

Devices

This chapter has details about the devices of the Cisco Nexus Dashboard Data Broker.

Beginning with Release 3.10.1, Cisco Nexus Data Broker (NDB) has been renamed to Cisco Nexus Dashboard Data Broker. However, some instances of NDB are present in this document, to correspond with the GUI, and installation folder structure. References of NDB/ Nexus Data Broker/ Nexus Dashboard Data Broker, can be used interchangeably.

- Devices, on page 1

Devices

The **Devices** tab has the following sub tabs:

- **NDB Devices**—aggregation devices managed by the NDB controller. See NDB Devices for more details.
- **Span Devices**— Switches (Nexus/ Catalyst) and controllers (Cisco APIC/ Cisco DNAC) connected to NDB. See Span Devices, on page 14 for more details.
- **Tap Devices** —tap devices connected to the NDB controller. See Tap Devices for more details.
- **Device Groups**—the groups to which the NDB devices are segregated into. See Device Groups for more details.

NDB Devices

The **NDB Devices** tab displays details of all the devices connected to the NDB controller.

A table is displayed with the following details:

Table 1: NDB Devices

Column Name	Description
Status (the first column of the table)	The current status of the device connected to the NDB; indicated by color. The options are: • Green—indicates that the device is operational and connected to the NDB controller. • Red—indicates failure and the device is not connected to the NDB controller. • Yellow—indicates that the device is connected but not ready yet. Reboot the device and wait for a few minutes for the status to turn green. Refresh and check. • Gray—indicates that the device is in maintenance mode.

Column Name	Description
IP Address	The IP address of the device. This field is a hyperlink. Click the IP address to view more details of the device. Click the **IP Address**. A new pane is displayed on the right which has more information about the device. Additional actions that can be performed from here are: • Edit Device • Take Device Offline • Edit Global Configuration **Note** The *Take Device Offline* action is generally grayed out and is available only for devices in maintenance mode. You can also view the **Ports**, **Port Channels** and **Port Groups** of the device by clicking the corresponding tab. For more information about Port Channels and Groups, see Port Channels and Groups. Click the **Details** icon () to get additional details of the device. A new window displays the following details for the selected device: • General • Ports • Port Channel • Port Groups • Global Configuration • Monitor Sessions • Flow Statistics • Port Statistics • TCAM Resource Utilization Additional actions that can be performed from **Details** tab: • Trigger Global ACLs—this action identifies the non-configured interfaces of a device and attaches global ACLs to all these interfaces. It is mandatory for all interfaces of a device to be configured with global ACLs. • Add Port Channel

Column Name	Description
Device Name	The device name (switch name) as indicated by the administrator while configuring the device. Device name is displayed only if the device status is green. If the status of the device is red or yellow, the device name is not displayed.
Platform	The device platform.
Node ID	The node ID of the device.
Profile Name	The profile of the device as configured during device addition.
NX-OS	The software version currently running on the device.
Mode	The mode the switch is currently using. The options are: • NDB mode—indicates that the whole switch (all interfaces) is managed by the NDB controller. • Hybrid—indicates that only some interfaces in the device are managed by the NDB controller. **Note** By default, this column is hidden. When Hybrid mode is enabled on the device during device addition, this column is displayed.
Port	The port used by the NDB controller to communicate to the NDB device.
Status Description	The status of the connection between the NDB device and the NDB controller. The options are: • Connection succeeded—indicates that the connection between the device and NDB controller is successful. • Connection failed—indicates that the connection between the device and NDB controller has failed. A reason for failure is also displayed, such as authentication failed, connection refused (incorrect port). • Connection not ready—indicates that the device reload was not successful.

The following actions can be performed from the **NDB Devices** tab:

- **Add Device**—Use this to add a new device. See Adding a Device for details.
- **Rediscover Device**—Select the required device by checking the check box at the beginning of the row. Click **Actions** > **Rediscover Device(s)**. A pop-up appears. Click **Rediscover** to rediscover the selected devices. When you rediscover devices, the global ACLs are reattached.

Note Rediscovering a device leads to UDF, ports, global and connections reconfigurations and this results in traffic loss.

When there is a configuration error, use rediscover to reconfigure the device.

