Cisco APIC and Intersight Device Connector

Revised: August 30, 2023

New and Changed Information

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

Table 1: New Features and Changed Behavior

Cisco APIC Release	Feature	Description
6.0(2)	New Cisco Intersight proxy added directly to switches	Usage of this new proxy requires a completed DNS Service Policy in the management VRF instance to program DNS onto all switch nodes to enable this new proxy to reach Cisco Intersight and share Asset Device Registration (Connected Device Sub Target) telemetry. Prior to the 6.0(2) release, this was handled through the Cisco APIC Connector, and switch DNS configuration was not a requirement. For more information, see the "Configuring a DNS Service Policy" section in the *Cisco APIC Basic Configuration Guide*.
6.0(1)	Switches get claimed automatically	When you claim a Cisco APIC, all switches in the fabric will also get claimed automatically in Cisco Intersight. For more information see Claiming a Device Using the GUI, on page 9.
5.2(1)	DNS and proxy configurations are no longer configured within the **Intersight - Device Connector** pages	The DNS and proxy configurations are no longer configured within the **Intersight - Device Connector** pages. Instead, these settings are configured in a centralized area in the Cisco APIC, outside of the **Intersight - Device Connector** pages.
4.2(5)	**Auto Update** is enabled by default	The **Auto Update** option is now enabled by default.
4.1(2)	Initial release of this feature	Initial release of this feature.

About Device Connector

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

When an Intersight-enabled device or application starts, the Device Connector starts at boot by default, and attempts to connect to the cloud service. If the **Auto Update** option is enabled, the Device Connector is automatically updated to the latest version through a refresh by the Cisco Intersight service when you connect to Cisco Intersight. For more information on the **Auto Update** option, see About the Auto Update Option, on page 3.

About the Auto Update Option

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

If a Device Connector upgrade is in progress, the following message displays:

```
DC upgrade is in progress. Wait for DC upgrade to complete before triggering APIC upgrade
```

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

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

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

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

We recommend that you enable the **Auto Update** option. Beginning in Cisco APIC release 4.2(5), this option is enabled by default.

If you downgrade the Cisco APIC to the 4.2(4) or earlier release, the Device Connector upgrade policy will be set to **Manual** if the policy was set to **Auto** in the 4.2(5) or later release.

About Device Connector Configuration Changes in Clustered APIC Nodes

The Cisco APIC appliance is deployed as a cluster. A minimum of three infrastructure controllers, or nodes, are configured in a cluster to provide control of the scale-out Cisco ACI fabric.

When you make a configuration change to a Device Connector in one of the clustered nodes in the Cisco APIC fabric, that configuration change is automatically reflected on the other Device Connectors in the other nodes in that Cisco APIC cluster.

For example, assume you have two DNS servers shown as configured in the **DNS Configuration** page for the Device Connector in one of the APIC nodes in the cluster. If you were to go into the same pages for the Device Connector in the other two APIC nodes in the cluster, you should see the same two DNS servers configured in those nodes as well. Then, if you were to add a third DNS server in the **DNS Configuration** page for the Device Connector in one of the APIC nodes in the cluster and click **Save** in that page, after the two-minute cycle for DNS change to take affect, that change will be shown in the **DNS Configuration** page for the Device Connector in the other two APIC nodes in the cluster.

This configuration change behavior applies to claimed and unclaimed Device Connectors in clustered nodes in the Cisco APIC fabric as well. For example, if you were to configure and claim the Device Connector in one of three APIC nodes in a cluster, you would see that the Device Connector is automatically configured and claimed in the other two APIC nodes in that cluster. Likewise, if you were to then unclaim the Device Connector in one of the APIC nodes in a cluster, you would then see that the Device Connector is unclaimed automatically in the other APIC nodes in that cluster.

