Cisco Network Insights Base Application for Cisco DCNM User Guide, Release 2.0.23

Table of Contents

The Cisco Network Insights Base Application for Cisco DCNM User Guide . . . 3
New and Changed Information . . . 4
Cisco Network Insights Base Installation . . . 5
About Cisco Network Insights Base Application . . . 5
Cisco Network Insights Base Upgrade . . . 6
Cisco NI-Base Pre-packaged App on Cisco DCNM . . . 6
Cisco Network Insights Base Setup and Settings . . . 8
About Cisco Network Insights Base on Cisco DCNM . . . 8
Cisco NI Base Settings . . . 8
Setting Up the Device Connector . . . 10
About Device Connector . . . 10
Configuring Smart Licensing . . . 10
Configuring the Intersight Device Connector . . . 11
Claiming a Device . . . 13
Navigating Cisco Network Insights Base . . . 16
Navigation Pane . . . 16
Cisco Network Insights Base Dashboard . . . 17
Cisco NI-Base Dashboard . . . 17
Devices Dashboard . . . 17
TAC Assist Dashboard . . . 17
TAC Assist - Upload to Cloud . . . 18
Enhanced TAC Assist . . . 19

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 figuresincluded in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbersin 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)

© 2017-2020 Cisco Systems, Inc. All rights reserved.

The Cisco Network Insights Base Application for Cisco DCNM 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 NI-Base application.

Feature	Description	Release	Where Documented
Cisco Network Insights Base, Release 2.0.23	The Cisco NI-Base app gets onboarded and configured automatically when device connector is configured.	2.0.23	About Cisco Network Insights Base Application
Smart license configuration on Cisco DCNM	After upgrading Cisco DCNM from 11.3.1 to 11.4.1 the Device Connector inherits the smart license configuration that was configured in Cisco DCNM 11.3.1.	2.0.23	Configuring Smart Licensing

Cisco Network Insights Base Installation

About Cisco Network Insights Base Application

Cisco Network Insights Base (Cisco NI-Base) application monitors utilities that can be added to the Cisco Data Center Network Manager (Cisco DCNM). 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 portal, using a secure Internet connection. See About Device Connector.

Cisco Intersight is a management platform delivered as a service. Cisco DCNM 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 DCNM Release 11.4, packages Cisco NI-Base app, Release 1.0.1 and 2.0.23. If you start Cisco NI-Base 2.0.23 then Cisco NI-Base 1.0.1 detects the latest application and disables its functionality.

Cisco NI-Base 1.0.1 app auto starts in clustered and unclustered modes of operation. Cisco NI-Base 2.0.1 and 2.0.23 apps do not auto start.

Cisco NI-Base 2.0.23 app works only in clustered mode. It does not work in unclustered mode.

Cisco NI-Base 2.0.23 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 on Cisco DCNM for specific telemetry details.

Starting with Cisco DCNM Release 11.4, Cisco NI-Base app queries for smart license information on Cisco DCNM. 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 lets you update the smart license. See Configuring Smart Licensing for details.

For a more detailed overview on Cisco Licensing, go to cisco.com/go/licensingguide.

Cisco Network Insights Base Upgrade

Cisco NI-Base Pre-packaged App on Cisco DCNM

App Version	1.0.1	2.0.1	2.0.23
Cisco NI-Base Auto Start	Yes	No	No
Cisco NI-Base Auto Onboard Fabric	Yes	No	Yes
Cisco DCNM Unclustered Mode	Yes	No	No
Cisco DCNM Clustered Mode	Yes	Yes	Yes
Cisco DCNM Version	11.3(1), 11.4(1)	11.3(1)	11.3(1), 11.4(1)
Upgrade Cisco DCNM	Yes	No	Yes • Cisco NI-Base 2.0.1 app left running with an upgrade available in UI.
Upgrade Cisco NI-Base App	Yes • 1.0.1 to 2.0.1 • 1.0.1 to 2.0.23 • 1.0.1 app in UI is inactive and 2.0.1 or 2.0.23 app is enabled.	Yes • 2.0.1 to 2.0.23 • 2.0.1 app in UI is inactive and 2.0.23 app is enabled.	N/A

Upgrading Cisco Network Insights Base Application

Cisco DCNM, Release 11.4 packages Cisco NI-Base 2.0.23 app. Only one instance of Cisco NI-Base app is supported on Cisco DCNM.