If you choose the rediscover action without selecting a check box, an error is displayed. You will be prompted to select a device.

- **Reconnect Device**— Select the required device by checking the check box at the beginning of the row. Click **Actions** > **Reconnect Device(s)**. A pop-up appears. Click **Reconnect** to reconnect the selected devices. The reconnect action is used to re-establish a failed connection between a device and NDB controller.

  If you choose the reconnect action without selecting a check box, an error is displayed. You will be prompted to select a device.

- **Update Profile**—Use this action to add or update the profile for a device. See Update Profile for details about this task.

- **Delete Device**—Select the required device by checking the check box which is available at the beginning of the row. Click **Actions** > **Delete Device(s)**. A pop-up window displays two options:

  - **Delete**—Use this option to delete the device from the NDB controller while retaining the device configuration.

Note From release 3.10.5, when you delete a device, the TLS information is retained in the controller. If you want to use the same certificates, then, when you add the device again, on the **Confirm Add Device** pop-up window, select **No** to use the existing certificates and enter the TLS port. If you select **Yes** , then, the existing certificates are deleted and new ones are created.

  - **Purge and Delete**—Use this option to delete the device and also remove device configuration from the NDB controller.

If you choose the delete action without selecting a check box, an error is displayed. You will be prompted to select a device.

Note If a device is not reachable and disconnects from the NDB controller, the NDB controller tries to locate and connect to the device after every 30 seconds.

Global deny ACLs are automatically added to all non-configured interfaces (Edge SPAN/TAP, Packet Truncation, Remote Source, and Local and Remote Monitor) on a device. By default, Global Deny ACL feature is enabled on all the devices. You can disable the Global Deny ACL feature by setting the configure.global.acls parameter to false in the **config.ini** file. Ensure that you restart NDB after making changes in the configuration file.

Adding a Device

Use this procedure to add a device to NDB controller.

Beginning with Nexus Dashboard Data Broker release 3.10.5, it is mandatory to configure the TLS certificates using the GUI. The required steps for TLS configuration is part of the **Add Device** screen. The CLI method for TLS is no longer supported.

Before you begin

Before adding a device to the NDB controller, do the following:

- Enable NXAPI on the device using the **feature nxapi** command.
- Use the Device Prerequisites option, if you are adding a device for the first time to the NDB controller.

Note Check the release-specific *Cisco Nexus Dashboard Data Broker Release Notes*, to see the supported Cisco Nexus Series switches and the supported NX-OS versions.

Procedure

Step 1 Navigate to **Devices** > **NDB Devices**.

Step 2 From the **Actions** drop down menu, select **Add Device**.

Step 3 In the **Add Device** dialog box, enter the following details:

Table 2: Add Device

Field	Description
General	
IP Address/ Hostname	Enter the name or IP address of the device. To add multiple devices, add the hostnames or IP Addresses separated with a comma. To enable TLS, it is mandatory to enter the Hostname (fully qualified hostname which includes the domain name).

Field	Description
Username/ Profile	Select either **Username** or **Profile**. If you click **Username**, the following fields are displayed: • **Username**—Enter the switch username to login to the device. • **Password**—Enter the switch password. If you click **Profile**, the following fields are displayed: • **Profile**—From the **Select Profile** drop-down list, select a profile. **Note** You can associate multiple switches to a profile. The profile configuration is applied to all the member switches.
Connection Type	Select the Connection Type from the drop- down list. Currently, only NX-API is supported.
Port	Enter the device communication port. Use port 80 for NX-API over HTTP and 443 for HTTPS. For TLS configuration, provide a port number to configure the port as a TLS port.
Device Prerequisites	Click the gray button to enable Device Prerequisites. The bar turns blue and the button moves to the right. The following check boxes appear: • Interface Commands—By default, this check-box is checked. Device Prerequisites automatically executes a set of default interface commands. • Reboot—Check the check-box to reboot the device before it gets added to NDB. • TCAM—Check the check-box to set a TCAM value. Select **Default** or **Scale**. A memory of 1024 or 2048 is allocated, respectively.