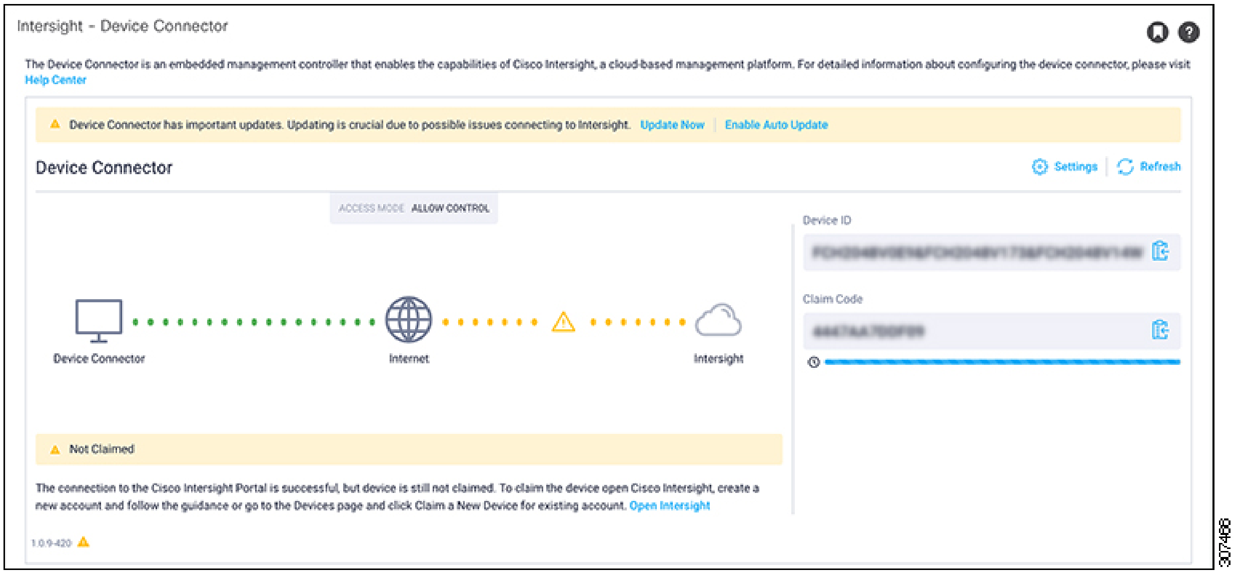
Configuring the Intersight Device Connector

Procedure

Step 1 In the Cisco Application Policy Infrastructure Controller (APIC), on the menu bar, choose **System** > **System Settings**.

Step 2 In the **Navigation** pane, click **Intersight**.

The **Intersight - Device Connector** overview pages appears. The Device Connector should be shown as connected to the Internet (green dotted lines) in the **Device Connector** graphic in this page.



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

ACCESS MODE ALLOW CONTROL

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 ⚠

- 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 12, on page 7.

Step 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 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.

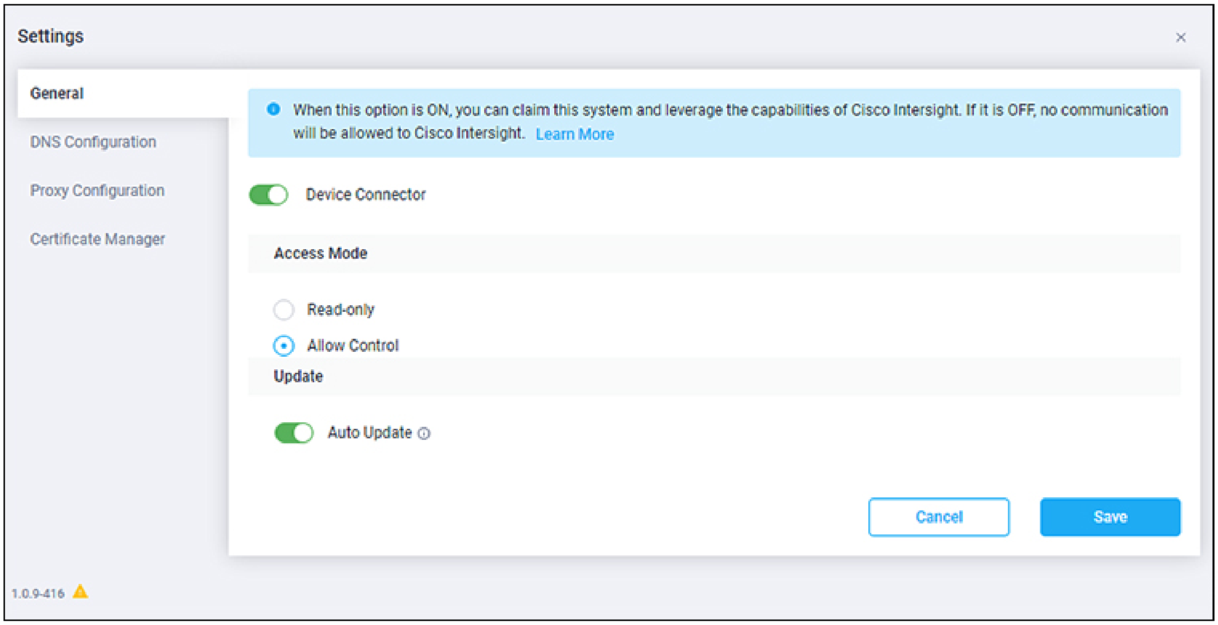
- If you do not want to update the software at this time, go to Step 4, on page 5 to begin configuring the Intersight Device Connector.

