Installing or Upgrading the Cisco Nexus Data Broker Software in Centralized Mode

This chapter contains details of procedures for installing and upgrading NDB in centralized mode.

Before your proceed with the upgrade/ install procedures in this chapter, compare the **md5sum** between the NDB CCO image and image file copied to linux. Use the following command to check (linux):

```
cisco@NDB-virtual-machine:~/3.9.2/$ md5sum ndb1000-sw-app-k9-3.9.2.zip
Displayed output: c2d273dce4abbba03c06aeee8774b901 ndb1000-sw-app-k9-3.9.2.zip
```

This chapter contains the following topics:

Installing or Upgrading the Cisco Nexus Dashboard Data Broker Software in Centralized Mode

Installing the Cisco Nexus Data Broker Software in Centralized Mode

Complete these steps to install Cisco Nexus Data Broker software in Centralized mode:

Step 1 In a web browser, navigate to **www.cisco.com**.

Step 2 Under **Support**, click **All Downloads**.

Step 3 In the center pane, click **Cloud and Systems Management**.

Step 4 If prompted, enter your Cisco.com **username** and **password** to log in.

Step 5 In the right pane, click **Network Controllers and Applications**, and then click **Cisco Nexus Data Broker.**

The file information for Release 3.9.2 is displayed: Cisco Nexus Data Broker Software Application: ndb1000-sw-app-k9-3.9.2.zip

Step 6 Download the Cisco Nexus Data Broker application bundle.

Step 7 Create a directory in your Linux machine where you plan to install Cisco Nexus Data Broker.

For example, in your Home directory, create `CiscoNDB`.

Step 8 Copy the Cisco Nexus Data Broker zip file into the directory that you created.

Step 9 Unzip the Cisco Nexus Data Broker zip file.

The Cisco Nexus Data Broker software is installed in a directory called `xnc`. The directory contains the following:

- `runxnc.sh` file—The file that you use to launch Cisco Nexus Data Broker.
- `version.properties` file—The Cisco Nexus Data Broker build version.
- `configuration` directory—The directory that contains the Cisco Nexus Data Broker initialization files.

  This directory also contains the `startup` subdirectory where configurations are saved.
- `bin` directory—The directory that contains the following script:
  - `xnc` file—This script contains the Cisco Nexus Data Broker common CLI.
- `etc` directory—The directory that contains profile information.
- `lib` directory—The directory that contains the Cisco Nexus Data Broker Java libraries.
- `logs` directory—The directory that contains the Cisco Nexus Data Broker logs.

  Note The `logs` directory is created after the Cisco Nexus Data Broker application is started.
- `plugins` directory—The directory that contains the OSGi plugins.
- `work` directory—The webserver working directory.

  Note The `work` directory is created after the Cisco Nexus Data Broker application is started.

Note To migrate from OVA-based Openflow to Native Openflow, see the Uninstalling Cisco Plug-in for OpenFlow chapter.

Upgrading the Application Software in Centralized Mode Using CLI

Use the **upgrade** command to upgrade to Cisco NDB Release 3.9.2.

Note

- Once you upgrade to Cisco NDB Release 3.9.2, you cannot use the downgrade option to rollback to a previous release. You have to use the configuration archive that is created during the upgrade process to rollback the software.
- When you upgrade the software to Cisco Nexus Data Broker Release 3.2 or later release, the hostname should not be changed during the upgrade process. If the hostname is changed during the upgrade process, the upgrade might fail. If you are upgrading from release 2.x, 3.0 and 3.1, the domain name configuration in the switch should be removed before upgrading the software.
- When you run the **upgrade** command, the installation and the configuration are upgraded. However, any changes you made to the shell scripts or configuration files, for example, `config.ini`, are overwritten. After you complete the upgrade process, you must manually reapply your changes to those files.

Before you begin

- Stop all controller instances that use the Cisco Nexus Data Broker installation. This will avoid conflicts with the file system, which is updated during the upgrade.
- For NDB configuration upload or Backup/Restore process, first bring up the NDB instance where configuration is uploaded or where Backup/Restore is done, then start rest of the nodes in the cluster.
- Backup up the NDB configuration. For more information, see *Backing Up or Restoring the Configuration Using NDB GUI* section.
- If you are using high availability clustering, stop all application instances in the cluster to ensure that there are no inconsistencies.
- Back up your `config.ini` file.

Important You should manually backup your `config.ini` file before upgrading, because the backup process does not back them up for you. If you do not backup your files before upgrading, any changes you made will be lost.