Field	Description
Transport Layer Security (TLS)	Enable TLS to set the TLS parameters. Hover over the info icon (*i*), a pop-up window is displayed. Click the link to **Update TLS Passwords**. **Note** It is mandatory to enter the TLS passwords at this stage, if you are adding a device with TLS for the first time. If you have already added the passwords earlier, then, you need not add them here again. Passwords can be added in the **Update TLS Passwords** screen. Click the gear icon in the *Header*. The displayed fields are discussed in the subsequent procedure, Configure Transport Layer Security , on page 8.

Step 4 Click **Add Device**.

Note
Global ACLs are automatically added to all the interfaces on a device. By default, Global ACLs are enabled for a device. To manage Global ACLs, you need to add the configure.global.acls parameter in the config.ini file. Set the configure.global.acls parameter to *false* and restart the device to disable Global ACLs on the device.

During the process of device addition, feature tap aggregation is enabled.

Configure Transport Layer Security

This procedure is part of the Adding A Device procedure discussed in the Devices chapter.

Beginning with NDDB release 3.10.5, the Transport Layer Security (TLS) configuration can be performed as part of the Add Device screen. The steps detailed here are for configuring TLS.

Before you begin

Ensure that you have domain name configured on the switch using the **ip domain-name** command for each NDB switch that acts as the Fully Qualified Domain Name (FQDN) for the switch. For example:

```
conf t
ip domain-name cisco.com
hostname N9k-117
end
```

The FQDN for the switch is configured to N9K-117.cisco.com.

Configure these TLS passwords:

- Truststore password
- Keystore password
- PEM passphrase (optional for self-signed TLS)
- Challenge password (optional for self-signed TLS)

Procedure

Step 1 Navigate to **NDB Devices** > **Actions** > **Add Device**.

Step 2 After entering the device details, enable the **Transport Layer Security** option.

Note
You will not be able to enable the TLS option if the prerequisite TLS passwords as mentioned in the *Before you begin* section are not configured. However, you can enter these passwords at this stage as well; enter the passwords in the **Update TLS Passwords** pop-up screen and click **Save**. When you are onboarding a device for the first time, it is recommended to change all the four passwords from the default value to the custom value.

Step 3 Select either the **Self-signed** or **Third-party** option.

Step 4 Enter the following details, these are used for generating the certificates:

a) Enter the **Country** name.
b) Enter the **State** name.
c) Enter the **Locality** name.
d) Enter the **Organization** name.
e) Enter the **Organization Unit** name.
f) Enter a valid **Email ID**.
g) Enter the **Validity Period** (in days). This field is applicable only for the **Self-signed** option.
h) Enable the **Secure Certificate** to encrypt the private key. This field is applicable only for the **Third-party** option.

Step 5 Click **Generate CSR and Add Device**(third-party certificate) or **Add Device** (self-signed certificate).

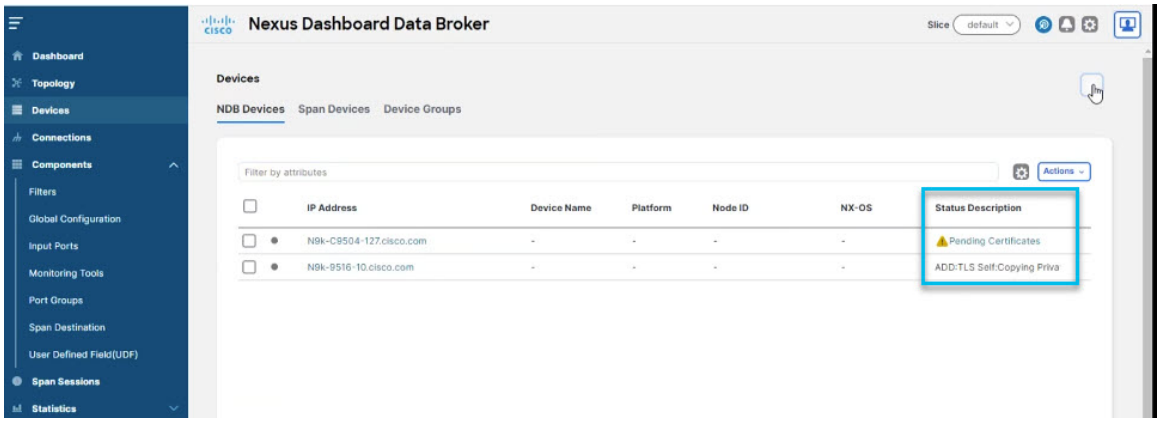
(self-signed certificate)The NDB devices screen is displayed which shows all the available NDB devices.

