Cisco Intersight Nexus Dashboard Base User Guide

Table of Contents

New and Changed Information . . . 3
Cisco Intersight Nexus Dashboard Base Overview . . . 4
About Cisco Intersight Nexus Dashboard Base . . . 4
Setting Up the Device Connector . . . 5
About Device Connector . . . 5
Configuring Smart Licensing . . . 5
Configuring the Intersight Device Connector on Cisco APIC . . . 6
Configuring the Intersight Device Connector on Cisco DCNM . . . 10
Configuring Device Connector Settings on Cisco Nexus Dashboard . . . 13
Target Claim . . . 13
Cisco Intersight Nexus Dashboard Base . . . 14
Cisco Intersight Nexus Dashboard Base Dashboard . . . 14
Viewing sites on Cisco Intersight Nexus Dashboard Base Dashboard . . . 15
Viewing Nexus Dashboards on Cisco Intersight Nexus Dashboard Base Dashboard . . . 16
Viewing Storage Networking on Cisco Intersight Nexus Dashboard Base Dashboard . . . 19

First Published: 2020-12-17

Last Modified: 2022-02-03

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

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

Feature	Description
Storage Networking	This feature enables you to view Cisco DCNM (SAN) and Cisco Nexus Dashboard Fabric Controller (SAN) inventory in your network.
Cisco Nexus Dashboard Services inventory	This feature enables you to view Nexus Dashboard Services inventory in your network.
Cisco Nexus Dashboard inventory	This feature enables you to view Nexus Dashboard inventory in your network.
Cisco Intersight Nexus Dashboard Base	The first release of this document was published.

Cisco Intersight Nexus Dashboard Base Overview

About Cisco Intersight Nexus Dashboard Base

Cisco Intersight Nexus Dashboard Base offers customers basic data center network asset, inventory, and status information in the Intersight portal. It provides customers a single, high level view of your Cisco Nexus infrastructure health. The consolidated view supports consistency and compliance checks and makes it easier to prevent administrative lapses in expiry of support contracts.

These benefits and business outcomes are made possible through a pre-packaged Cisco Nexus Insights Cloud Connector that comes with the Cisco data center network controllers such as Cisco APIC and Cisco DCNM. It is also included in Cisco Nexus Dashboard, a common platform for hosting services such Cisco Nexus Dashboard Insights, Cisco Nexus Dashboard Orchestrator, and Cisco Nexus Dashboard Fabric Controller.

The Cisco Nexus Insights Cloud Connector provides the added benefit of faster time to remediation with a Cisco TAC assist feature. Customers can automate the collection and secure upload of tech-support logs to the Cisco cloud.

TAC assist feature is not supported for Cisco DCNM SAN.

All product usage telemetry data is transmitted securely through an encrypted channel. The data collected is limited to product usage, and no personally identifiable information or network traffic data is collected or processed. For more information, see Cisco Nexus Dashboard Insights Data Sheet.

Setting Up the Device Connector

About Device Connector

Devices are connected to the Cisco 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.

Configuring Smart Licensing

Cisco Intersight Nexus Dashboard Base also 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 Intersight Nexus Dashboard Base UI alerts you that the Device Connector is disconnected and allows you to update the smart license.

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 Intersight Nexus Dashboard Base 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 Intersight Nexus Dashboard Base 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 on Cisco APIC

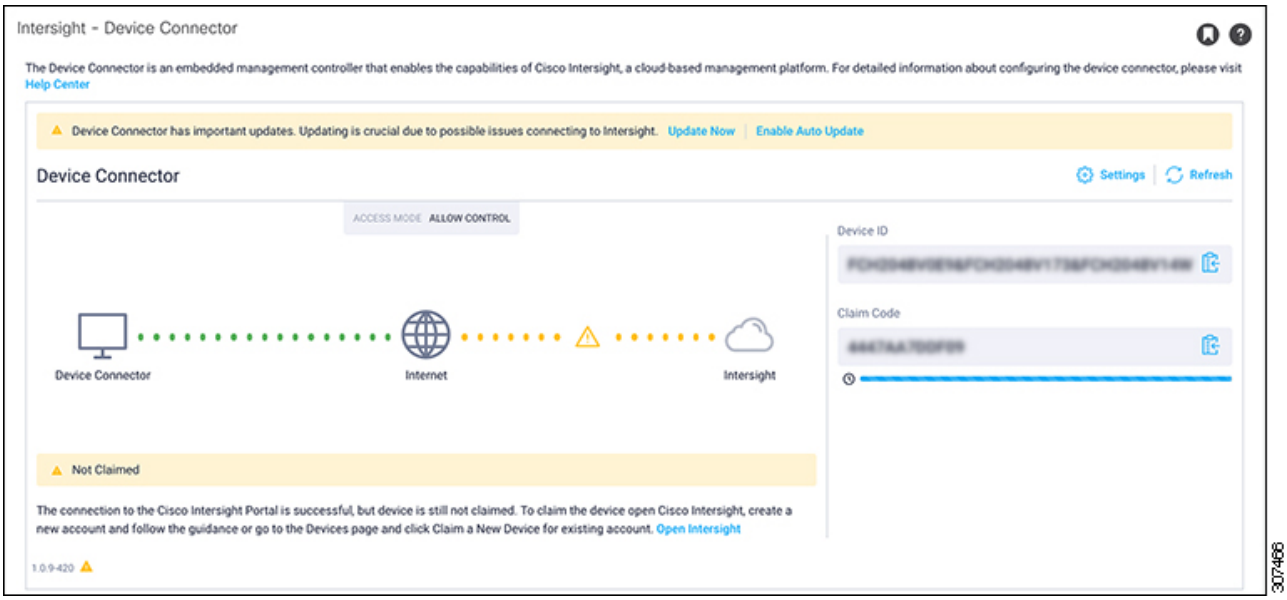
Cisco Intersight Nexus Dashboard Base is connected to the Cisco Intersight Cloud portal through a Device Connector which is embedded in the management controller of the Cisco APIC platform.

