Cisco Network Insights Base Application for the Cisco Application Policy Infrastructure Controller Release Notes, Release 1.0.1

Cisco Network Insights Base application consists of a monitoring utility that are added to the Cisco Application Policy Infrastructure Controller (APIC).

This document describes the features, caveats, and limitations for Cisco Network Insights Base on the Cisco APIC.

Table 1 shows the online change history for this document.

Table 1 Online History Change

Date	Description
Mar 29, 2020	Compatibility information for Cisco NI Base.
November 5, 2019	Release 1.0.1 became available.

Contents

This document includes the following sections:

New Software Features

The following table lists the new software features in this release:

Table 2 New Software Features

Feature	Description
Cisco Network Insights Base Application	Cisco Network Insights Base is available on Cisco APIC.

About Cisco Network Insights Base Application

Cisco Network Insights Base application is pre-installed and enabled with Cisco APIC, release 3.2(9). Cisco Network Insights Base allows the application to share environment specific data with Cisco when connected and claimed in the Device Connector.

For details on device connector, see Setting Up the Device Connector.

Disabling Cisco Network Insights Base Application

The following steps are required to disable the Cisco Network Insights Base application enabled with Cisco APIC, release 3.2(9):

1. Login to the Cisco APIC GUI with admin privileges.
2. Click the Apps tab on the top navigation bar. Then click Open from the Cisco Network Insights Base application dialog.
3. The Cisco Network Insights Base application dialog appears.
4. Uncheck Help Cisco improve its products option.

Upgrading Cisco Network Insights Base Application

Cisco Network Insights Base application is supported on Cisco APIC, release 3.2(9). This application is not compatible with Cisco APIC, releases 4.0.x, 4.1.x, 4.2(1i), and 4.2(2e).

When you upgrade from Cisco APIC, release 3.2(9) to Cisco APIC, releases 4.0.x, 4.1.x, 4.2(1i), or 4.2(2e) the application goes into disabled state. The application shows the screen with unsharing environment specific data.

Setting Up the Device Connector

Cisco Network Insights Base application requires you to setup the device connector for the application to share environment specific data. This section contains steps required to setup the device connector.

- About Device Connector

About Device Connector

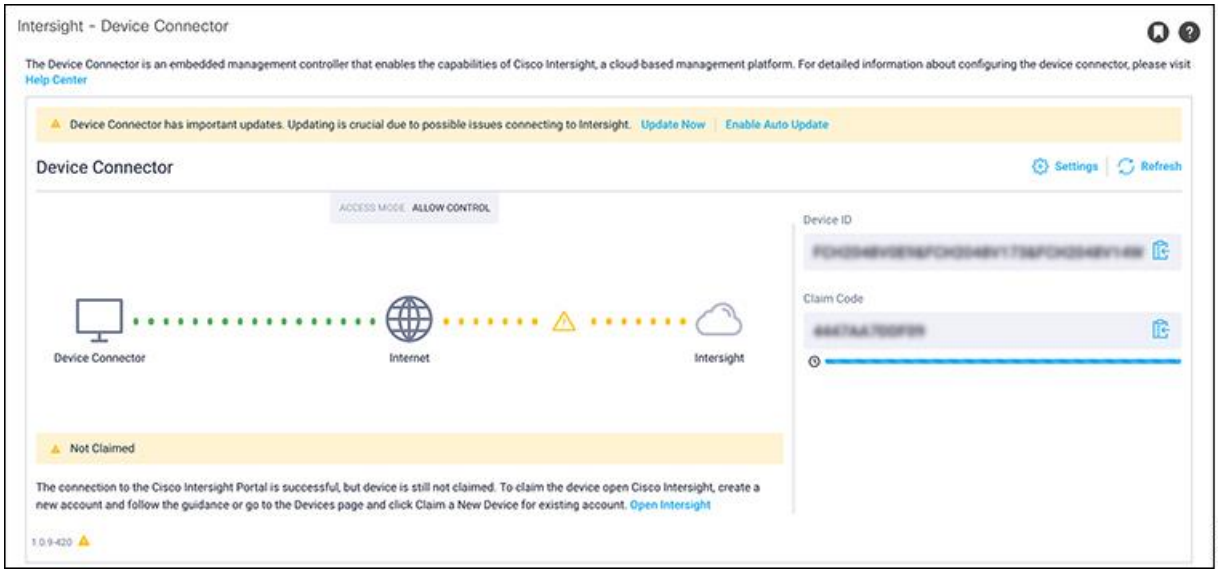
Devices are connected to the Intersight portal through a Device Connector that is embedded in the management controller of each system. Device Connector provides a secure way for the connected devices to send information and receive control instructions from the Cisco Intersight portal, using a secure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

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.