(third-party certificate) see the subsequent section, *What to do Next*.

What to do next

For third-party TLS, you will need to upload the **Pending Certificates**.

Figure 1: Adding Pending Certificates



Click the **Pending Certificates** link displayed in the Status Description column.

Depending on the tier of the CA you choose, you can get up to three certificates (certificate chain) for each CSR. This means you get three certificates (root, intermediate and domain) from CA for each NDB switch. You need to check with CA to identify each type of certificate. Certificate naming convention might be different for different certifying authorities. For example: test-root-ca-2048.cer (root), test-ssl-ca.cer (intermediate), N9K-117.cisco.com.cer (domain).

When you submit the request to the third party certification authority, follow the relevant procedures and get the three (certificate) files.



Note The supported format for the certificates is .PEM.

Editing a Device

Use this procedure to edit a device.

Before you begin

Create one or more devices.

Procedure

Step 1 Navigate to **Devices** > **NDB Devices**.

Step 2 In the displayed table, click an **IP Address**.

A new pane is displayed on the right.

Step 3 Click **Actions** and select **Edit Device**.

Step 4 In the **Edit Device** dialog box, the current device information is displayed. Modify these fields, as required:

Table 3: Edit Device

Field	Description
General	
IP Address/ Hostname	The current IP address of the device. This field cannot be edited.

Field	Description
Username/ Profile	Select either **Username** or **Profile**. If you click **Username**, the following fields are displayed: • **Username**— Username used to login to the device is displayed; you can edit this field. • **Password**—Enter the password for the username. If you click **Profile**, the following fields are displayed: • **Profile**—From the **Select Profile** drop-down list, select a profile. **Note** You can associate multiple switches to a profile. The profile configuration is applied to all the member switches.
Connection Type	Select the Connection Type from the drop down menu. Currently, only NXAPI is supported.
Port	Enter the device communication port. Use port 80 for NX-API over HTTP and 443 for HTTPS.
Device Prerequisites	Click the gray button to enable Device Prerequisites. The bar turns blue and the button moves to the right. The following check boxes appear: • **Interface Commands**—By default, this check box is checked. Device Prerequisites automatically executes a set of default interface commands. • **Reboot**—Check the check box to reboot the device before it gets added to NDB. • **TCAM**—Check the check box to set a TCAM value. Select **Default** or **Scale**. A memory of 1024 or 2048 is allocated, respectively. For more information about Device Prerequisites, see Device Prerequisites, on page 13.

Step 5 Click **Save**.

Updating Device Profile

Use this procedure to assign (associate) a profile to a device or update the profile for a device.

Before you begin

Create one or more profiles.

Procedure

Step 1 Navigate to **Devices** > **NDB Devices**.

Step 2 From the **Actions** drop-down menu, select **Assign/ Update Profile**.

Step 3 In the **Assign/ Update Profile** dialog box, enter the following details:

Table 4: Assign/ Update Profile

Field	Description
General	
Profile	Select a **Profile** from the drop down menu.
Connection Type	The default NXAPI connection type is displayed.

Step 4 Click **Assign/ Update Profile**.

Adding a Port Channel

Use this procedure to add a port channel.

See Port Channels and Groups for more information about port channels.

Procedure

Step 1 Navigate to **Devices** > **NDB Devices**.

Step 2 Click an **IP Address** and select the Details icon.

Step 3 In the **Add Port Channel** dialog box, enter the following details:

Table 5: Add Port Channel

Field	Description
General	
ID	Enter a name for the port channel.
Description	Enter a description for the port channel.
Port	Click **Select Port**. Select the required check boxes and click **Select**.

Step 4 Click **Add Port Channel**.

Device Prerequisites

Nexus Dashboard Data Broker pushes basic configuration to a newly added device. Ensure NX-API is enabled on the new device for Nexus Dashboard Data Broker to push prerequisite configuration successfully. Manual configuration of the NX-API devices to make it ready for Nexus Dashboard Data Broker is not required.

