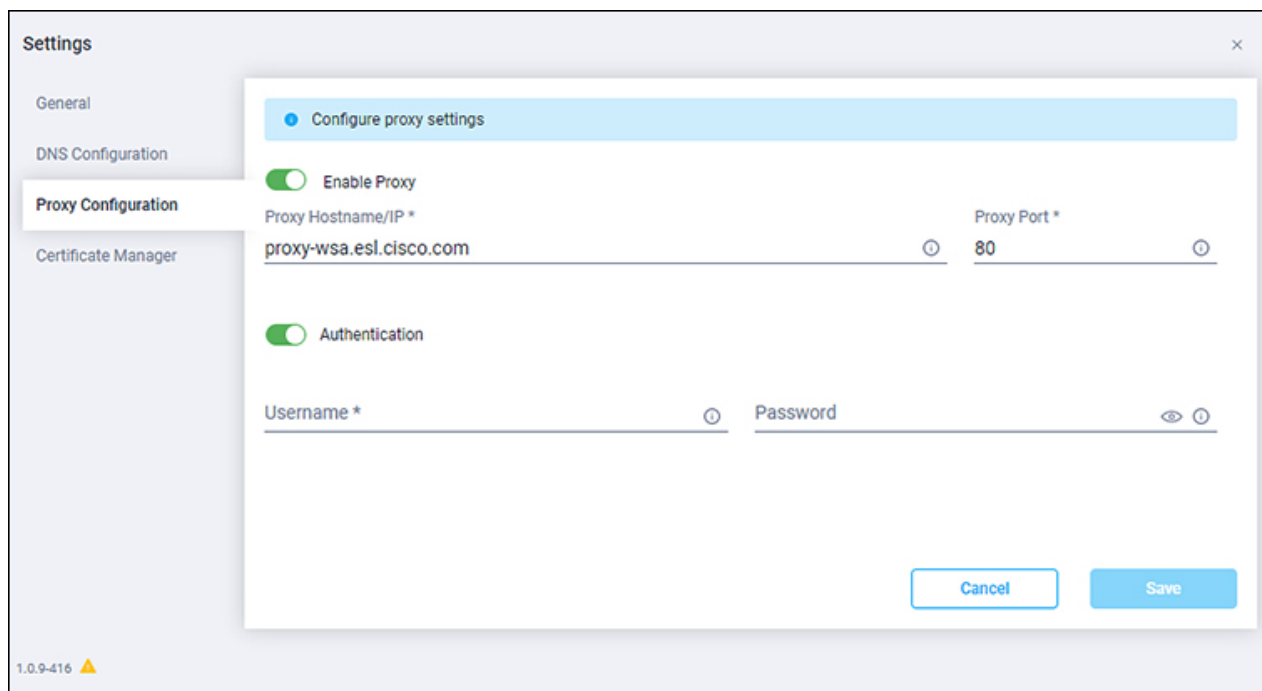
If the **Auto Update** option is turned OFF, that may periodically cause the Device Connector to be out-of-date, which could affect the ability of the Device Connector to connect to Intersight.

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 Connector:

- 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.
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.



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.



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.