- If you would like to update the software at this time, click one of the two links in the yellow bar toward the top of the page, depending on how you would like to update the software:
  - **Update Now**: Click this link to update the Device Connector software immediately.
  - **Enable Auto Update**: Click this link to go to the **General** page, where you can toggle the **Auto Update** field to ON, which allows the system to automatically update the Device Connector software. See About the Auto Update Option, on page 3 for more information.

Step 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.

Note The following screenshots show tabs in the Settings page that are displayed in releases prior to release 5.2(1). These tabs changed beginning with release 5.2(1), as described in Step 7, on page 6.



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.

Device Connector: ON

Access Mode

○ Read-only

● Allow Control

Update

Auto Update: ON

Step 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.

See About the Auto Update Option, on page 3 for more information.

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

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

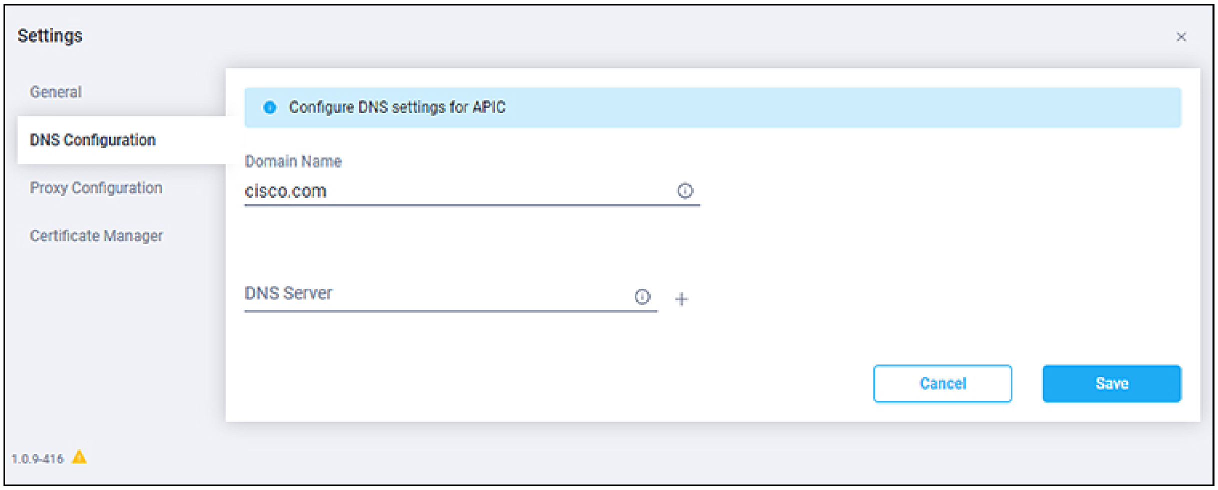
Step 7 Continue with the next steps of the configuration process, depending on the release of the software.

- If you are running on a release prior to release 5.2(1), you can make or verify several DNS or proxy configuration settings for the Intersight Device Connector in these **Intersight - Device Connector** pages:
  - To configure or verify the DNS settings, go to Step 8, on page 6.
  - To configure the proxy that the Device Connector will use to communicate with the Intersight cloud, go to Step 11, on page 7.

