Working with Cisco Intersight, Release 4.2.1

Table of Contents

New and changed information

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

Release Version	Feature	Description
Nexus Dashboard 4.2.1	There were no major changes from the previous release.	

Working with Cisco Intersight

Cisco Intersight, a Software-as-a-Service (SaaS) infrastructure management platform, integrates with other intelligent systems to enhance its capabilities. It enables you to manage the Cisco Unified Computing System (Cisco UCS), Cisco Hyperconverged Infrastructure Solutions, Cisco APIC, and other platforms, including Nexus Dashboard, on a global scale.

Data center apps, such as Cisco Nexus Dashboard Insights, connect to the Cisco Intersight portal through a Device Connector that is embedded in the management controller of each system, in this case your Nexus Dashboard. 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 Cisco Intersight. For more information on the **Auto Update** option, see Configure Device Connector settings.

For additional information on Cisco Intersight, see https://www.intersight.com/help/saas/getting_started/overview.

Guidelines and limitations

- Nexus Dashboard is compatible with Intersight SaaS, but Intersight Connected Virtual Appliance (CVA) is not supported with the Nexus Dashboard.
- Nexus Dashboard does not require additional licensing to claim Nexus Dashboard on Intersight. The Intersight account used to claim Nexus Dashboard license should also be registered with Smart Licensing. Please follow Cisco Intersight Help Center documentation for instructions on how to register Intersight with Cisco Smart Software Manager.

Configure Device Connector settings

Devices are connected to the Cisco Intersight portal through a Device Connector, which provides a secure way for the connected devices to send information and receive control instructions from the Cisco Intersight portal.

All device connectors must properly resolve svc.intersight.com and allow outbound initiated HTTPS connections on port 443. If a proxy is required for an HTTPS connection, you must configure the proxy settings in your Nexus Dashboard.

> The Device Connector relies on Nexus Dashboard proxy settings to connect to Cisco Intersight. If these proxy settings change (for example, during a Nexus Dashboard configuration restore) the connection to Cisco Intersight may be interrupted.

Follow these steps to configure the basic Device Connector settings.

1. Navigate to the **Intersight Device Connector** page.

   Go to **Admin > Intersight**.

2. In the top right of the **Intersight Device Connector** page, click **Settings**.
3. Click the **General** tab to configure basic options.
   a. Use the **Device Connector** knob to enable or disable the Device Connector.

      This enables you to claim the device and leverage the capabilities of Intersight. If it is disabled, no communication is allowed to Cisco Intersight.

   b. In the **Access Mode** area, choose whether to allow Intersight the capability to make changes to this device.

      - Allow Control (default)—enables you to perform full read or write operations from the cloud based on the features available in Cisco Intersight.
      - Read-only—ensures that no changes are made to this device from Cisco Intersight.

        For example, actions such as upgrading firmware or a profile deployment will not be allowed in read-only mode. However, the actions depend on the features available for a particular system.

   c. Use the **Auto Update** knob to enable automatic Device Connector updates.

      We recommend that you enable automatic updates so that the system automatically updates the Device Connector software. When enabled, the Device Connector will automatically upgrade its image whenever there is any upgrade push from Intersight.

      If you disable the automatic updates, you will be asked to manually update the software when new releases become available. Note that if the Device Connector is out-of-date, it may be unable to connect to Cisco Intersight.

4. Click **Save** to save the changes.
5. Click the **Certificate Manager** tab if you want to import additional certificates.

   By default, the device connector trusts only the built-in certificate. If the device connector establishes a TLS connection and a server sends a certificate that does not match the built-in certificate, the device connector terminates TLS connections because it cannot determine if the server is a trusted device.

   You can choose to upload additional certificates by clicking the **Import** button in this screen. 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.

   You can click the **View** icon at the end of the certificate's row to view its details such as name, issue and expiration dates.

Claim targets

This section describes how to claim the Nexus Dashboard platform as a device for Cisco Intersight.

Before you begin

You must have configured the Intersight Device Connector as described in Configure Device Connector settings.

To claim the device:

1. From the main navigation menu, click **Admin > Intersight**.
2. Check whether the Device Connector is already configured.
   - If you see a green dotted line connecting **Internet** to **Intersight** in the **Device Connector** page and the text **Claimed**, then your Intersight Device Connector is already configured and connected to the Intersight cloud service, and the device is claimed. In this case, you can skip the rest of this section.
   - If you see a red dotted line connecting to **Internet** in the **Device Connector** page, you must configure a proxy for your Nexus Dashboard cluster to be able to access the Internet, as described in Working with System Settings before continuing with the rest of this section.
   - If you see a yellow dotted line and a caution icon connecting **Internet** to **Intersight** in the **Device Connector** page and the text **Not Claimed**, 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 cloud service, and claim the device. In this case, proceed with the rest of the steps to configure the device.
3. If necessary, update the device connector software.

   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 at the top of the screen informing you that Device Connector has important updates available. Enabling the auto-update feature is described in Configure Device Connector settings.

   To manually update the Device Connector, click the **Update Now** link.
4. Note down the Device ID and Claim Code listed on the Nexus Dashboard's **Intersight** page.
5. Log into the Cisco Intersight cloud fabric at https://www.intersight.com.
6. Follow the instructions described in the Claim Targets section of the Intersight documentation to claim the device.

   After the device is claimed in Intersight, you should see green dotted lines connecting **Internet** to **Intersight** in your Nexus Dashboard's **Device Connector** page along with the text **Claimed**.

   > You may need to click **Refresh** in top right of the page to update the latest status.

Unclaiming the device

To unclaim the Nexus Dashboard as a device from Intersight:

1. From the main navigation menu, click **Admin > Intersight**.
2. In the main pane, click **Unclaim**.

Copyright

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.

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: https://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)

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

USA
https://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883