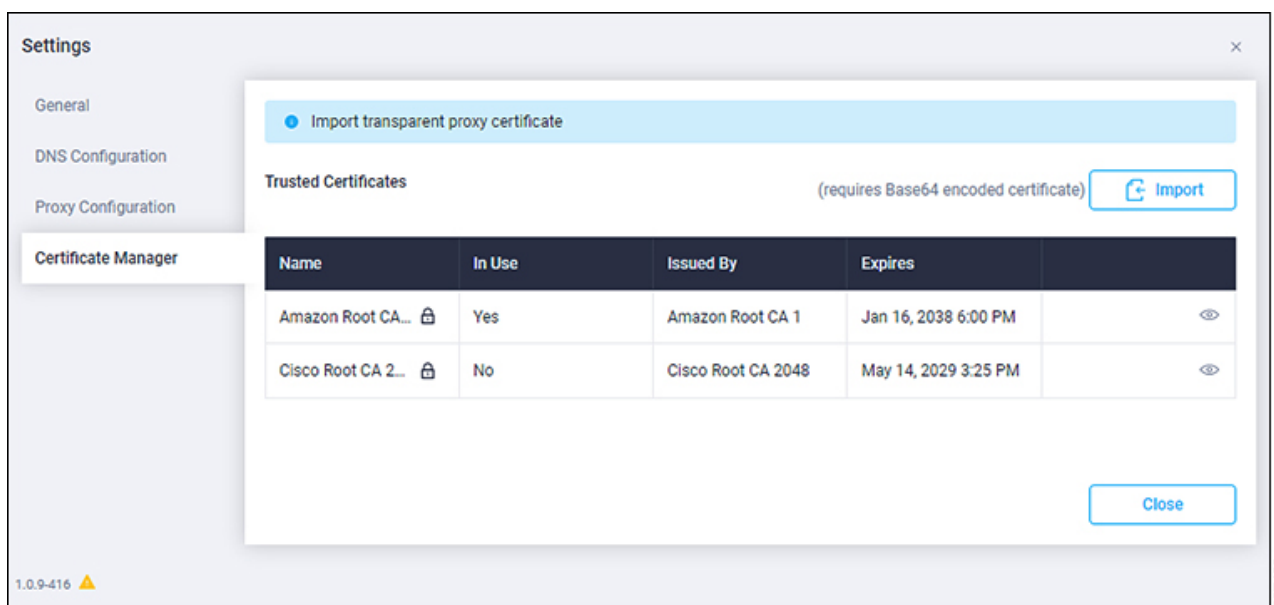
- a. In the **Enable Proxy** field, toggle the option to ON to configure the proxy settings.
  - b. In the **Proxy Hostname/IP** field, enter a Proxy Hostname and IP Address.
  - c. In the **Proxy Port** field, enter a Proxy Port.
  - d. In the **Authentication** field, toggle the **Authentication** option to ON to configure the proxy authentication settings, then enter a Proxy Username and Password for authentication.
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.

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

The **Certificate Manager** page appears.



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.

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](#).

## Claiming a Device

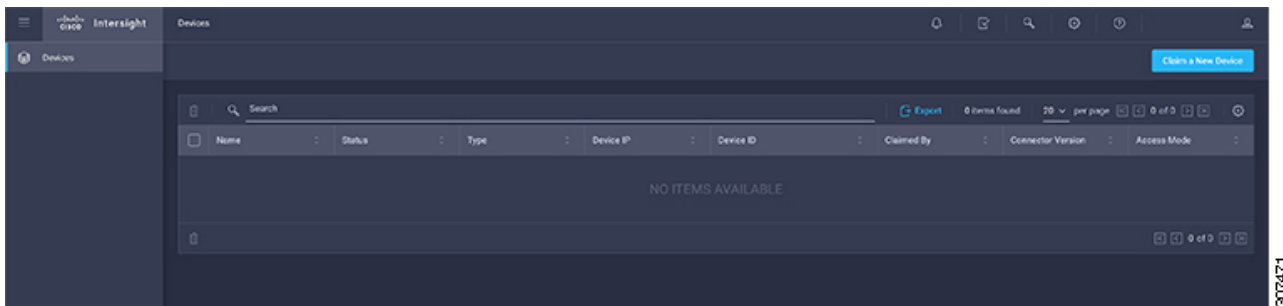
### Before you begin:

Configure the Intersight Device Connector information from the Cisco APIC site using the instructions provided in [Configuring the Intersight Device Connector](#).

1. Log into the Cisco Intersight Cloud site:

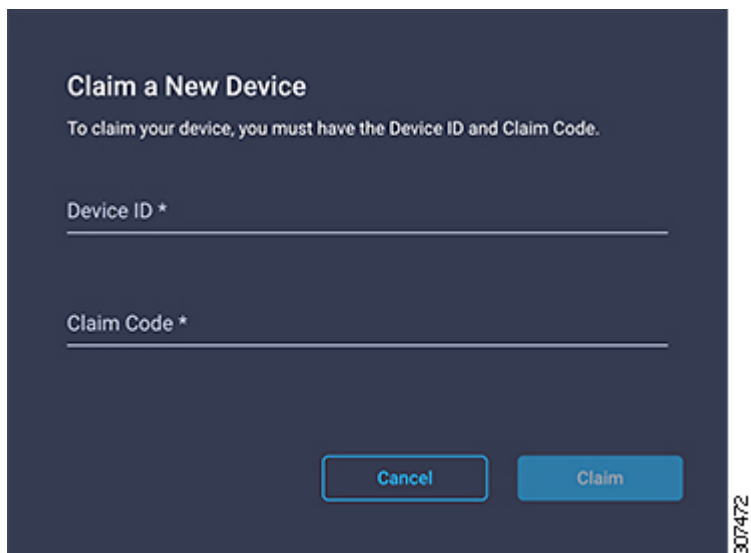
<https://www.intersight.com>

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



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





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**.
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.