When Device Connector is connected to the Cisco Intersight Cloud, on upgrading Cisco DCNM to the latest release or on installing Cisco DCNM, 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 DCNM to newer version the Device Connector inherits the smart license configuration that was configured in the older version.

To upgrade Cisco NI-Base 1.0.1 or 2.0.1 pre-packaged app running on Cisco DCNM, 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 DCNM 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 DCNM, Release 11.3(1) in either clustered or unclustered mode with only Cisco NI-Base 1.0.1 app enabled then Cisco DCNM is upgraded to Release 11.4 and Cisco NI-Base 1.0.1 app still stays enabled.

When you upgrade Cisco DCNM, Release 11.3(1) in clustered mode with Cisco NI-Base 2.0.1 app enabled, then Cisco DCNM is upgraded to Release 11.4(1) and Cisco NI-Base 2.0.1 app stays running. You will see an option in the applications tab to upgrade the Cisco NI-Base 2.0.1 app to the newly packaged Cisco NI-Base 2.0.23 app.

Cisco Network Insights Base Setup and Settings

About Cisco Network Insights Base on Cisco DCNM

The Cisco Network Insights Base (Cisco NI-Base) application provides TAC Assist functionalities and collection of logs which are useful when working with Cisco TAC.

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 information 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
Fabric	Choose a fabric containing the pod you want visible to the Cisco NI-Base application.

Property	Description
	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. Cisco NI-Base app collects telemetry data. • **Connected / Claimed**: 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. For more information, see Configuring the Intersight Device Connector.
	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 Network Insights Base application. • **Rerun Setup**—Allows you to edit the Data Collection Setup by adding or removing fabrics.
	Displays the user guide for Cisco Network Insights Base application on Cisco DCNM.

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 DCNM 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 DCNM, 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. However, Cisco NI-Base app UI alerts you that the Device Connector is disconnected and lets you update the smart license.

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.

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 DCNM platform.

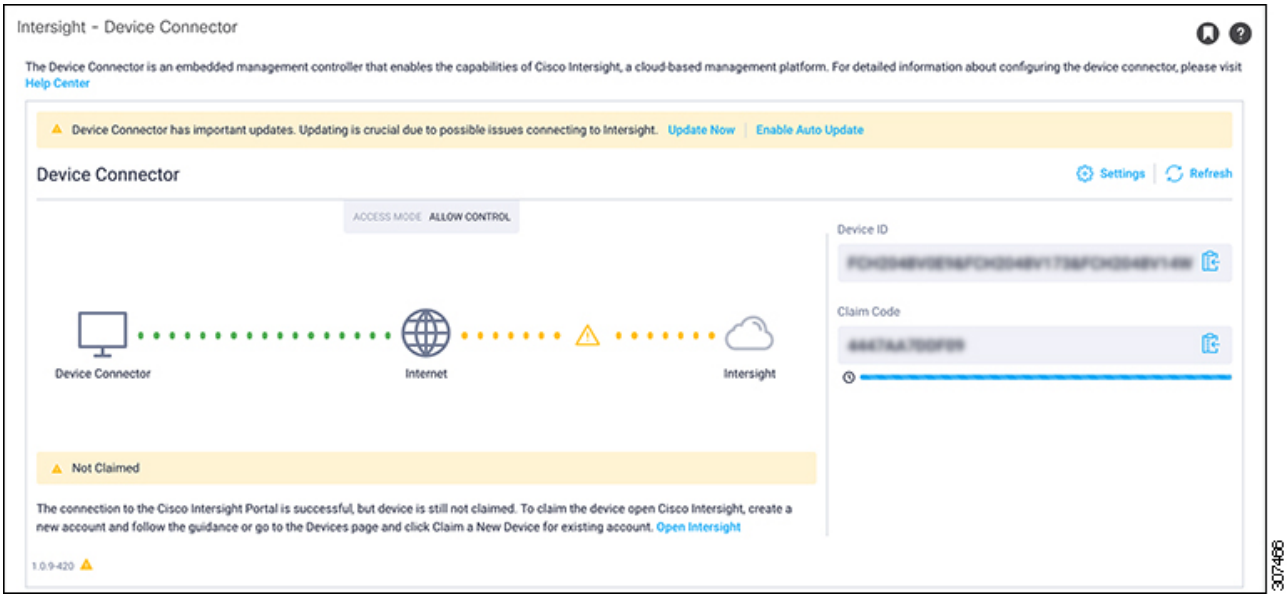
Cisco Intersight is a management platform delivered as a service. Cisco DCNM platform has a Device Connector that is packaged with the software that connects to Cisco Intersight Cloud. Device Connector is used to provide Cisco NI-Base Cloud connectivity feature sets.