  In addition, if you want to manage certificates with the Device Connector, go to Step 14, on page 8.
- If you are running on release 5.2(1) or later, the DNS and proxy configurations are no longer configured within the **Intersight - Device Connector** pages. Instead, these settings are configured in a centralized area in APIC, outside of the **Intersight - Device Connector** pages, as described later in these procedures.
  - To manage certificates with the Device Connector, go to Step 14, on page 8.
  - To configure the DNS or proxy configuration settings, go to Step 17, on page 9.

Step 8 If you want to configure or verify the DNS settings, click **Settings**, then click **DNS Configuration**.

The **DNS Configuration** page appears.



Domain Name: cisco.com

DNS Server

Step 9 In the **DNS Configuration** page, configure or verify the DNS settings.

While you can configure DNS servers in this page, we recommend that you use the general Cisco APIC settings instead to configure a DNS service policy to connect with DNS providers. You can do this by navigating to **Fabric** > **Fabric Policies** > **Policies** > **Global** > **DNS Profiles**, then right-clicking on **DNS Profiles** and selecting **Create DNS Profile**. For more information on configuring a DNS service policy, see the *Cisco APIC Basic Configuration Guide*.

If you use the general Cisco APIC settings instead to configure a DNS service policy to connect with DNS providers as described above, you should see the DNS configuration information already populated in this **DNS Configuration** page. If you do not, or if you would rather configure DNS servers in this page, follow these steps:

a) In the **Domain Name** field, add a DNS domain name.

b) In the **DNS Server** field, configure at least one DNS Server to enable DNS name resolution. The Intersight device connector must be able to successfully resolve DNS records.

Every two minutes, the Device Connector queries the Cisco APIC for any DNS changes, so you might see a warning message at this point, saying "APIC DNS changes can take up to two minutes to take effect."

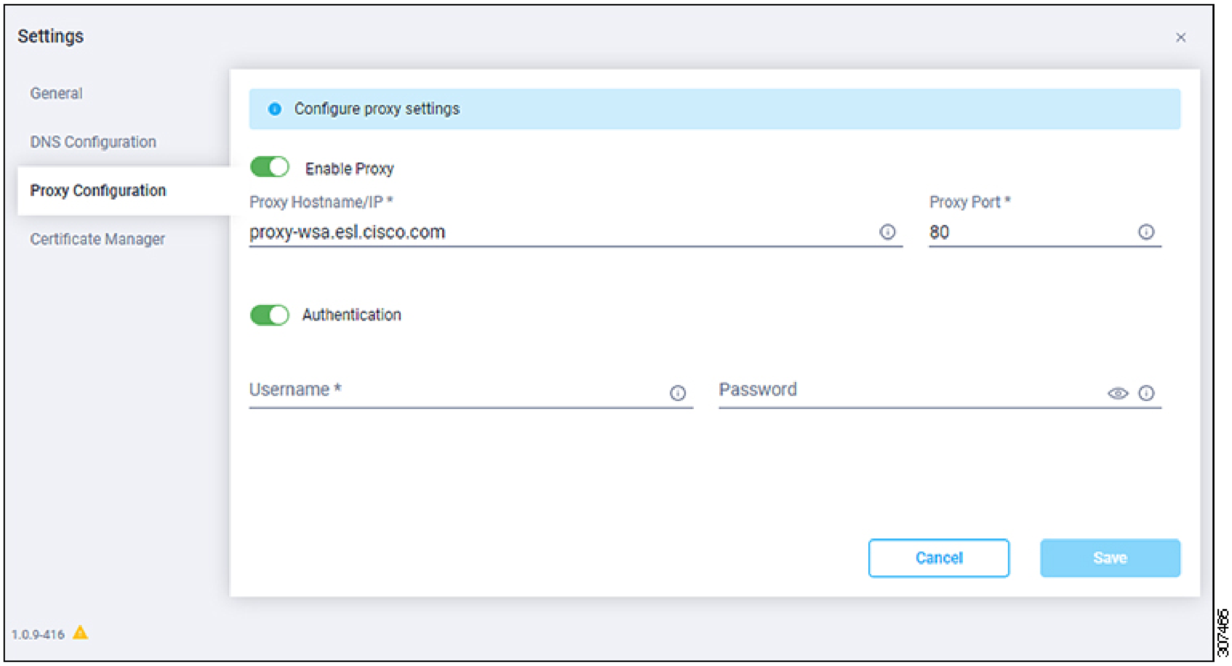
Step 10 When you have completed the configurations in the **DNS Configuration** page, click **Save**.