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 Intersight Nexus Dashboard 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

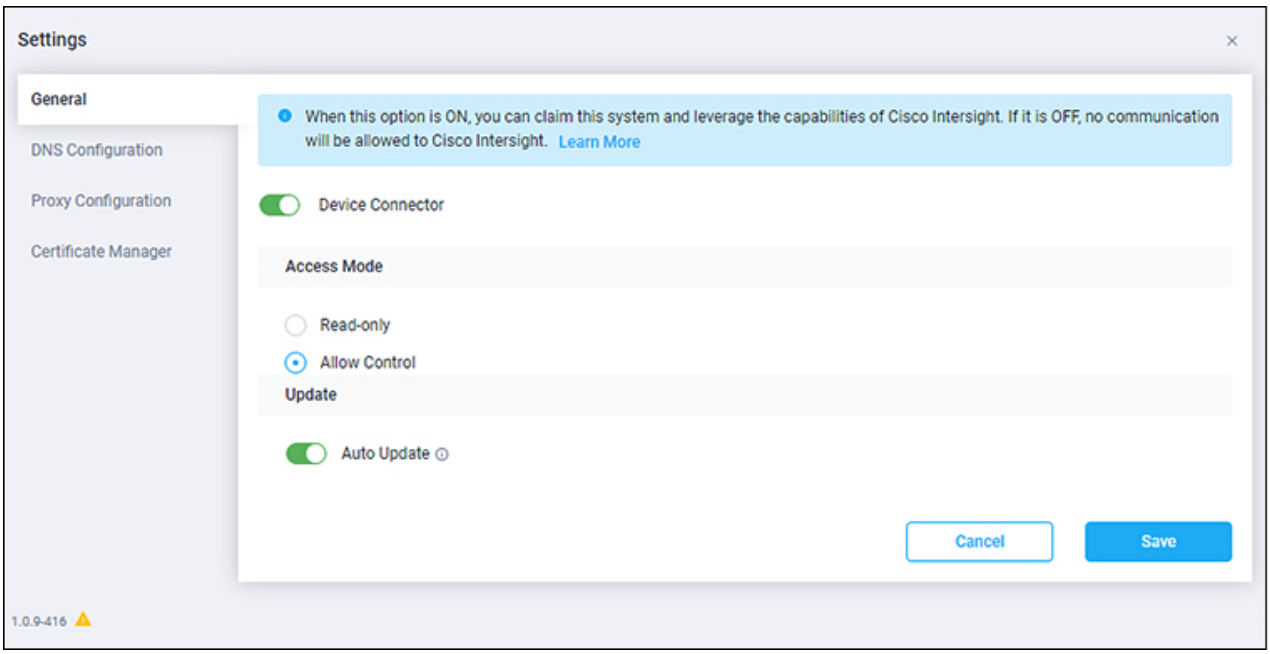
Connector software version available.

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.

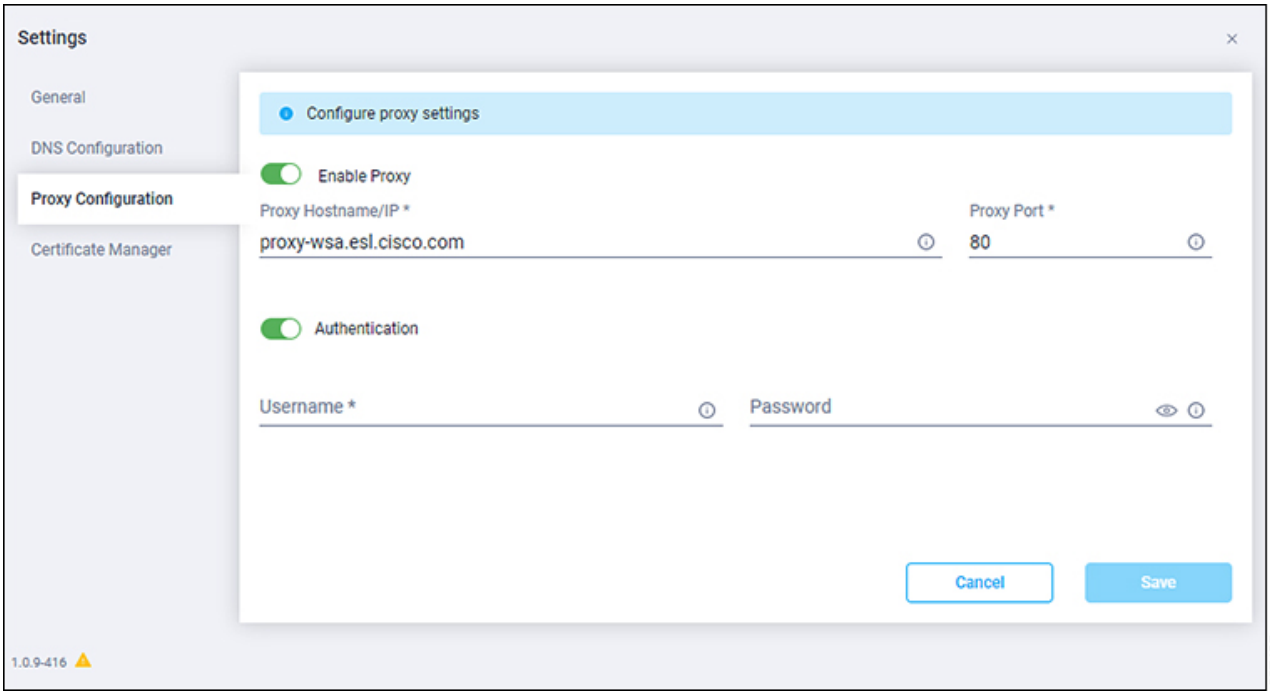
5. When you have completed the configurations in the **General** page, click **Save**.

   The **Intersight - Device Connector** overview pages appears again. At this point, you can make or verify several configure settings for the Intersight Device Connnector:

   - 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.