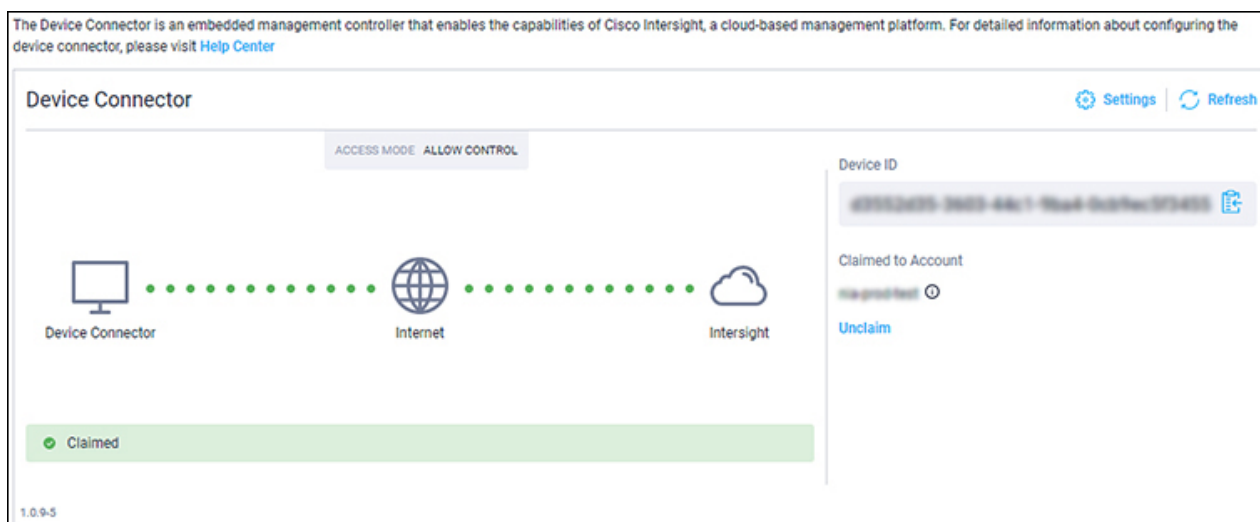
Click on the clipboard next to the fields in the Cisco APIC site to copy the field information into the clipboard.

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.

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.





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

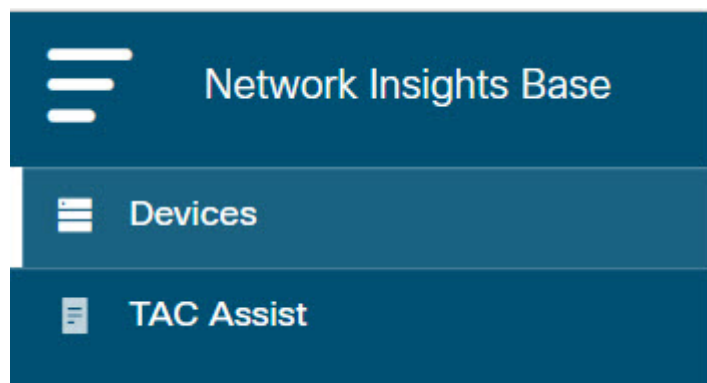
If you decide to unclaim this device for some reason, locate the **Unclaim** link in the **Intersight - Device Connector** page and click that link.

# Navigating Cisco Network Insights 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 select 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.

# Cisco Network Insights Base Dashboard

## Cisco NI-Base 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
<b>Devices</b>	Displays devices by device name, serial number, IP address, version, and platform in your network.
<b>TAC Assist</b>	Displays the total number of TAC assist logs currently being collected or finished being collected.

### Devices Dashboard

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 Dashboard

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.