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 11, on page 7.
- If you want to manage certificates with the Device Connector, go to Step 14, on page 8.

Step 11 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.



Configure proxy settings

Enable Proxy

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

Proxy Port * 80

Authentication

Username *

Password

Step 12 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.

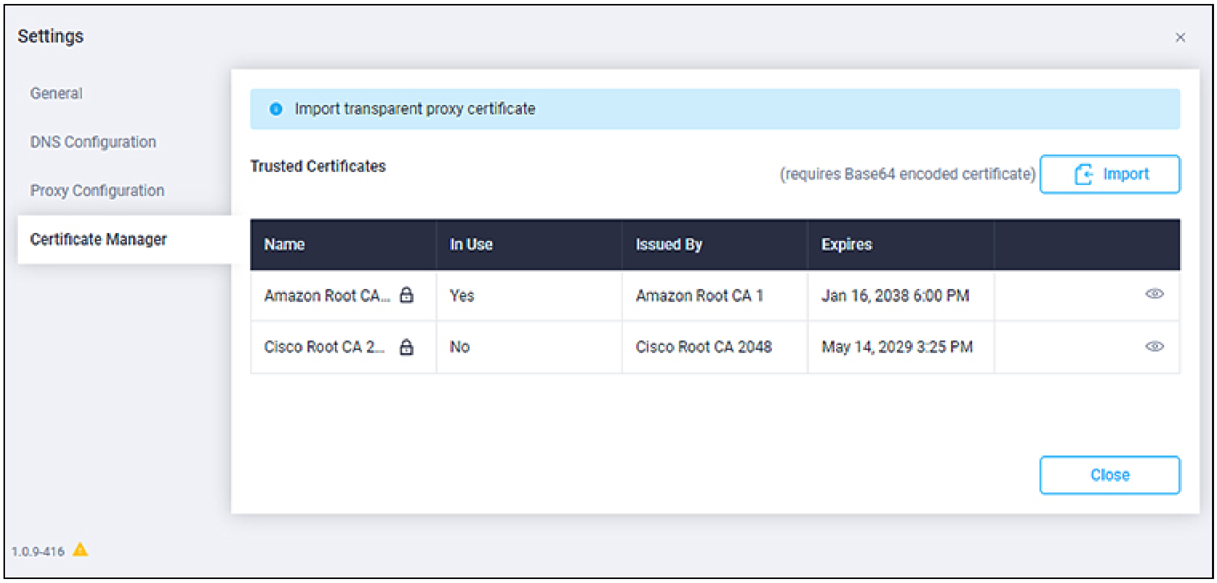
Step 13 When you have completed the configurations in the **Proxy Configuration** page, click **Save**.

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

The **Certificate Manager** page appears.



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	

307462

Step 15 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 16 When you have completed the configurations in the **Certificate Manager** page, click **Close**.

Step 17 If you are running on release 5.2(1) or later, configure the proxy settings in the centralized area in APIC by navigating to the following locations:

- To configure the DNS settings, navigate to:

  Fabric > **Fabric Policies** > **Policies** > **Global** > **DNS Profiles**

  Right-click on **DNS Profiles** and select **Create DNS Profile**. For more information on configuring a DNS service policy, see the *Cisco APIC Basic Configuration Guide*.

- To configure the proxy settings, navigate to:

  System > **System Settings** > **Proxy Policy**

  In the **Proxy Policy** page, configure a proxy server for the HTTP or HTTPS protocol, or set the configuration to allow a direct connection to certain hosts. When authentication is required for a proxy server, use the following format:

  ```
  http[s]://[username:password]@proxy-server[:proxyport]
  ```

  For more information on configuring the proxy settings, see the *Cisco APIC Basic Configuration Guide*.

You can also configure both the DNS and the proxy settings through the First Time Setup wizard. For more information, see the chapter "First Time Setup Wizard" in the *Cisco APIC Basic Configuration Guide*.