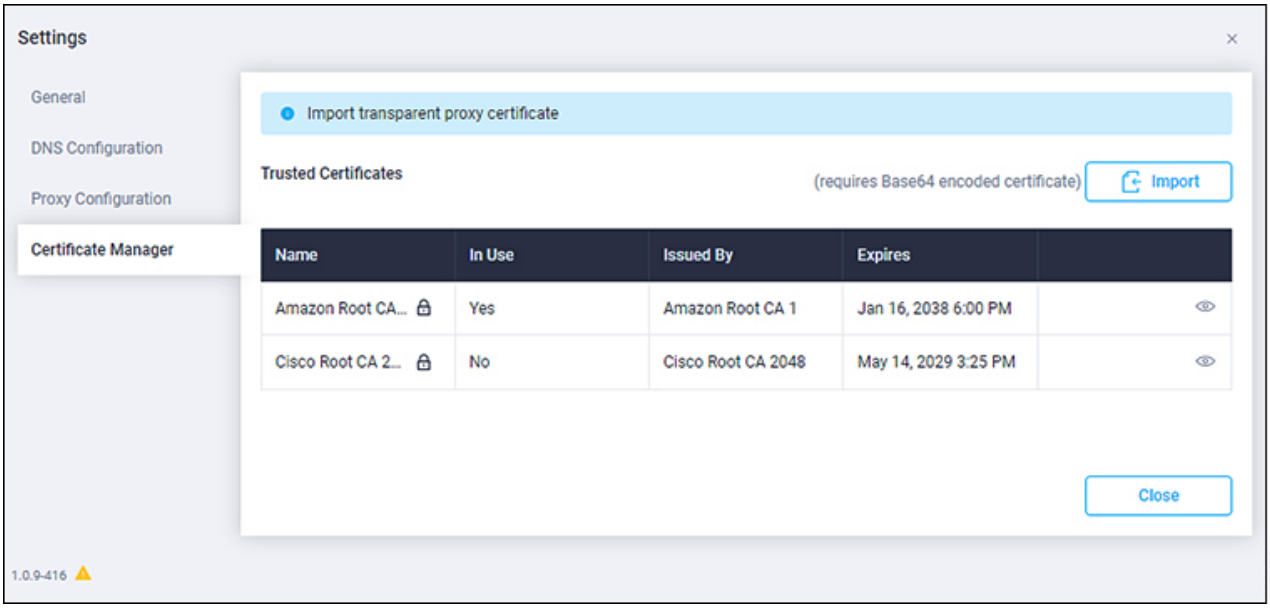
8. When you have completed the configurations in the **Proxy Configuration** page, click **Save**.

   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**.

See the Target Claim to claim a new target.

Configuring the Intersight Device Connector on Cisco DCNM

Cisco Intersight Nexus Dashboard Base is connected to the Cisco Intersight Cloud portal through a

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

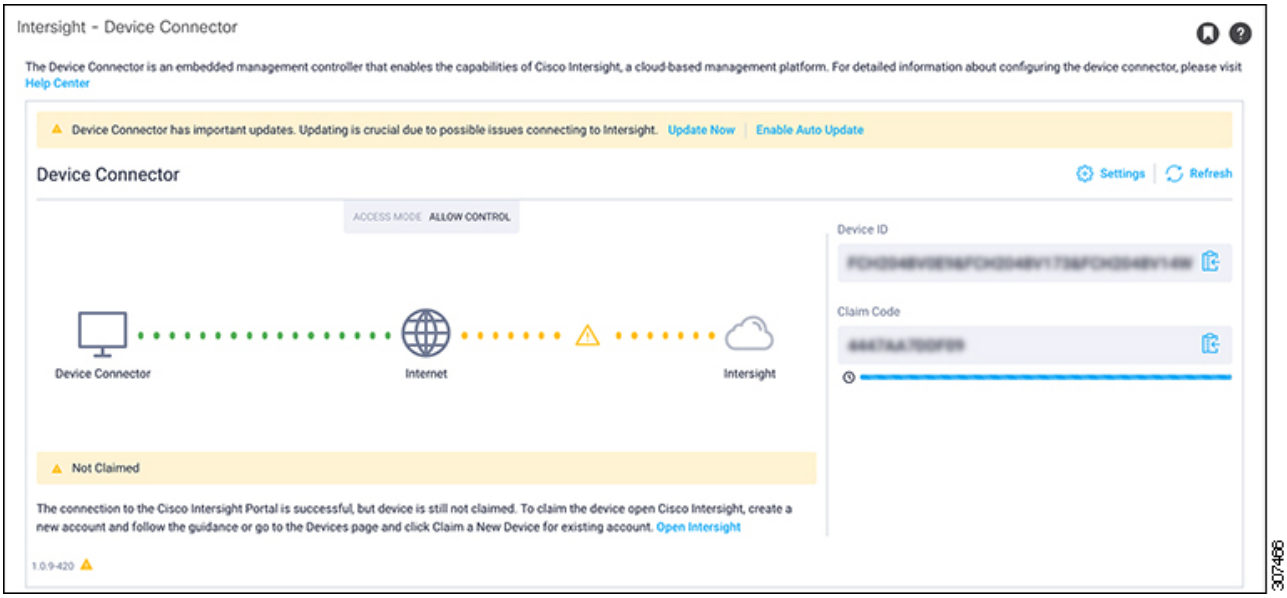
Cisco Intersight is a management platform delivered as a service. Cisco DCNM platform has a Device Connector that is packaged with the software that connects to Cisco Intersight Cloud. Device Connector is used to provide Cisco Intersight Nexus Dashboard Base Cloud connectivity feature sets.

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:

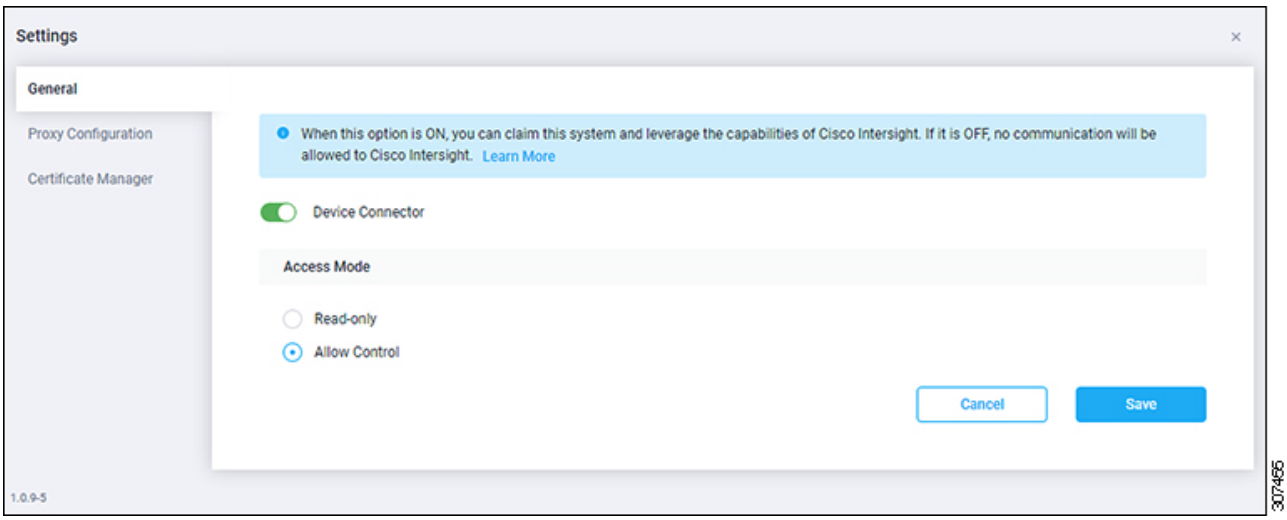
1. On the Cisco DCNM navigation pane, click Administration.
2. Under the Cisco DCNM Server list, click Device Connector.