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

To setup the Device Connector, follow these steps:

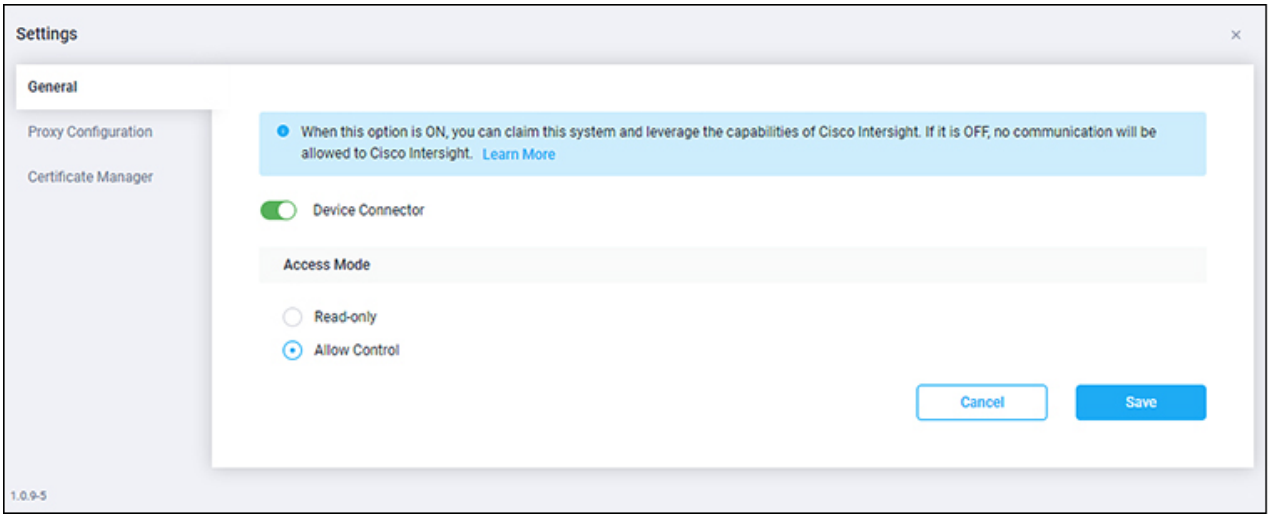
1. On the Cisco DCNM navigation pane, click Administration.
2. Under the Cisco DCNM Server list, click Device Connector.

   The Device Connector work pane appears:



3. At the far right of the screen, click **Settings**.

   The **Settings - General** dialog appears:



Device Connector (switch)

This is the main switch for the Device Connector communication with Cisco Intersight. When the switch is on (green highlight), the system is claimed and the capabilities of the Cisco Intersight can be leveraged. If the switch is off (gray highlight), no communication can occur between the platform and Cisco intersight.