Device Prerequisites can be configured when you add or edit a device, or when you add or change profile to a device. See Adding a Device, on page 6 and/or Editing a Device, on page 10.

Following configurations are pushed into the new switch by Nexus Dashboard Data Broker:

- While onboarding an NDB device, without following STP pre-requisites (when independent links or port channels are connected to NDB devices), you need to manually configure the **switchport mode trunk** and **spanning-tree bpdufilter enable** commands.
- TCAM configurations based on the device platform
- MST mode is enabled on the Spanning Tree
- Basic VLAN configuration
- Feature tap aggregation is enabled.
- LLDP feature is enabled (only for the centralized mode).

Device is rebooted after all the configurations are successfully pushed by Nexus Dashboard Data Broker. The device reboot is required because of the TCAM configurations. The reboot is supported from NX-OS is 9.2(3) and above.

Port Channels and Port Groups

Port Channels

A port channel is an aggregation of multiple physical interfaces that creates a logical interface. You can bundle up to 8 individual active links into a port channel to provide increased bandwidth and redundancy. If a member port within a port channel fails, the traffic previously carried over the failed link switches to the remaining member ports within the port channel. Port channeling also load balances traffic across these physical interfaces. The port channel stays operational as long as at least one physical interface within the port channel is operational.

You create a port channel by bundling compatible interfaces. You can configure and run either static port channels or ports channels running the Link Aggregation Control Protocol (LACP). Any configuration changes that you apply to the port channel are applied to each member interface of that port channel. For example, if you configure Spanning Tree Protocol (STP) parameters on the port channel, the Cisco NX-OS applies those parameters to each interface in the port channel.

You can use static port channels, with no associated protocol, for a simplified configuration. For more efficient use of the port channel, you can use the Link Aggregation Control Protocol (LACP), which is defined in IEEE 802.3ad. When you use LACP, the link passes protocol packets.

Port Groups

Ports of a device (or different devices) can be grouped together to form a port group. The port groups can be a combination of the edge-span and the edge-tap ports across different switches. Selecting individual ports of a port group is disabled when using a port group.

Symmetric and Non-Symmetric Load Balancing

You can configure symmetric load balancing and enable MPLS tag stripping on the Cisco Nexus 9000 Series switches using NX-API configuration mode, from the Cisco Nexus Data Broker GUI and the REST API interfaces.

The following table lists the symmetric and non-symmetric load balancing options:

Configuration Type	Hashing Configuration	Platforms	Options
Symmetric	SOURCE_DESTINATION	Nexus 9000 Series (all), N3K-C3164xx, N3K-C32xx	IP, IP-GRE, IP-L4PORT, IP-L4PORT-VLAN, IP-VLAN, L4PORT, MAC
		REST API	IP, IP-GRE, PORT, MAC, IP-ONLY,PORT-ONLY
Non-symmetric	SOURCE, DESTINATION	Nexus 9000 Series (all), N3K-C3164xx, N3K-C32xx	IP, IP-GRE, IP-L4PORT, IP-L4PORT-VLAN, IP-VLAN, L4PORT, MAC
		REST API	IP, IP-GRE, PORT, MAC

Span Devices

Switch port Analyzer (SPAN) is an efficient and high performance traffic monitoring system. It duplicates the network traffic and routes the packets to an the analyzer for monitoring. SPAN is used for troubleshooting connectivity issues and calculating network utilization, and performance monitoring.You can add, edit, remove, and rediscover a device to SPAN using Nexus Dashboard Data Broker.

Beginning with Cisco Nexus Dashboard Data Broker Release, 3.10.1, Cisco Catalyst 9300 Series Switches are supported as a production switch. For details of Catalyst switches, see *relevant Cisco documentation on Cisco.com*.

Note Catalyst series switches 9300-24UB have been qualified for Release 3.10.1. Supported IOS XE versions are, 16.09.05 and above.

Catalyst switches can be directly onboarded and managed using the Nexus Dashboard Data Broker GUI. Catalyst switches can also be onboarded using Cisco DNA Center (Cisco DNAC). See Integrating Cisco Nexus Dashboard Data Broker with Cisco DNA Center , on page 19.