   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.

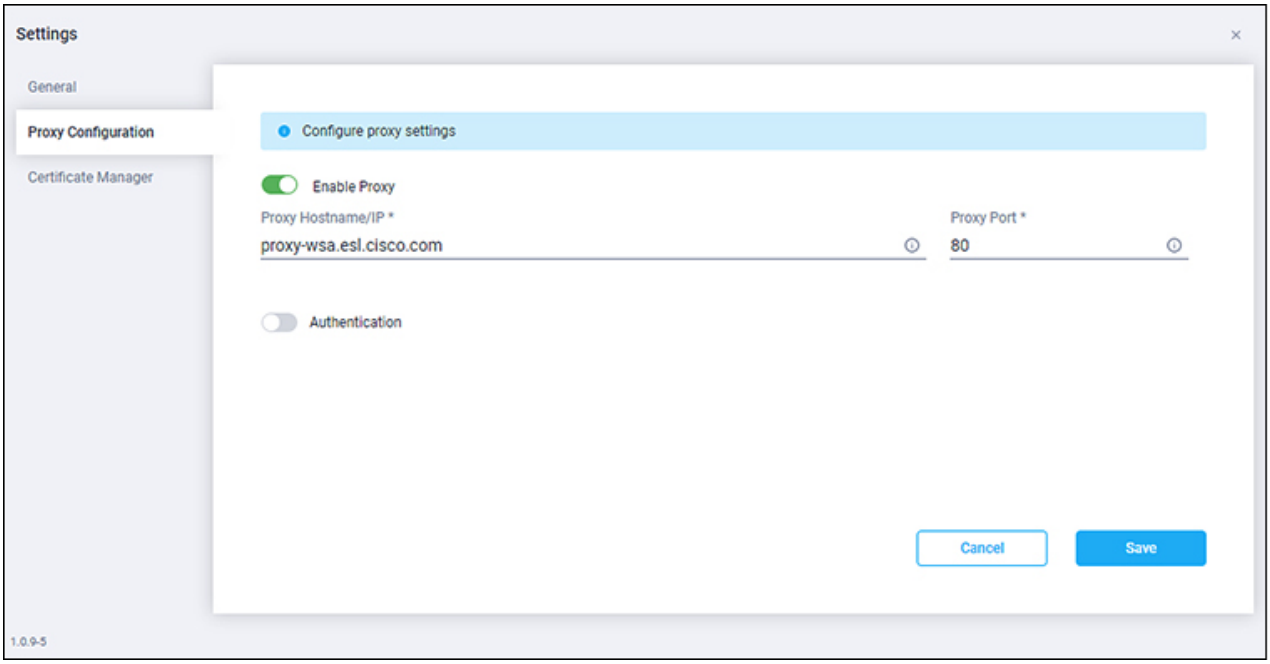
Access Mode

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**.

See the Target Claim to claim a new target.

Configuring Device Connector Settings on Cisco Nexus Dashboard

See Cisco Nexus Dashboard User Guide, section *Configuring Device Connector Settings* for more information.

Target Claim

Before you begin

You have configured Intersight Device Connector in Cisco APIC and Cisco DCNM.

Procedure

See Target Claim for more information.

Cisco Intersight Nexus Dashboard Base

Cisco Intersight Nexus Dashboard Base Dashboard

The Cisco Intersight Nexus Dashboard Base dashboard on Cisco Intersight enables you to view all your data center networking inventory. It provides immediate access to a high-level view of the data center platforms such as Cisco APIC, Cisco DCNM, and Cisco Nexus Dashboard in your network.

The summary view on the dashboard displays a graphical information about the sites and Cisco Nexus Dashboards in your network.

Sites

The **Sites** tab displays information about the sites such as Cisco APIC, Cisco DCNM (LAN or SAN), Cisco Nexus Dashboard Fabric Controller (NDFC) (LAN or SAN) and the sites onboarded to Cisco Nexus Dashboard. The information displayed includes type, status, and firmware versions. The Details Table displays information about the site such as name, status, type, IP address, firmware version, nodes, and organization.

You can use the search functionality to search for attributes and export the search results to a CSV file.

In the Inventory page you can view the summary and detailed information of the controllers, switches, and licenses in your network. You can also view the port information for a specific switch.

Nexus Dashboards

The **Nexus Dashboards** tab displays information about the Cisco Nexus Dashboards and services in your network.

The information displayed includes health, type, and firmware versions. The Details Table displays information such as name, health, cluster size, type, version, sites, and services.

You can use the search functionality to search for attributes and export the search results to a CSV file.

In the Inventory page you can view the summary and detailed information of the nodes, sites, and services in your network.

Storage Networking

The **Storage Networking** tab displays information about the sites such as Cisco DCNM (SAN) and Cisco NDFC (SAN) and the sites onboarded to Cisco Nexus Dashboard. The information displayed includes type and firmware versions. The Details Table displays information about the site such as name, status, type, Nexus Dashboard, IP address, firmware version, nodes, and organization.

You can use the search functionality to search for attributes and export the search results to a CSV file.

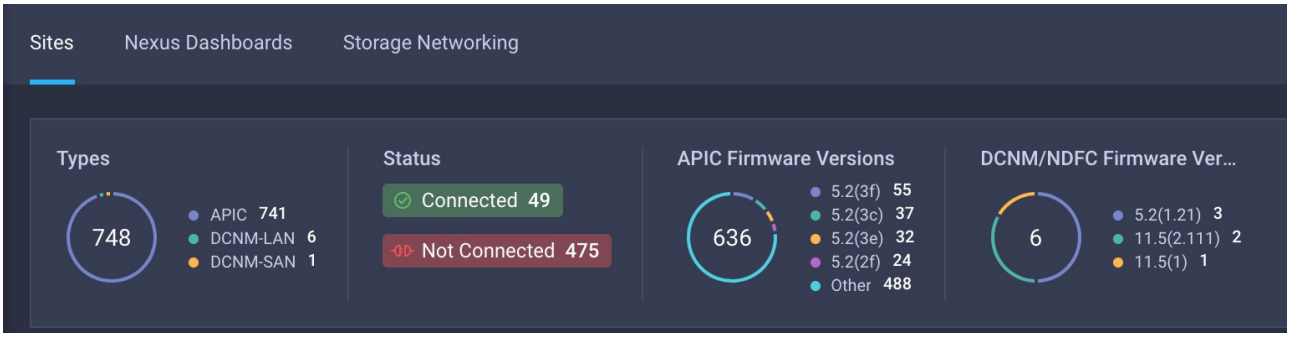
In the Inventory page you can view the summary and detailed information of the controllers, switches, and licenses in your network. You can also view the port information for a specific switch.

