



## Viewing and Adding Devices

---

This chapter contains the following sections:

- [Viewing and Adding Devices](#) , on page 1

## Viewing and Adding Devices

On the **Devices** screen, the following tabs are displayed:

- Nodes Learned
- Device Connections
- Device Groups
- SPAN Management
- Subnet Gateway Configuration

On the **Nodes Learned** tab, the following details are displayed for each node:

- The name of the node
- The ID of the node
- IP Address of the node
- The number of ports on the node

When you click the node name under the tab **Node Name**, the **Update Node Information** window is displayed. Update the following fields in the window:

- **Node ID:** Enter the node ID.
- **Node Name:** The name of the node.
- **Tier:** Select the tier of the node from the following options in the drop-down list: Unknown, Access, Distribution, and Core.
- **Operation Mode:** Choose how the traffic is handled based on the flows. This can be one of the following:  
Allow reactive forwarding—No default flows are programmed. How traffic that does not match a flow is treated depends upon the switch implementation.

Proactive forwarding only—The following default flows are programmed on the switch:

- Punt Link Layer Discovery Protocol (LLDP) packets.
- Drop all other traffic.

On the **Device Connections** tab, click **Add Device** to add a device, click **Remove Devices** to remove a device, or click **Rediscover Devices** to rediscover a device. When you click **Rediscover Devices** tab, the **Rediscover Device** window is displayed. Click **Rediscover Device** so that the device gets deleted and rediscovered again.

In each device window, click **View**, **Edit**, or **Delete** to add a device, edit an existing device, or delete a device. The following details are displayed for each device in each device window:

- The name of the device and its IP address
- The username on the device
- The type of the mode, for example, NX-API
- The uptime on the device, for example, date and time
- The hardware on the node

On the **Device Groups** tab, click + **Group** to add a group of devices. In each group window, click **View**, **Edit**, or **Delete** to add a group of devices, edit an existing group of devices, or delete a group of devices respectively. The following details are displayed in each group window:

- The name of the node group, for example, Node Group Name One
- The names of the nodes in the group, for example, nx-tap-agg-sw1 and nx-tap-agg-sw2

On the **SPAN Management** tab, click + **Add Device** to add an APIC device or the production switch to the network. Click **Remove Devices** to delete the devices or click **Rediscover Devices** to rediscover the devices. The production switch should be a Cisco Nexus 9000 Series switch or Cisco Nexus 3000 Series switch in NXOS mode. The feature NXAPI has to be enabled on these production switches.




---

**Note** If a device is unreachable and disconnects from NDB, NDB tries to locate and connect to the device after every 30 seconds.

---

The following columns are displayed on the **SPAN Management** tab to display the information about the devices:

- IP Address
- Username
- Type: The APIC device is listed as AC and the production switch will belated here is listed as PS.
- Active IP
- Secondary IP Address
- Tertiary IP Address
- Action

You must add an APIC controller before you can set up SPAN session and SPAN destination.

Starting with Cisco NDB release 3.6, Global deny ACLs are automatically added to all non-configured (Edge SPAN/TAP & Monitor) interfaces on a device. The Global deny ACL feature is equivalent to Block Rx feature. By default, Global Deny ACL feature is enabled for a device. To disable the Global Deny ACL feature, you need to add the `configure.global.acls` parameter and set it to *false* in the `config.ini` file. After setting the `configure.global.acls` parameter, you need to restart the system to disable Global Deny ACLs on the newly added devices.



**Note** To disable Global Deny ACL during CLI upgrade, run the CLI upgrade command and then configure the `configure.global.acls` parameter to *false* in the `config.ini` file before restarting the NDB. For example:

```
/xnc upgrade --perform --target-home {xnc_directory_to_be_upgraded} [--verbose] [--backupfile
{xnc_backup_location_and_zip_filename}]
// In the config.ini file//
configure.global.acls=false
```

To disable Global Deny ACL features during configuration upload, set the `configure.global.acls` parameter to *false* in the `config.ini` file before restarting the NDB.

Starting with Cisco NDB release 3.6, when a new switch is discovered on NDB, the following connections are installed on the ISL interfaces:

- Default-Deny-ISL connection with Default-Deny-All, Default-Deny-MPLS, and Default-Deny-ARP filters. This connection is supported on all the types of switches in NXAPI mode.
- Default-Deny-ISL-ICMP connection with Default-Deny-ICMP and Default-Deny-ICMP-All filters. This connection is supported on 9200, 9300EX, 9300FX, 9500EX, and 9500FX switches in NXAPI mode.

All the ACLs related to the default filters are installed on the ISL interfaces of the new switch. By default, this feature is enabled for all the new ISL interfaces.



**Note** You can manage this feature using the `mm.addDefaultISLDenyRules` parameter in `config.ini` file. By default, the `mm.addDefaultISLDenyRules` parameter is not present in `config.in` file. To disable this feature, you need to add the `mm.addDefaultISLDenyRules` parameter to `config.ini` file and set it to *false* and restart the device. For example:

```
mm.addDefaultISLDenyRules = false
```



**Note** To disable Default-Deny-ISL Default-Deny-ISL-ICMP features during CLI upgrade, run the CLI upgrade command and then configure the `mm.addDefaultISLDenyRules` parameter to *false* in the `config.ini` file before restarting the NDB. For example:

```
./xnc upgrade --perform --target-home {xnc_directory_to_be_upgraded} [--verbose] [--backupfile
{xnc_backup_location_and_zip_filename}]
// In the config.ini file//
mm.addDefaultISLDenyRules=false
```

To disable Default-Deny-ISL Default-Deny-ISL-ICMP features during configuration upload, set the `mm.addDefaultISLDenyRules` parameter to *false* in the `config.ini` file before restarting the NDB.