You can choose to download the collected logs to a device and use it for further debugging or make them available to Cisco TAC as part of SR to analyze any traffic or service disruption.

### Status Messages for Log Collection

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

Property	Description
<b>Upload in Progress</b>	Displays when uploading the logs from Intersight Device Connector to Cisco Intersight Cloud is in progress.
<b>Complete</b>	Displays when upload to Cisco Intersight Cloud is complete.

## TAC Assist - Upload to Cloud

Before you upload the collected logs to Cloud, make sure the fabric is connected to Cisco Intersight Cloud. See [Configuring the Intersight Device Connector](#) for details.

### Procedure

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).

1. Click **TAC Assist** from the Cisco APIC navigation pane.
2. Click **Begin** to initiate the log collection process.
3. From the **Collect Logs** page check the device(s) for which 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.

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

The screenshot shows the TAC Assist interface. At the top, there is a 'Fabric' dropdown menu set to 'mutate-fab'. Below this, the 'TAC Assist' section contains a 'Begin the Log Collection Process' button and a sub-instruction: 'You will be asked to select the device(s) for which to collect Logs to assist TAC.' Below this is a 'Log Collection' table with the following data:

Type	Start Time	Status	Devices	Action
TAC Assist	Dec 15, 2019 09:10 am	COMPLETE	2	<a href="#">View details</a>
TAC Assist	Dec 15, 2019 08:48 am	COMPLETE	2	<a href="#">View details</a>
TAC Assist	Dec 12, 2019 04:20 pm	FAILED	1	<a href="#">View details</a>
TAC Assist	Dec 12, 2019 04:18 pm	COMPLETE	2	<a href="#">View details</a>

At the bottom of the table, there is a pagination control showing 'Page 1 of 1' and 'Objects Per Page 10 rows'. The footer indicates 'Displaying Objects 1 - 4 of 4'.

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	TACASSISTNWBt7vifSjqfNqXTTJtbA

Logs (2 of 2 Successful)

Device Name	Related Job ID	Status	Status Message	Log Location	Cloud
L81_STMORITZ	N/A	Success		/var/afw/vois/ceti/uploads/TACASSISTNWBt7vifSjqfNqXTTJtbA	Upload
ACC21_SAPORO	N/A	Success		/var/afw/vois/ceti/uploads/TACASSISTNWBt7vifSjqfNqXTTJtbA	Upload

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

Cisco NI-Base app enables Cisco TAC to send a request to collect and upload logs for an SR on Cisco APIC. Cisco TAC relies on the telemetry information available from the network to see a list of managed devices and then based on your SR request sends a trigger for collection of logs on the device to Cisco NI-Base.

The Enhanced TAC Assist feature triggered by Cisco TAC enables collection of logs for specified devices and uploads the logs to Cloud without any user explicit action. 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	TACASSISTlziTCzogRUuRQ4fhGTxvZw

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 Cisco TAC and hence no subsequent actions can be invoked on this job.

# Troubleshooting Cisco NI-Base

## Recovering Deleted Pre-Packaged Cisco NI-Base App

Follow these steps to recover a pre-packaged app if you accidentally deleted the pre-packaged app.

1. Remove the pre-packaged apps policy:
  - a. Login to Cisco APIC GUI with admin privileges.
  - b. Click the **Apps** tab on the top navigation bar.
  - c. Click **Settings** on the far-right side of the work pane.
  - d. Click **Change Prepackaged Apps Policy > Remove all**.
  - e. Wait until all pre-packaged apps are deleted, which may take several minutes.
2. To verify that MO is deleted execute the following:

```
# moquery -c 'apRsPrepackagedPlugin'  
  
# No Mos found
```

3. Install the pre-packaged apps policy:
  - a. Click the **Apps** tab on the top navigation bar.
  - b. Click **Settings** on the far-right side of the work pane.
  - c. Click **Change Prepackaged Apps Policy > Install all**.
4. Verify that the MO is configured and Cisco NI-Base app is in installing state:

```
# moquery -c 'apRsPrepackagedPlugin'  
Total Objects shown: 1  
  
# ap.RsPrepackagedPlugin  
tDn          : fwrepo/fw-Cisco_NIBASE  
appCtxRoot   : Cisco_NIBASE  
childAction  :
```