What to do next

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

Claiming a Device Using the GUI

Before you begin

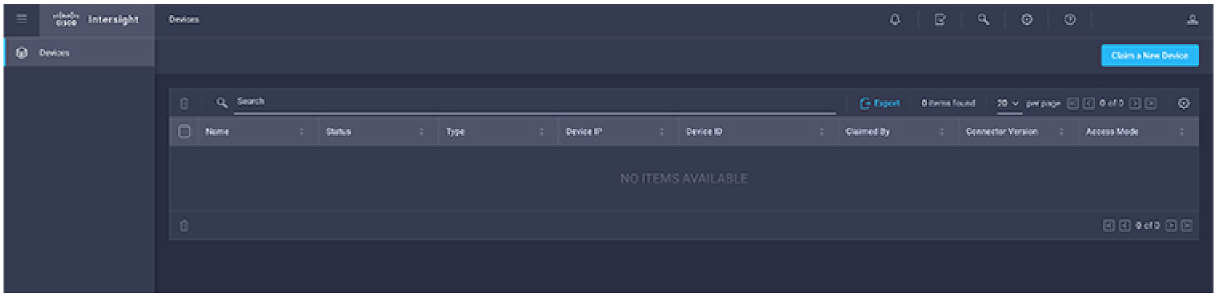
Configure the Cisco Intersight Device Connector information from the Cisco Application Policy Infrastructure Controller (APIC) site using the instructions provided in Configuring the Intersight Device Connector, on page 4.

Procedure

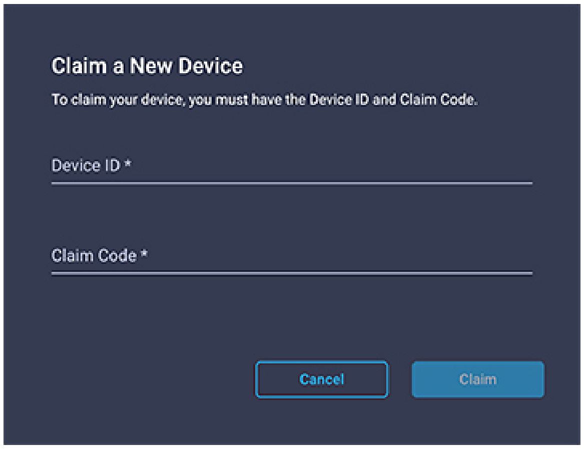
Step 1 Log into the Cisco Intersight cloud site:

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 Cisco Intersight cloud site.

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

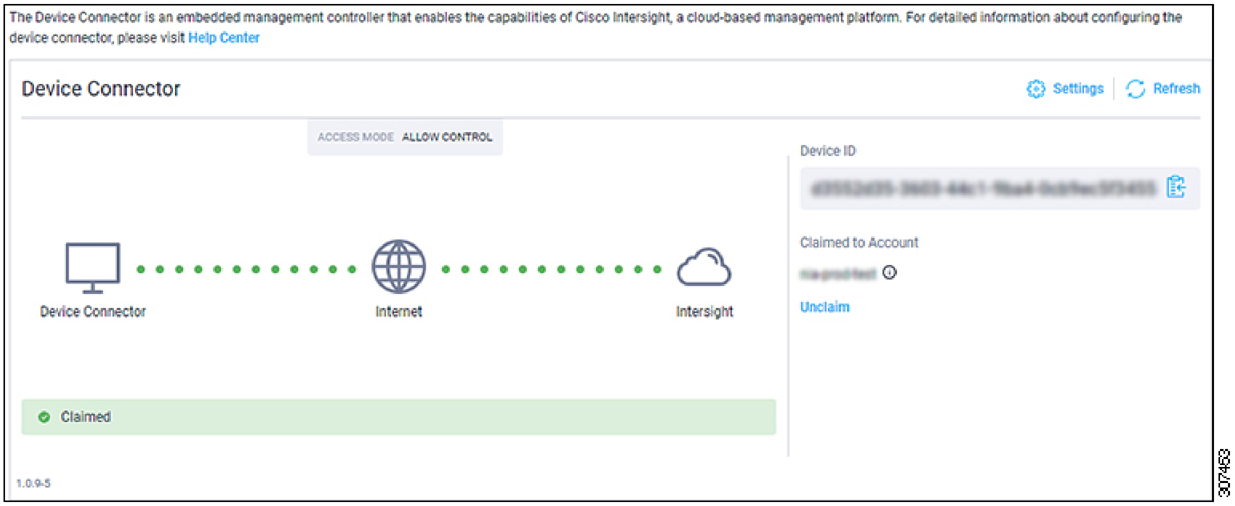
Step 5 In the **Claim a New Device** page in the Cisco Intersight cloud site, click **Claim**.