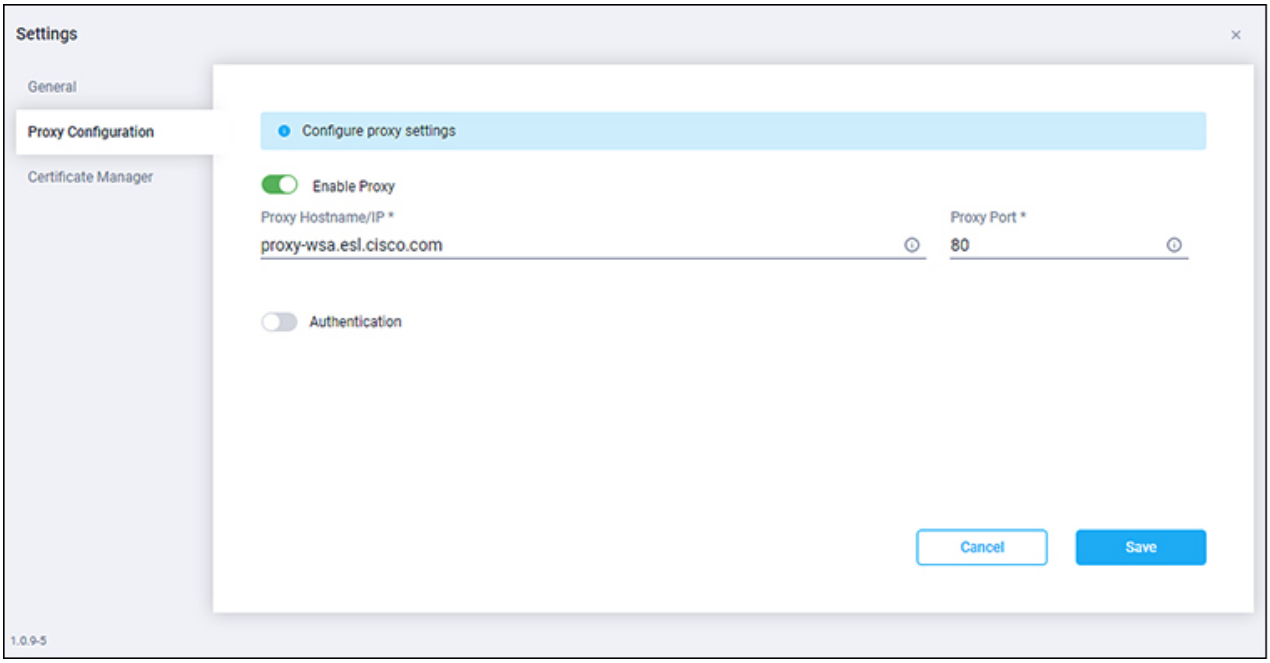
Access Mode

Read-only: This option ensures that no configuration changes are done by Cisco Intersight on Cisco DCNM. 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.

Allow Control: This option (selected by default) enables you to perform full read/write operations from the appliance, based on the features available in Cisco Intersight. This function is not used for changes from Cisco Intersight Cloud to customer network.

4. Set the Device Connector to on (green highlight) and choose **Allow Control**.
5. Click **Proxy Configuration**.

   The **Settings - Proxy Configuration** dialog appears.



Enable Proxy (switch)

Enable HTTPS Proxy to configure the proxy settings.

Proxy Hostname/IP * and **Proxy Port***: Enter a proxy hostname or IP address, and a proxy port number.

Authentication (switch)

Enable proxy access through authentication. When the switch is on (green highlight), authentication to the proxy server is required. If the switch is off (gray highlight), no authentication is required.

Username* and **Password**: Enter a user name and password for authentication.

Proxy settings are required for Network Insights.

6. Enable the proxy (green highlight) and enter a hostname and port number.
7. Optional: If proxy authentication is required, enable it (green highlight) and enter a username and password.
8. Click **Save**.

Claiming a Device

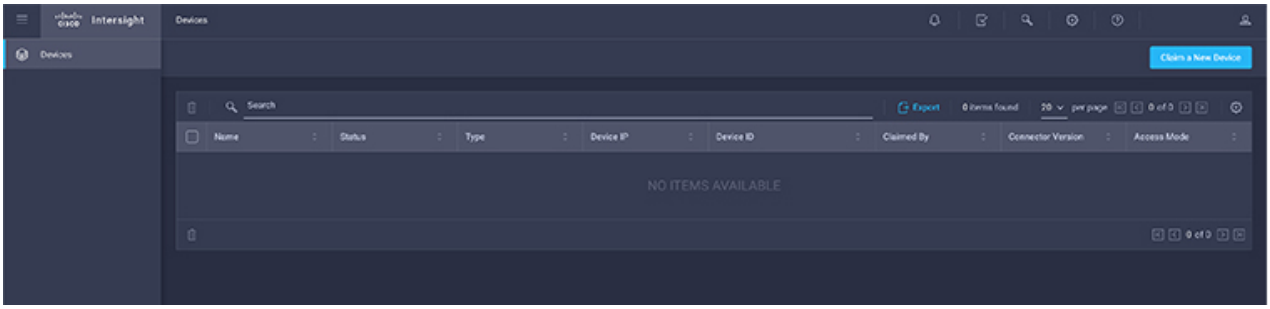
Before you begin:

Configure the Intersight Device Connector information from the Cisco DCNM site using the instructions provided in Configuring the Intersight Device Connector.