Viewing sites on Cisco Intersight Nexus Dashboard Base Dashboard

Use this procedure to view inventory of sites in your network.

Procedure

1. Log in to Cisco Intersight as a user with System Administrator role.
2. Choose **OPERATE** > **Networking**> **Sites**.
3. Cisco Intersight Nexus Dashboard Base dashboard on Cisco Intersight is displayed. The summary view on top of the page displays a graphical information about the Cisco APIC or Cisco DCNM or Cisco NDFC sites in your network. The information displayed includes type, status, and firmware versions.

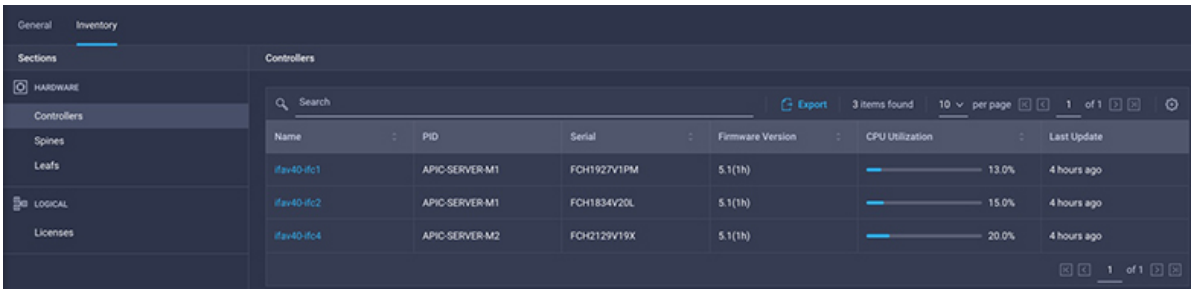


4. Click a specific type, status, and firmware version to view additional details on the Details Table below. The Details Table displays information about the site such as name, status, type, Nexus Dashboard, IP address, firmware version, and nodes.

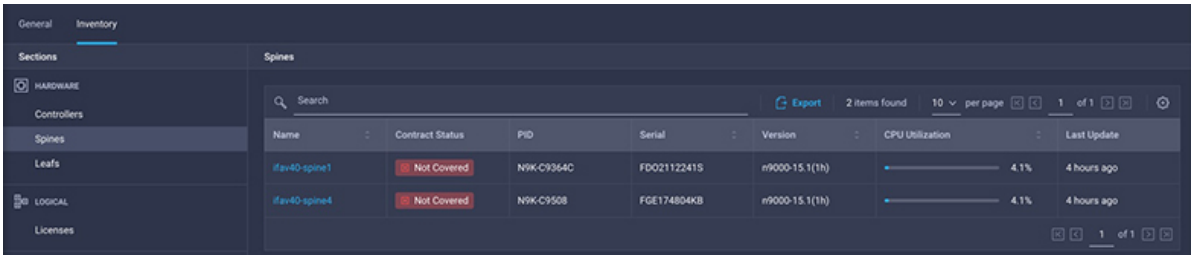
   The Type column lists the site types such as APIC, DCNM-LAN, DCNM-SAN, NDFC-LAN, and NDFC-SAN. The Nexus Dashboard column lists the cluster name of Nexus Dashboard corresponding to the site.

   a. Click the **Search** field and from the drop-down list select the attributes to search for. The search results are displayed in the Details Table.
   b. Click **Export** to export the search results to a CSV file.
   c. Click **Settings** icon to customize the columns and choose which columns to display. You can filter and sort on each column.
   d. Hover on the status icon next to the name of the site to view the connection status.
5. In the Details Table, click name to view detailed information of the specific site.
   a. Click **General** tab to view details such as status, name, type, and firmware version. The summary view of controllers, switches, and licenses are also displayed.
   b. Click **Inventory** tab to view detailed view of controllers, switches, and licenses in a tabular format. For Cisco APIC sites, detailed view of leaf switch and spine switch is displayed.

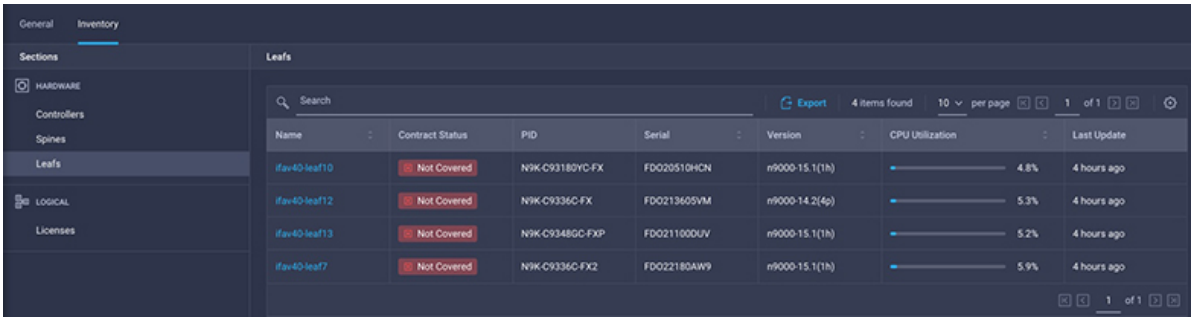
i. The Details Table for controllers displays information such as name, PID, serial number, firmware version, CPU utilization and the last update for telemetry data. Click a specific controller name to view additional details.



ii. The Details Table for spine switches displays information such as name, contract status, PID, serial number, version, CPU utilization and the last update for telemetry data. Click a specific spine switch name to view additional details.



iii. The Details Table for leaf switches displays information such as name, contract status, PID, serial number, version, CPU utilization and the last update for telemetry data. Click a specific leaf switch name to view additional details.



iv. Click a specific switch name to view port information. In the switch page, click **Ports** to view port information such as number of interfaces present, operational status, and if the transceiver is present in the interfaces.

v. The Details Table for licenses displays information such as license, node, PID, and the last update for telemetry data. Click a specific node name to view additional details.

c. Click the **Search** field and from the drop-down list select the attributes to search for.