Configuring the Intersight Device Connector

To setup the Device Connector, follow these steps:

1. In the Cisco APIC site, on the menu bar, choose Apps.
2. In the Apps pane, click Device Connector. 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.

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 7.

3. 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 Auto Update enabled, you will see a message towards the top of the screen, telling you that Device Connector has important updates available.

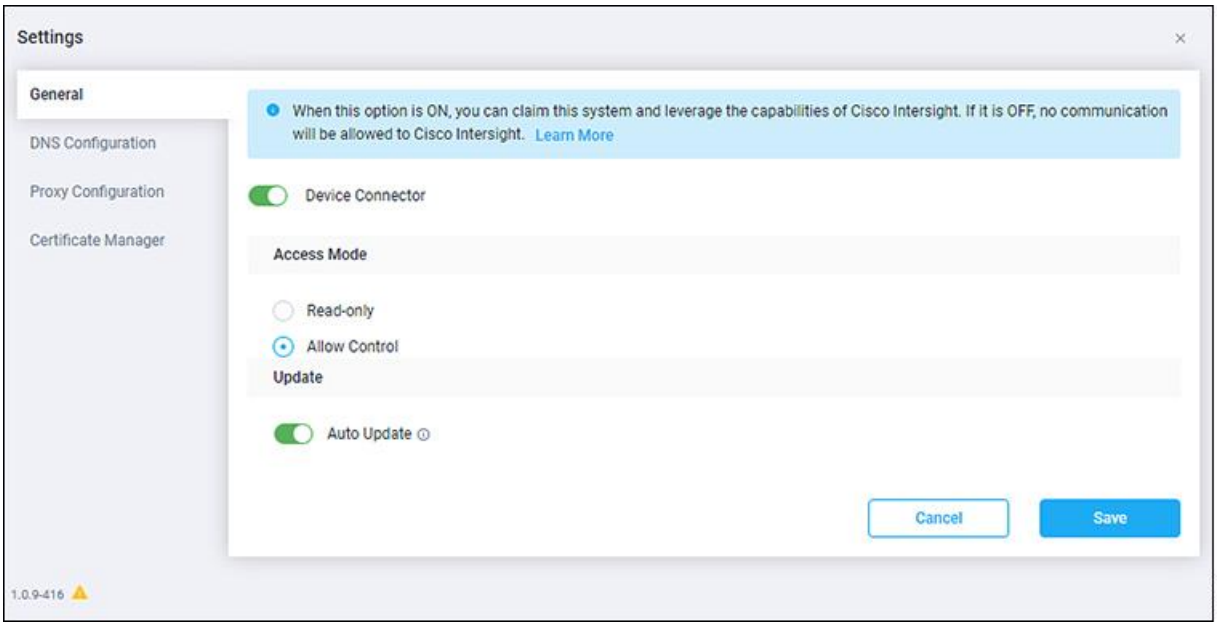
   - If you do not want to update the software at this time, go to Step 4, to begin configuring the Intersight Device Connector.
   - If you would like to update the software at this time, click one of the two links in the yellow bar towards the top of the page, depending on how you would like to update the software.

     a) Update Now: Click this link to update the Device Connector software immediately.

     b) 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 5.c, for more information.

4. 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.



5. 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.
      - 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.