The **Span Devices** tab displays details of the devices connected to the SPAN.

Select **Controllers** or **Production Switches** to see the details.

- **Controllers** —networks or devices connected to the Nexus Dashboard Data Broker controller via Cisco APIC or Cisco DNAC.

- **Production Switches**—standalone Nexus or Catalyst switches connected to the Nexus Dashboard Data Broker controller.

Table 6: Controllers

Column	Description
Active IP	Active IP address of the controller. Click the IP address and a new pane is displayed on the right. Additional actions that can be performed from here are: • Editing a Span Device, on page 17 Current IP address of the Cisco APIC/ Cisco DNAC controller communicating with the Nexus Dashboard Data Broker controller. Click the IP address and a new pane is displayed on the right side with more details. For Cisco DNAC controllers, the template names that Nexus Dashboard Data Broker installs on Cisco DNAC are displayed. The templates are: • NDB Monitor Session Deletion • NDB Monitor Session Creation
Username	Username currently logged in to the controller .
Name	Name of the controller.
Primary IP Address	Primary IP address of the controller.
Secondary IP Address	(Only for APIC) Secondary IP address of the controller .
Tertiary IP Address	(Only for APIC) Tertiary IP address of the controller.

Table 7: Production Switches

Column	Description
Active IP	Active IP address of the device. Click the IP address and a new pane is displayed on the right. Additional actions that can be performed from here are: • Editing a Span Device, on page 17
Username	Username currently logged in to the device.
Platform	Platform of the device.

The following actions can be performed from the **Span Devices** tab:

- **Add Span Device**—Use this to add a new span device. See Adding a Span Device , on page 16 for details.
- **Rediscover Span Device**—Select the required device by checking the check box at the beginning of the row. Click **Actions** > **Rediscover Span Device**. A pop-up window is displayed. Click **Rediscover** to rediscover the selected devices.

  Use the **Rediscover Span Device** option to re-establish the connection between the Nexus Dashboard Data Broker controller and the Span device(s).

  If you choose the rediscover action without selecting a check box, an error is displayed. You will be prompted to select a device.
- **Delete Span Device**—Select the required device by checking the check box which is available at the beginning of the row. Click **Actions** > **Delete Span Device**.

  If you choose the delete action without selecting a check box, an error is displayed. You will be prompted to select a device.

Adding a Span Device

Use this procedure to add a device to SPAN.

Procedure

Step 1 Navigate to **Devices** > **Span Devices**.

Step 2 From the **Actions** drop down list, select **Add Span Device**.

Step 3 In the **Add Span Device** dialog box, enter the following details:

Table 8: Add Span Device

Field	Description
General	Select **Controller** or **Production Switch**. A controller can be a Cisco APIC or Cisco DNAC. A Production Switch (PS) can be a Nexus or a Catalyst switch. The options available for each are discussed in the rows, below.
Fields displayed for **Controller** :	
Controller Type	Select a controller type from the drop down list. The options are: • Cisco APIC • Cisco DNAC
IP Address/ Hostname	Enter the IP address for the controller.
IP Address (Secondary)	(Optional; only for APIC) Enter a secondary IP address for the controller.

Field	Description
IP Address (Tertiary)	(Optional; only for APIC) Enter a tertiary IP address for the controller.
Username	Enter a username.
Password	Enter the required password for authentication.
Cisco DNAC Name	(Only for Cisco DNAC) Enter a name for the Cisco DNAC. This name is used for identification by the Nexus Dashboard Data Broker controller.
Fields displayed for **Production Switch**:	
Address	IP address of the Nexus or Catalyst switch.
Platform Type	Select from the drop down list. The options are: • Nexus • Catalyst
Port	The device communication port. Enter a port number for Nexus switches. If you have selected the **Platform Type** as Catalyst, the default port value of 22 is displayed. Communication to catalyst switches is via SSH.
Username	Enter a username for the device.
Password	Enter the required password to authenticate the username.
Enable Password	(Only for Catalyst switches) Enter the required password. **Note** If the switch is not in enable mode, then enter the password.

Step 4 Click **Add Span Device**.