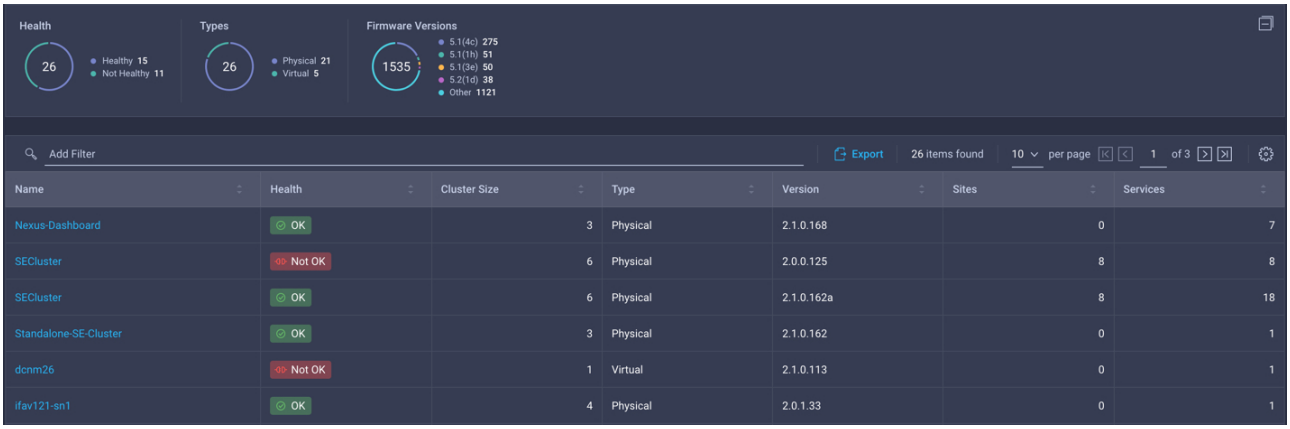
d. Click **Export** to export the inventory results as a CSV file.

Viewing Nexus Dashboards on Cisco Intersight Nexus Dashboard Base Dashboard

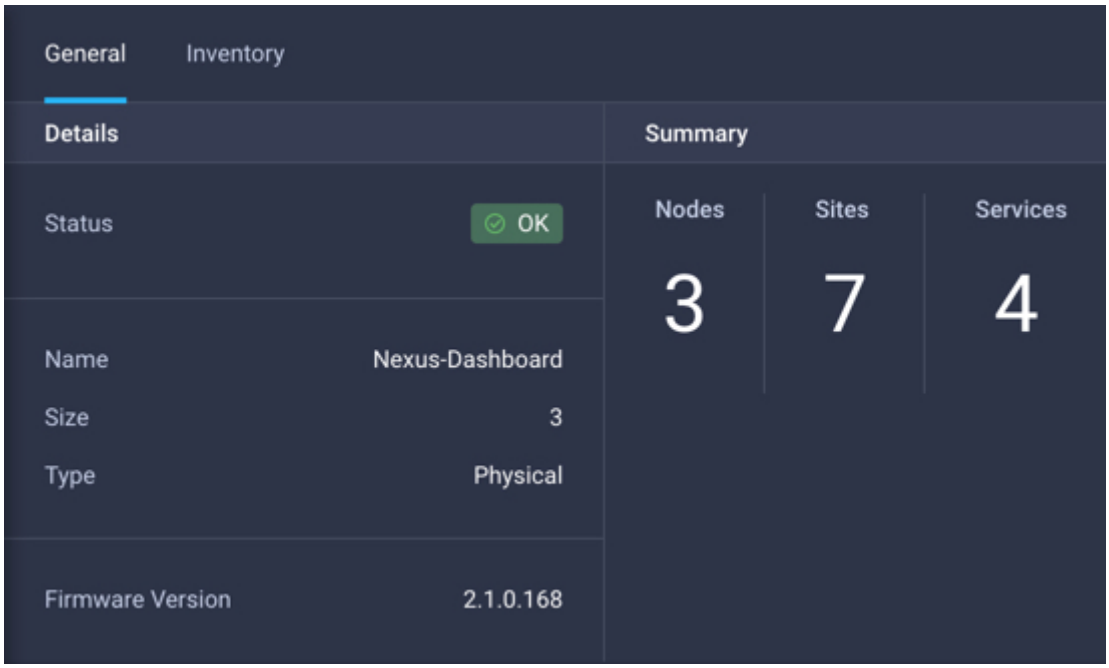
Use this procedure to view inventory of Nexus Dashboards and services in your network.

Procedure

1. Log in to Cisco Intersight as a user with System Administrator role.
2. Choose **OPERATE** > **Networking**> **Nexus Dashboards**.
3. Cisco Intersight Nexus Dashboard Base dashboard on Cisco Intersight is displayed. The summary view on top of the page displays a graphical information about the Nexus Dashboards in your network. The information displayed includes health, type, and firmware versions.

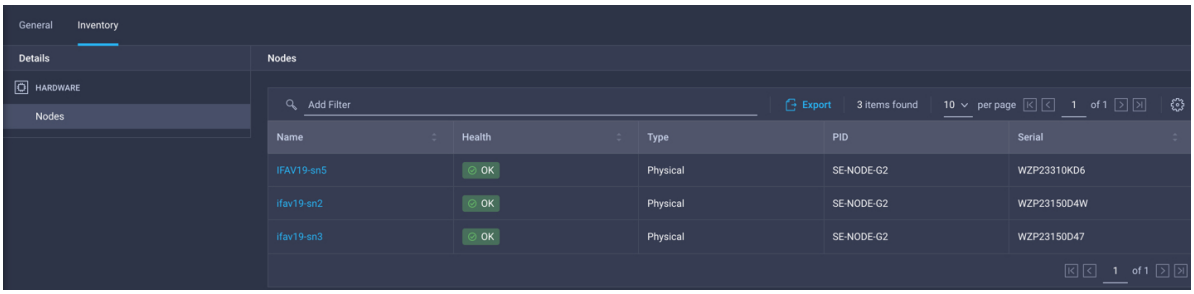


4. Click a specific type, status, and firmware version to view additional details on the Details Table below. The Details Table displays information about the Nexus Dashboard such as name, health, cluster size, type, version, sites, and services.
    a. Click the **Search** field and from the drop-down list select the attributes to search for. The search results are displayed in the Details Table.
    b. Click **Export** to export the search results to a CSV file.
    c. Click **Settings** icon to customize the columns and choose which columns to display.
5. In the Details Table, click name to view detailed information.
    a. Click **General** tab to view details such as status, name, size, type, and firmware version. The summary view of nodes, sites, and services are also displayed.