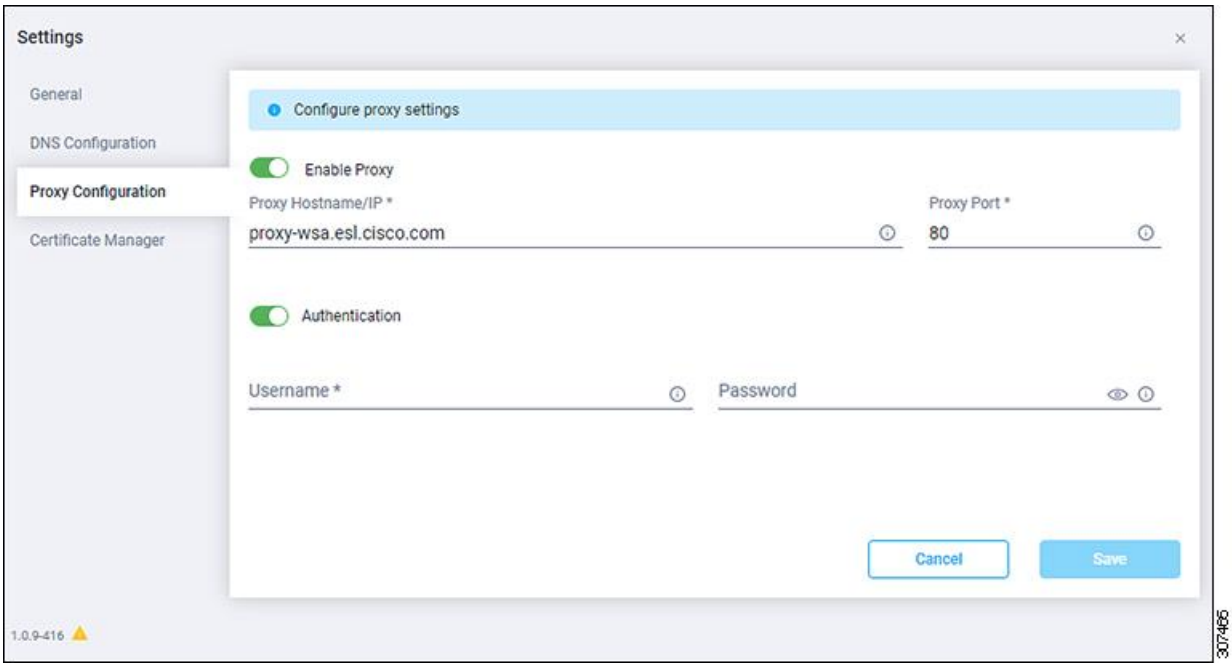
6. When you have completed the configurations in the General page, click Save.

   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 7.
   - If you want to make manage certificates with the Device Connector, go to Step 10.

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.



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.

   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.

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.

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

    The Certificate Manager page appears.

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.

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

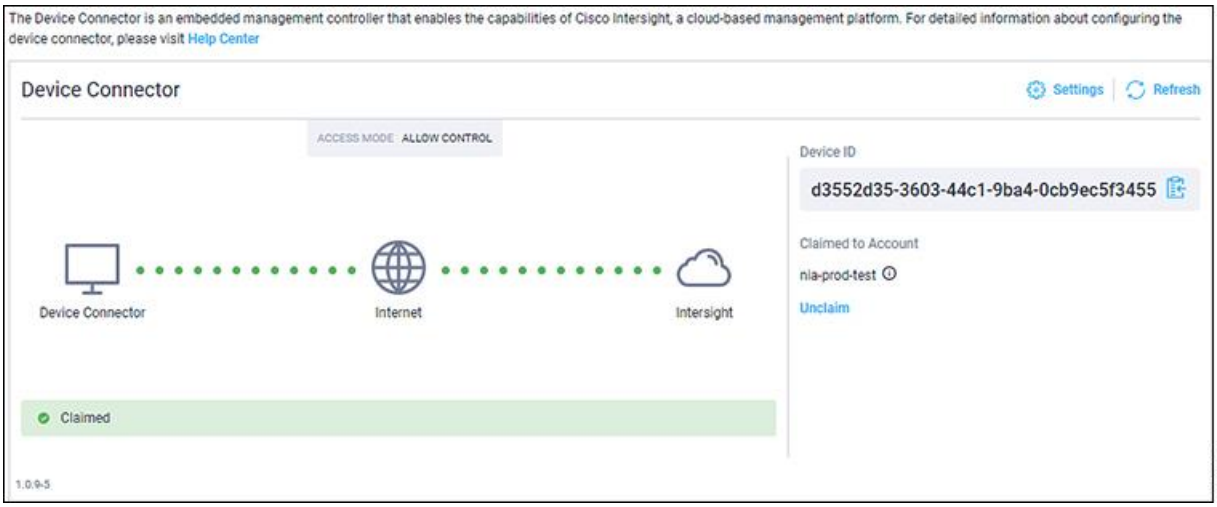
Claiming a Device

Claim the device using the following steps:

1. Log into the Intersight cloud site.
2. In the Intersight cloud site, under the Devices tab, click Claim a New Device.
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.

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.

Compatibility Information

For Cisco NI Base on compatibility with Day-2 Operations apps, see the Cisco Day-2 Operations Apps Support Matrix.

Table 3 Compatibility Information in This Release

Software/Hardware	Release
Cisco APIC cluster	Any APIC cluster

Open Caveats

There are no open caveats in this release.

Resolved Caveats

There are no resolved caveats in this release.

Related Documentation

The Cisco Network Insights Advisor documentation can be accessed from the following website:

https://www.cisco.com /c/en/us/support/data - center- analytics/network - insights- advisor/model.html

The documentation includes installation, upgrade, configuration, technical references, and release notes, as well as other documentation.

Documentation Feedback

To provide technical feedback on this document, or to report an error or omission, send your comments to cisconetworkinsights - docfeedback@cisco.com.