Note When you run `runxnc.sh` script, there is a thread in the script that monitors the log and the Cisco Nexus Data Broker JAVA process to monitor the health of the Cisco Nexus Data Broker. The default value for this option is 30 Seconds.

SUMMARY STEPS

1. In a web browser, navigate to Cisco.com.
2. Under **Support**, click **All Downloads**.
3. In the center pane, click **Cloud and Systems Management**.
4. In the right pane, click **Network Controllers and Applications**, and then click **Cisco Nexus Data Broker.**

5. Download the Cisco NDB Release 3.9.2 applicable bundle: Cisco Nexus Data Broker Software Application—ndb1000-sw-app-k9-3.9.2.zip
6. Create a temporary directory in your Linux machine where you plan to upgrade to Cisco NDB.
7. Unzip the Cisco NDB Release 3.9.2 zip file into the temporary directory that you created.
8. Navigate to the `xnc` directory that was created when you installed the Cisco Nexus Data Broker release earlier.
9. Backup your Cisco Nexus Data Broker release installation using your standard backup procedures.
10. Stop running all Cisco Nexus Data Broker release processes.
11. Navigate to the `xnc/bin` directory in the temporary directory that you created for Cisco NDB Release 3.9.2 upgrade software.
12. Upgrade the application by entering the **./xnc upgrade --perform --target-home** {*xnc_directory_to_be_upgraded*} **[--verbose] [--backupfile** {*xnc_backup_location_and_zip_filename*}**]** command.
13. Navigate to the `xnc` directory where you originally installed Cisco XNC Monitor Manager.
14. If TLS certification is enabled between NDB server and NXOS switch, copy the tlsTrustStore and tlsKeyStore files to /xnc/configuration from the old xnc backup.
15. Start the application processes that you previously stopped.
16. If the secondary/cluster NDB server is configured, start the server.

DETAILED STEPS

Step 1 In a web browser, navigate to Cisco.com.

Step 2 Under **Support**, click **All Downloads**.

Step 3 In the center pane, click **Cloud and Systems Management**.

Step 4 In the right pane, click **Network Controllers and Applications**, and then click **Cisco Nexus Data Broker.**

Step 5 Download the Cisco NDB Release 3.9.2 applicable bundle: Cisco Nexus Data Broker Software Application—ndb1000-sw-app-k9-3.9.2.zip

Step 6 Create a temporary directory in your Linux machine where you plan to upgrade to Cisco NDB.

Step 7 Unzip the Cisco NDB Release 3.9.2 zip file into the temporary directory that you created.

Step 8 Navigate to the `xnc` directory that was created when you installed the Cisco Nexus Data Broker release earlier.

Step 9 Backup your Cisco Nexus Data Broker release installation using your standard backup procedures.

Step 10 Stop running all Cisco Nexus Data Broker release processes.

Step 11 Navigate to the `xnc/bin` directory in the temporary directory that you created for Cisco NDB Release 3.9.2 upgrade software.

Step 12 Upgrade the application by entering the **./xnc upgrade --perform --target-home** {*xnc_directory_to_be_upgraded*} **[--verbose] [--backupfile** {*xnc_backup_location_and_zip_filename*}**]** command.

You can use one of the following options:

Option	Description
--perform --target-home {*xnc_directory_to_be_upgraded*}	Upgrades the Cisco XNC Monitor Manager intallation to Cisco NDB.

Option	Description
--perform --target-home {*xnc_directory_to_be_upgraded*} **--backupfile** {*xnc_backup_location_and_zip_filename*}	Upgrades the Cisco XNC Monitor Manager installation to Cisco NDB and creates a backup.zip file in the directory path that you set. **Note** • You must provide the name of the backup file and the .zip extension. • The backup file should not be saved in the xnc directory with current NDB installation or its subdirectory.
--verbose	Displays detailed information to the console. This option can be used with any other option and is disabled by default.
--validate --target-home {*xnc_directory_to_be_upgraded*}	Validates the installation.
./xnc help upgrade	Displays the options for the **upgrade** command.

Step 13 Navigate to the `xnc` directory where you originally installed Cisco XNC Monitor Manager.

Step 14 If TLS certification is enabled between NDB server and NXOS switch, copy the tlsTrustStore and tlsKeyStore files to /xnc/configuration from the old xnc backup.

Step 15 Start the application processes that you previously stopped.