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

Beginning in the 6.0(1) release, when you claim a Cisco APIC, all switches in the fabric also get claimed automatically in Cisco Intersight.

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

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



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 ID

[redacted]

Claimed to Account

[redacted]

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.

About Auto-Populating the Data Center HTTP or HTTPS Proxy Configuration

Starting with the 4.2(4o) release, the Cisco Application Policy Infrastructure Controller (APIC) can automatically populate the proxy configuration for the data center by using values from the smart license HTTP or HTTPS proxy configuration. This feature simplifies the process of configuring the data center proxy and reduces the possiblity of human error. The data center reads the proxy configuration only during the data center bootstrap time--either during the Cisco APIC or the data center upgrade time. The Cisco APIC auto-populates the configuration under the following conditions:

- If there is no proxy is configured in the data center, the Cisco APIC reads from the license manager during the data center bootstrap time as a result of a Cisco APIC or data center upgrade, and populates the proxy information from the smart license configuration.
- The data center will not monitor for any configuration changes from the Cisco APIC or smart license.
- Any changes made to the smart license proxy configuration after the data center bootstrap is complete are not reflected in the data center. If the data center is not able to communicate with Cisco Intersight, there will be an appropriate alert raised in the GUI.
- If configuration is already present in the data center as a result of pre-populating the configuration from the smart license or user configuration, the data center will not use the configuration from smart license on the next bootstrap time.
- Even though proxy information is pre-populated in the data center, inventory sharing with the Cisco APIC is still controlled from Cisco Network Insights Advisor.
- The data center cannot pre-populate the proxy authentication configuration (username/password) if the proxy server requires authentication, because this information is not available from the smart license.

The data center reads the proxy configuration from the licenseLicPolicy managed object and only populates the configuration if the mode is set to **proxy**.

Disabling the Data Center HTTP or HTTPS Proxy Configuration Auto-Population

If you do not want to share the Cisco Application Policy Infrastructure Controller (APIC) inventory with Cisco, you can disable the proxy configuration in the Cisco APIC, which also disables the proxy configuration auto-population feature.

Note These procedures apply for releases prior to release 5.2(1). For release 5.2(1) or later, the proxy configurations are no longer configured within the **Intersight - Device Connector** pages. Instead, these settings are configured in this centralized area in APIC:

System > **System Settings** > **Proxy Policy**

Procedure

Step 1 In the Cisco APIC, on the menu bar, choose **System** > **System Settings**.

Step 2 In the Navigation pane, choose **Intersight.**

Step 3 In the Work pane, click **Settings** > **Proxy Configuration**.

Step 4 Click the **Enable Proxy** slider to disable it. The slider will move to the left side and the slider's background will turn gray.

Step 5 Click **Save**.

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS REFERENCED IN THIS DOCUMENTATION ARE SUBJECT TO CHANGE WITHOUT NOTICE. EXCEPT AS MAY OTHERWISE BE AGREED BY CISCO IN WRITING, ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS DOCUMENTATION ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED.

The Cisco End User License Agreement and any supplemental license terms govern your use of any Cisco software, including this product documentation, and are located at: http://www.cisco.com/go/softwareterms.Cisco product warranty information is available at http://www.cisco.com/go/warranty. US Federal Communications Commission Notices are found here http://www.cisco.com/c/en/us/products/us-fcc-notice.html.

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 products and features described herein as in development or available at a future date remain in varying stages of development and will be offered on a when-and if-available basis. Any such product or feature roadmaps are subject to change at the sole discretion of Cisco and Cisco will have no liability for delay in the delivery or failure to deliver any products or feature roadmap items that may be set forth in this document.

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.

The documentation set for this product strives to use bias-free language. For the purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

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: 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. (1721R)

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

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

Europe Headquarters
CiscoSystemsInternationalBV
Amsterdam,TheNetherlands

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