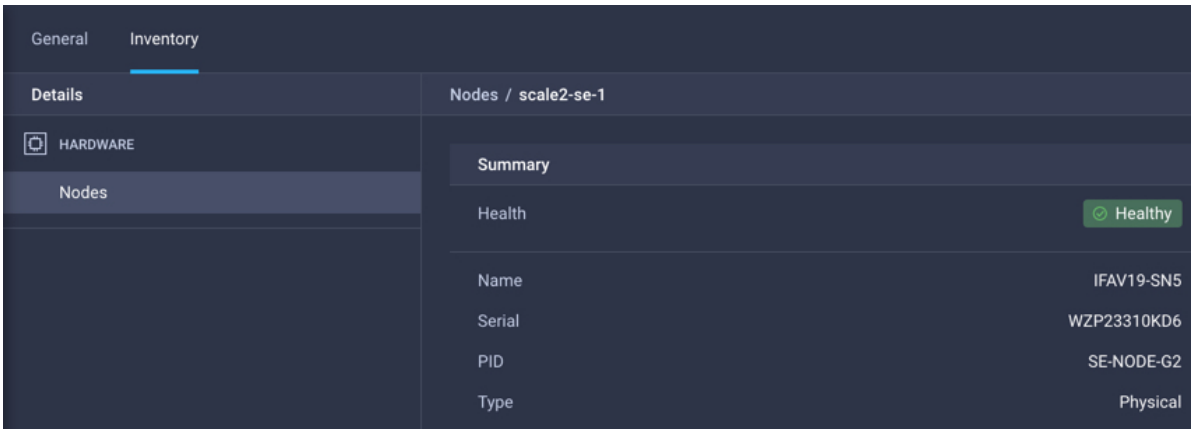


b. Click **Inventory** tab to view detailed view of nodes, sites, and services in a tabular format.

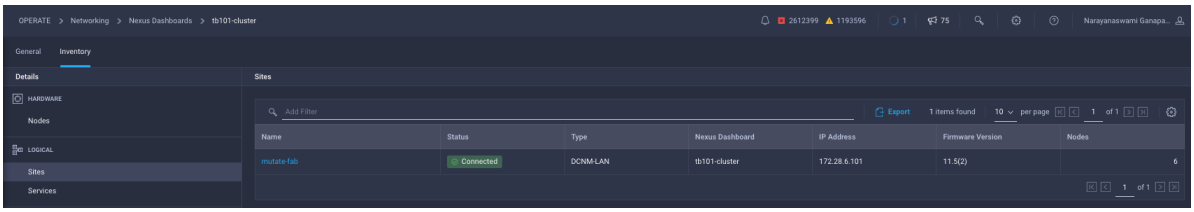
   i. The Details Table for nodes displays information such as name, health, type, PID, and serial number.



   ii. Click a specific node name to view additional details about the node.

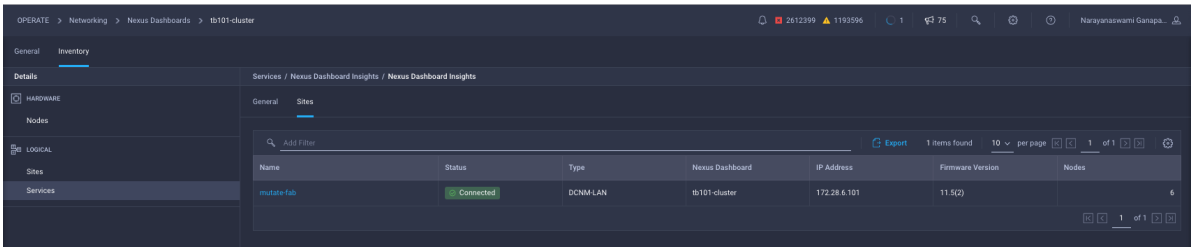


   iii. The Details Table for sites displays information such as name, status, type, Nexus Dashboard, IP address, firmware version, and nodes. The sites displayed are the sites onboarded on to Cisco Nexus Dashboard.



   iv. Click a specific site to view additional details.

   v. The Details Table for services displays information such as type, status, Nexus Dashboard, app version, and number of sites onboarded on to Cisco Nexus Dashboard and added to the service.



   vi. Click a specific service to view additional details.

c. Click the **Search** field and from the drop-down list select the attributes to search for.

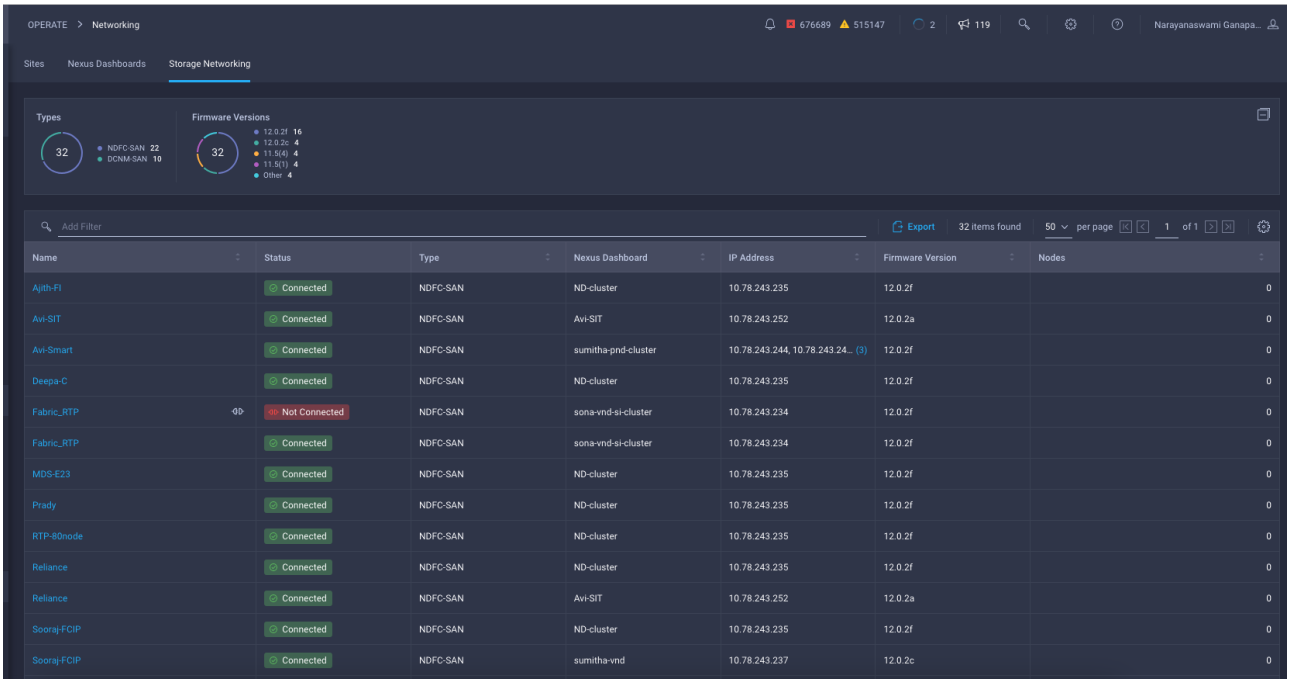
d. Click **Export** to export the inventory results as a CSV file.