Note
- Clear the browser cache. Use Shift+Ctrl+Delete keys to clear the cache.
- Press Ctrl–F5, or press the Cmd, Shift, and R keys simultaneously when you access through a web UI following an upgrade.

Step 16 If the secondary/cluster NDB server is configured, start the server.

Note If TLS certification is enabled, start the secondary/cluster using the commands as shown below:

```
./runxnc.sh -tls -tlskeystore ./configuration/tlsKeyStore -tlstruststore
./configuration/tlsTrustStore
cd bin
./xnc config-keystore-passwords --user <NDB_username> --password <NDB_password> --url
https://<Cluster_NDB_IP>:8443 --verbose --prompt --keystore-password <keystore-password>
 --truststore-password <truststore-password>
```

Upgrading the Application Software in Centralized Mode Using GUI

Complete the following steps to upgrade the application software in the Centralized mode using GUI:

Step 1 Log into NDB.

Step 2 Navigate to the **System** tab under **Administration**.

The **System Administration** window is displayed.

Step 3 Click **Download Configuration** to download the switch configuration file in a .zip file format.

The default name of the zip file is **configuration_startup.zip**.

OR

Navigate to the **Backup/Restore** tab under **Administration** > **System** tab. Click **Backup and Backup Locally** to download the configuration in zip file format.

Step 4 Stop the current NDB instance using the **runxnc.sh -stop** command.

Example:

```
./runxnc.sh -stop
```

Step 5 If TLS certification is enabled between NDB server and NXOS switch, copy the tlsTrustStore and tlsKeyStore files to /xnc/configuration from the old xnc backup.

Step 6 Start the new NDB installation using the **runxnc.sh -start** command.

Example:

```
./runxnc.sh -start
```

Step 7 Navigate to the **Backup/Restore** tab under **Administration** > **System** tab.

Step 8 Click **Restore Locally** and upload the configuration_startup.zip

Step 9 Restart the new NDB instance using the **runxnc.sh -restart** command.

Example:

```
./runxnc.sh -restart
```

Upgrading the Application Software when TLS is enabled in the Standalone Controller

Use this procedure for upgrading the application software in centralized mode, using the GUI, when the TLS certification is enabled in the standalone controller.

Step 1 Log in to the existing NDB GUI instance using *https://<server IP>:8443*.

Step 2 Navigate to **Administration** > **System**> **Backup/ Restore** > **Backup** tab.

Step 3 Click **Backup now Locally** to download the configuration as a zip file.

Step 4 Stop the current NDB instance using the `runxnc.sh -stop` command.

Step 5 After the NDB instance is stopped, navigate to */xnc/configuration* folder, and copy the tlsTrustStore and tlsKeyStore files to *local/common* folder.

Step 6 Download the NDB 3.9.2 software from the standard Downloads page and start the new NDB 3.9.2 installation using the `runxnc.sh -start` command.

Step 7 Log in to the new instance of NDB GUI using *https://<server IP>:8443*.

Step 8 Navigate to **Administration** > **System**> **Backup/ Restore** > **Backup** tab.

Step 9 Click **Restore Locally** to upload the configuration file which you have downloaded earlier (see Step 3, above).

After the configuration is uploaded successfully, you will see a *success* message on the GUI.

Step 10 Connect using SSH to the NDB server, and copy the tlsTrustStore and tlsKeyStore files to NDB 3.9.2 */xnc/configuration/startup* folder (which is copied to *local/common* folder in step 5).

Step 11 Stop the NDB 3.9.2 instance using the `runxnc.sh -stop` command.

Step 12 Start the NDB 3.9.2 instance again using the following command:

```
./runxnc.sh -tls -tlskeystore ./configuration/startup/tlsKeyStore -tlstruststore
./configuration/startup/tlsTrustStore
```

Upgrading the Application Software when TLS is enabled in the HA-Clustered Controller

Use this procedure for upgrading the application software in centralized mode, using the GUI, when the TLS certification is enabled in the HA-clustered controller.

Step 1 Log in to the existing NDB GUI instance using *https://<server IP>:8443*.

Step 2 Navigate to **Administration** > **System**> **Backup/ Restore** > **Backup** tab.

Step 3 Click **Backup now Locally** to download the configuration as a zip file.

Step 4 Stop all the current NDB instance(s) using the `runxnc.sh -stop` command.

Step 5 After the NDB instance is stopped, navigate to */xnc/configuration* folder, and copy the tlsTrustStore and tlsKeyStore files to *local/common* folder.