After a Cisco DNAC controller is successfully added as a span device, Nexus Dashboard Data Broker installs the required projects and templates on the Cisco DNAC controller. You can check the created projects and templates under *Template Editor* on the Cisco DNAC.

Editing a Span Device

Use this procedure to edit parameters for a Span device.

Before you begin

Create one or more Span devices.

Procedure

Step 1 Navigate to **Devices** > **Span Devices**.

Step 2 In the displayed table, click an **IP Address**.

A new pane is displayed on the right.

Step 3 Click **Actions** and select **Edit Span Device**.

Step 4 In the **Edit Span Device** dialog box, the current span device information is displayed. Modify these fields, as required:

Table 9: Edit Span Device

Field	Description
General	This field can not be edited. If you have selected a **Controller** or **Production Switch**, earlier, that selection can not be changed. However, the parameters for these can be edited and they are discussed in the rows, below.
Fields displayed for **Controller** :	
Controller Type	The earlier selected controller type. This field can not be edited.
IP Address/ Hostname	The primary IP address of the controller . This field can not be edited.
IP Address (Secondary)	(Only for APIC) Enter a secondary IP address for the APIC device.
IP Address (Tertiary)	(Only for APIC) Enter a tertiary IP address for the APIC device.
Username	Username for the controller.
Password	Enter the required password for authentication.
Cisco DNAC Name	(Only for Cisco DNAC) Name of the Cisco DNAC. This name is used for identification by the Nexus Dashboard Data Broker controller.
Fields displayed for **Production Switch**:	
Address	IP address of the Nexus or Catalyst switch.
Platform Type	The earlier selected platform type. This field can not be edited.
Port	The device communication port. The port number is 80 for Nexus switches and 22 for Catalyst switches.
Username	Username for the device.
Password	Enter the required password to authenticate the username.

Field	Description
Enable Password	(Only for Catalyst switches) Enter the required password to enable the switch.

Step 5 Click **Save**.

Integrating Cisco Nexus Dashboard Data Broker with Cisco DNA Center

Cisco Digital Network Architecture Center (Cisco DNAC) is a powerful network controller and management dashboard that lets you take charge of your network.

For details about Cisco DNAC, see *relevant Cisco DNAC documentation.*

The Cisco DNAC controller can be integrated with Nexus Dashboard Data Broker. SPAN session configurations on the Catalyst switches are managed from the Nexus Dashboard Data Broker UI. Nexus Dashboard Data Broker creates a separate Project and Template(s) on Cisco DNAC while onboarding. Nexus Dashboard Data Broker shares the ports details of the Catalyst switches to Cisco DNAC. Based on the templates, Cisco DNAC creates SPAN sessions on the Catalyst switches.

Examples of Nexus Dashboard Data Broker templates on the Cisco DNAC controller:

```
monitor session $sessionNumber source $sourceType $sources $direction
monitor session $sessionNumber destination interface $destinationInterfaces
```

REST APIs are used for communication between the Nexus Dashboard Data Broker controller and Cisco DNAC.

Tap Devices

Cisco Nexus Dashboard Data Broker supports Cisco Nexus 3550-F L1 series switch as a Tap device. A Tap device is a device that makes a copy of network data but does not alter the data. Traffic from the Tap device reaches the Cisco Nexus Dashboard Data Broker for further processing.

Table 10: Tap Devices

Column	Description
IP Address	IP address of the tap device.
Device Name	Name of the device.
Platform	Platform of the tap device.
Node ID	The unique ID of the tap device used for identification by the Nexus Dashboard Data Broker controller.
Profile Name	Associated profile name. If the **Profile** option was not selected while creating a tap device, no information is displayed here.
Version	The software version of the tap device.