Viewing Storage Networking on Cisco Intersight Nexus Dashboard Base Dashboard

Use this procedure to view inventory of Cisco DCNM (SAN) and Cisco NDFC (SAN) in your network.

Procedure

1. Log in to Cisco Intersight as a user with System Administrator role.
2. Choose **OPERATE** > **Networking**> **Storage Networking**.
3. Cisco Intersight Nexus Dashboard Base dashboard on Cisco Intersight is displayed. The summary view on top of the page displays a graphical information about the Cisco DCNM (SAN) and Cisco NDFC (SAN) sites in your network. The information displayed includes type and firmware versions.



4. Click a specific type and firmware version to view additional details on the Details Table below. The Details Table displays information about the site such as name, status, type, Nexus Dashboard, IP address, firmware version, and nodes.

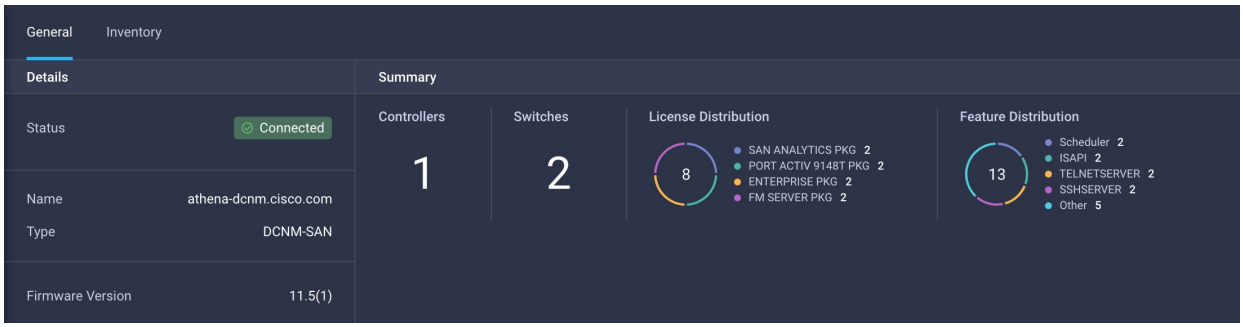
   The Type column lists the site types such as DCNM-LAN, DCNM-SAN, NDFC-LAN, and NDFC-SAN. The Nexus Dashboard column lists the cluster name of Nexus Dashboard corresponding to the site.

   a. Click the **Search** field and from the drop-down list select the attributes to search for. The search results are displayed in the Details Table.
   b. Click **Export** to export the search results to a CSV file.
   c. Click **Settings** icon to customize the columns and choose which columns to display. You can filter and sort on each column.

d. Hover on the status icon next to the name of the site to view the connection status.

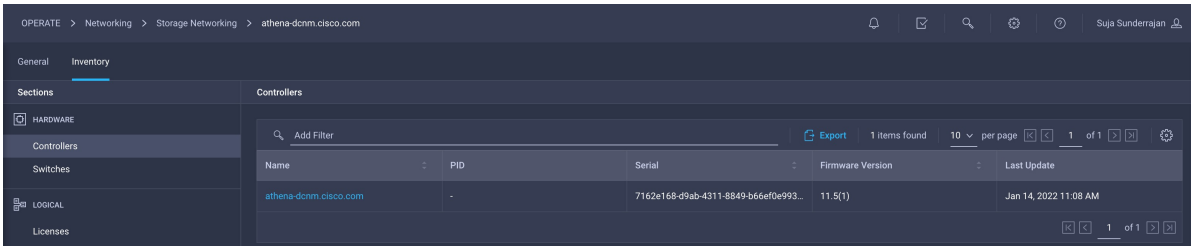
5. In the Details Table, click name to view detailed information of the specific site.

   a. Click **General** tab to view details such as status, name, type, and firmware version. The summary view of controllers, switches, licenses, and feature distribution are also displayed.

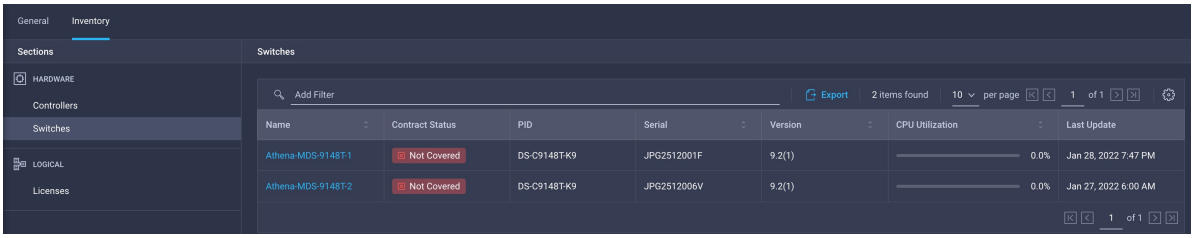


   b. Click **Inventory** tab to view detailed view of controllers, switches, licenses, and feature distribution in a tabular format.

      i. The Details Table for controllers displays information such as name, PID, serial number, firmware version, and the last update for telemetry data. Click a specific controller name to view additional details.



      ii. The Details Table for switches displays information such as name, contract status, PID, serial number, version, CPU utilization and the last update for telemetry data. Click a specific switch name to view additional details.



      iii. Click a specific switch name to view port information. In the switch page, click **Ports** to view port information such as number of interfaces present, operational status, and if the transceiver is present in the interfaces.

      iv. The Details Table for licenses displays information such as license, node, PID, and the last update for telemetry data. Click a specific node name to view additional details.

   c. Click the **Search** field and from the drop-down list select the attributes to search for.

   d. Click **Export** to export the inventory results as a CSV file.