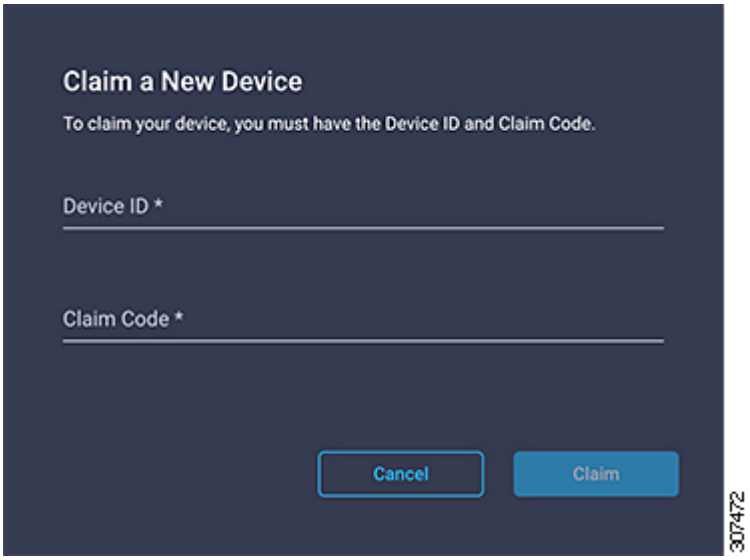
1. Log into the Cisco Intersight cloud site:

   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 DCNM 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 DCNM site and paste them into the proper fields in the **Claim a New Device** page in the Intersight cloud site.

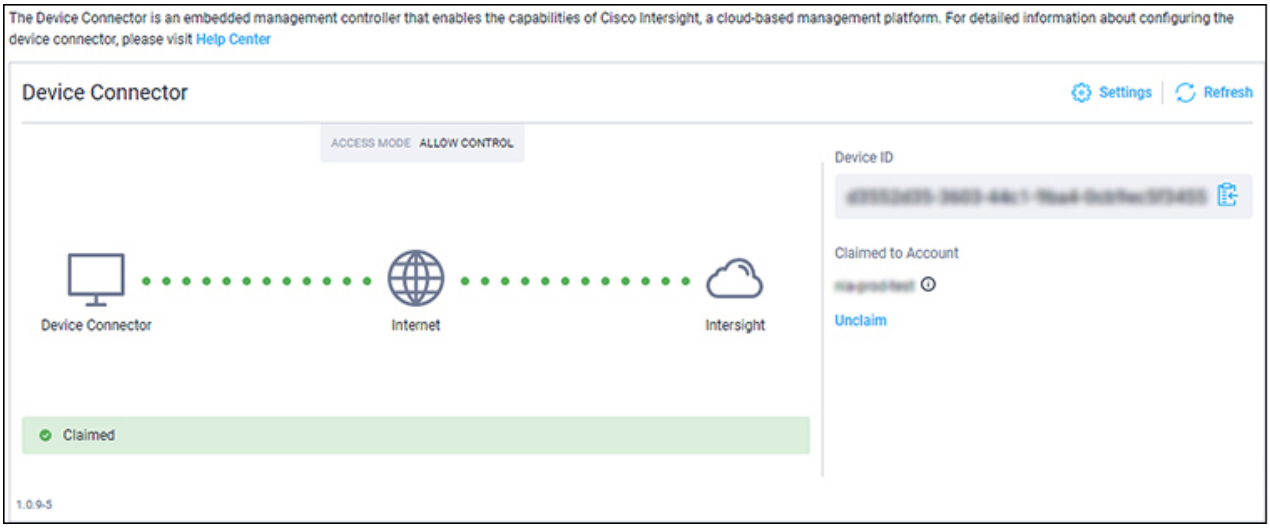
   Click on the clipboard next to the fields in the Cisco DCNM site to copy the field information into the clipboard.

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 DCNM system, with Connected shown in the Status column.

6. Go back to the **Intersight - Device Connector** page in the Cisco DCNM 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.