Column	Description
Status Description	The status of the connection between the Nexus Dashboard Data Broker controller and the tap device. The available options are: • Successfully connected—successful connection • Authentication failure—incorrect credentials of the tap device • Connection timed-out—tap device not reachable within a period of time. • No route to host—wrong IP address of the tap device • Invalid response from device—incorrect device (any other device besides Cisco Nexus 3550-L1)

The following actions can be performed from the **Tap Devices** tab:

- **Add Tap Device**—Use this to add a new tap device. See Adding a Tap Device, on page 20 for details.
- **Assign/ Update Profile**—Use this action to add or update the profile for a tap device. See *Update Profile* for details about this task.
- **Reconnect Tap Device(s)**— Select the required device by checking the check box at the beginning of the row. Click **Actions** > **Reconnect Tap Device(s)**. A pop-up appears. Click **Reconnect** to reconnect the selected tap devices. Use this option when you see a *Connection Timed Out* error between the tap device and Nexus Dashboard Data Broker controller.
- **Delete Tap Device**—Select the required tap device by checking the check box which is available at the beginning of the row. Click **Actions** > **Delete Device(s)**. You have two options:
  - **Delete**—disconnects the tap device from the Nexus Dashboard Data Broker controller.
  - **Purge and Delete**—disconnects the tap device from the Nexus Dashboard Data Broker controller and deletes associated configurations from the Nexus Dashboard Data Broker controller.

Adding a Tap Device

Use this procedure to add Cisco Nexus 3550-F L1 as a tap device. The minimum supported software version is 1.15.0.

Before you begin

- Enable HTTP on the tap device, using **configure http enable**.
- Ensure there are no pre-existing configurations on the tap device.

Procedure

Step 1 Navigate to **Devices** > **Tap Devices**.

Step 2 From the **Actions** drop down list, select **Add Tap Device**.

Step 3 In the **Add Tap Device** dialog box, enter the following details:

Table 11: Add Tap Device

Field	Description
IP Address/ Hostname	Enter the IP address of the tap device.
You can choose to add a tap device by either using the username of the device or using an associated profile. Select **Username** or **Profile** and fill in the relevant fields.	
Username	
Username	Enter a username to login to the device.
Password	Enter the password for the username.
Profile	
Profile	Select a profile from the drop-down list.
Connection Type	This field is read-only. The default value (REST) is displayed.

Step 4 Click **Add Tap Device**.

Device Groups

The **Device Groups** tab displays details of the device groups. A table is displayed with the following details:

Table 12: Device Groups

Column Name	Description
Group	The device group name. This field is a hyperlink. Click the group name and a new pane is displayed on the right that has the list of devices included in the group. Additional actions that can be performed from here are: • Editing a Device Group
Devices	The number of devices in the device group.

The following actions can be performed from the **Device Groups** tab:

- **Add Device Group**—Use this to add a new device group. See Adding a Device Group.
- **Delete Device Group**—Select the required device group by checking the check box which is available at the beginning of the row. Click **Actions** > **Delete Device Group(s).** The selected device group(s) are deleted. If you choose the delete action without selecting a check box, an error is displayed. You will be prompted to select a device group.

Adding a Device Group

Use this procedure to add a new device group.

Procedure

Step 1 Navigate to **Devices** > **Device Groups**.

Step 2 From the **Actions** drop down menu, select **Add Device Group**.

Step 3 In the **Add Device Group** dialog box, enter the following details:

Table 13: Add Device Group

Field	Description
General	
Device Group Name	Enter a name for the device group.
Devices	Click **Select Device(s)**. The **Select Device** dialog box opens. Check the check box corresponding to the device(s) you want to add to the group. Click **Select**. **Note** Check if the device is already part of another group; if yes, the device is removed from the previous group and added to the new group.

Step 4 Click **Add Device Group**.

Editing a Device Group

Use this procedure to edit a device group.

Before you begin

Add one or more device groups.

Procedure

Step 1 Navigate to **Devices** > **Device Groups**.

Step 2 Click a **Device Group** name.

A new pane is displayed on the right.

Step 3 Click **Action** > **Edit Device Group**.

Enter the following details, in the displayed window.

Table 14: Edit Device Group

Field	Description
General	
Device Group Name	Device group name. This field cannot be edited.
Devices	The devices which are currently part of the device group are displayed. You can delete devices from a group. To add more devices to the group, click **Select Device(s)**. The **Select Device** dialog box opens. Check the check box corresponding to the device(s) you want to add to the group. Click **Select**. **Note** Check if the device is already part of another group; if yes, the device is removed from the previous group and added to the new group.

Step 4 Click **Save**.