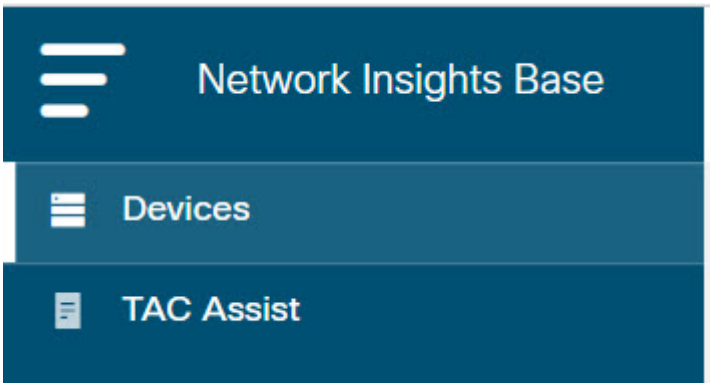
If you decide to unclaim this device for some reason, locate the **Unclaim** link in the **Intersight - Device Connector** page and click that link.

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
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 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.

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.

Status Messages for Log Collection in 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 - Upload to Cloud

Before you begin:

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

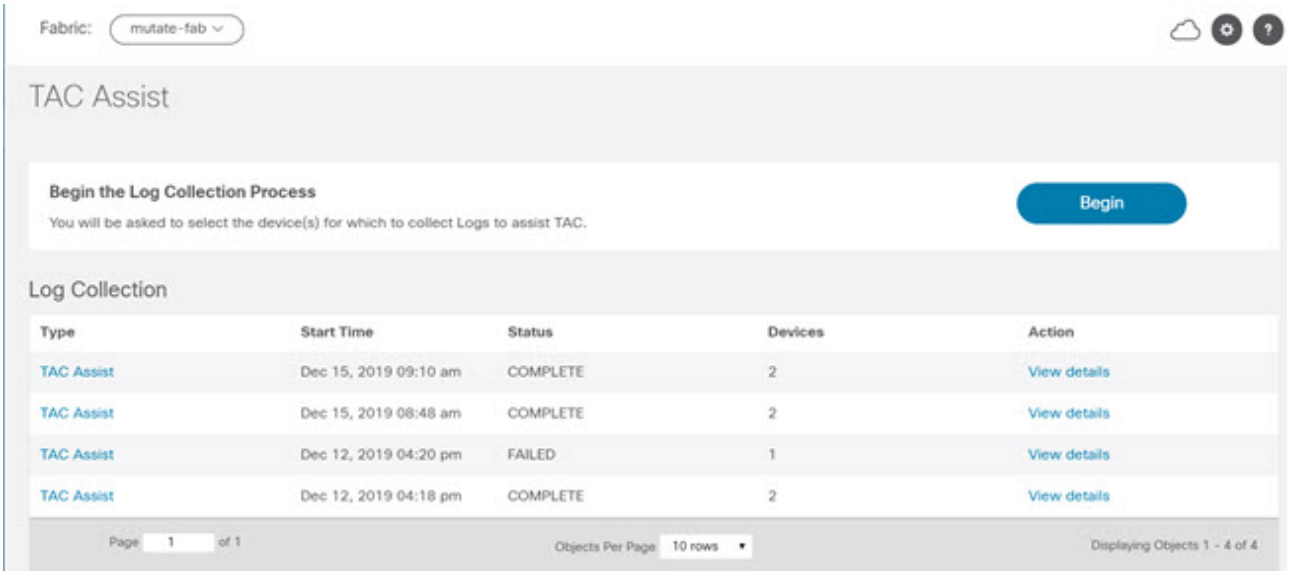
Procedure

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 Cisco Intersight Cloud. The collected logs for specified devices then can be attached to the service requests (SRs).

1. Click **TAC Assist** in the Cisco DCNM navigation pane.

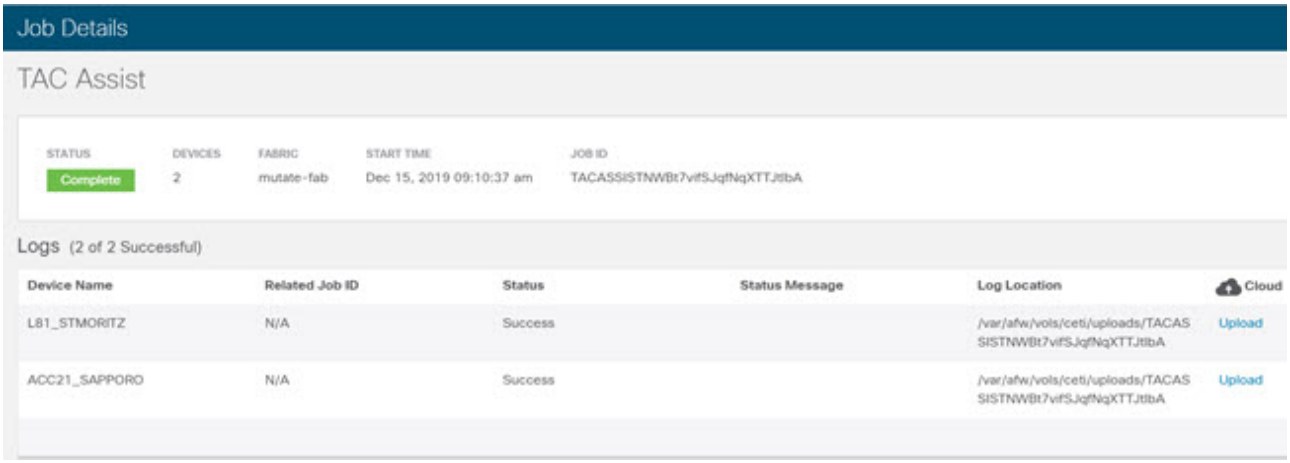
2. Click **Begin** to choose the fabric device(s).
3. From the **Collect Logs** page check the device(s) for which to collect logs to assist TAC.

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



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.



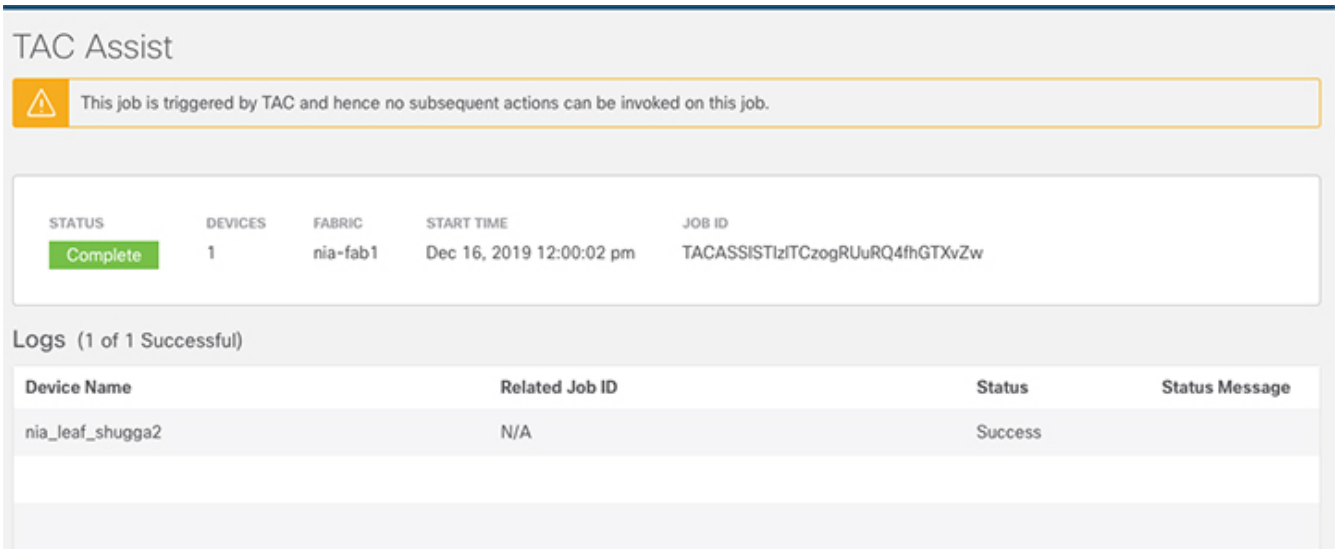
5. Click **Upload** to upload the collected logs to Cisco Intersight Cloud.

   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 DCNM. 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 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.



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.