Step 6 Download the NDB 3.9.2 software from the standard Cisco downloads page and configure the cluster mode with "supernodes" configuration in the *config.ini* file and start the new NDB 3.9.2 cluster using the `runxnc.sh -start` command on all the controllers.

Step 7 On the primary controller, navigate to **Administration** > **Syste,** > **Backup/Restore** > **Backup** tab.

Step 8 Click **Restore Locally** to upload the configuration file which you have downloaded earlier (see Step 3, above).

After the configuration is uploaded successfully, you will see a *success* message on the GUI.

Step 9 Connect using SSH to the NDB server, and copy the tlsTrustStore and tlsKeyStore files to NDB 3.9.2 */xnc/configuration/startup* folder (which is copied to *local/common* folder in step 5).

Step 10 Stop the NDB 3.9.2 instances on all the controllers of the cluster, using the `runxnc.sh -stop` command.

Step 11 Start the NDB 3.9.2 instance on the primary controller using the following command.

```
./runxnc.sh -tls -tlskeystore ./configuration/startup/tlsKeyStore -tlstruststore
./configuration/startup/tlsTrustStore
```

Wait for a few minutes; a *ready* message is displayed.

Step 12 Start the NDB 3.9.2 instance on the other controllers of the cluster using the following command:

```
./runxnc.sh -tls -tlskeystore ./configuration/startup/tlsKeyStore -tlstruststore
./configuration/startup/tlsTrustStore
```

Upgrading NDB Using the Hitless Method

You can upgrade Cisco NDB using the either the upload or the CLI upgrade hitless methods.

Upgrading Cisco NDB - Hitless Method (Using Upload)

You can upgrade Cisco NDB to Release 3.9.2 with the hitless method using upload.

Before you begin

If the Cisco NDB version is earlier than Release 3.8, you must edit the config.ini file and update the **skipConfigurtionStateDBfiles** key to false on both the controllers, and restart all the earlier version controllers.

Step 1 Log into NDB.

Step 2 Navigate to the location (`/home/3.9.2/xnc`) of the xnc for Release 3.9.2 in both, server 1 and server 2.

Step 3 Navigate to the **System** tab under **Adminstration** to view the **System Administration** window.

Step 4 Navigate to **Administration** > **system** > **Backup/Restore** > **Backup** > **Backup now locally** to download the configuration in zip file format and save it on your local desk.

Note The server that is started first will become the primary server, while the second server will become the member.

Step 5 Verify the versions of the servers to confirm that it displays Release 3.9.2. Also, verify that the primary server and member is assigned.

Step 6 If TLS certification is enabled between NDB server and NXOS switch, copy the tlsTrustStore and tlsKeyStore files to /xnc/configuration from the old xnc backup.

Step 7 Navigate to **Administration** > **system** > **Backup/Restore** > **Restore** > **Restore locally** to upload the configuration to the primary server. Stop Cisco NDB on the second server and restart the first server. After you restart the server, Release 3.9.2 configurations are successfully uploaded in Cisco NDB Release 3.9.2. Verify all the configurations.

Step 8 If secondary / cluster NDB server is configured, start the server.

Note If TLS certification is enabled, start the secondary/ cluster using the commands as shown below:

```
./runxnc.sh -tls -tlskeystore ./configuration/tlsKeyStore -tlstruststore
./configuration/tlsTrustStore
cd bin
./xnc config-keystore-passwords --user <NDB_username> --password <NDB_password> --url
https://<Cluster_NDB_IP>:8443 --verbose --prompt --keystore-password <keystore-password>
--truststore-password <truststore-password>
```

Upgrading NDB - Hitless Method (Using CLI)

You can upgrade Cisco NDB to Release 3.9.2 with the hitless method using CLI.

Before you begin

If the Cisco NDB version is earlier than Release 3.8, you must edit the config.ini file and update the **skipConfigurtionStateDBfiles** key to false on both the controllers, and restart all the earlier version controllers.

Step 1 Stop both the servers.

Step 2 Navigate to the the s server location `/home/3.9.2/xnc/bin` and enter the **. /xnc upgrade --perform --target-home {xnc directory to be upgraded} --verbose** command.

Note You must provide the location of the XNC directory in the target home. For example, provide the location of the 3.9.2 XNC directory which is /home/3.9.2/xnc.

Step 3 Navigate to the the secondary server location `/home/3.9.2/xnc/bin` and enter the **. /xnc upgrade --perform --target-home {xnc directory to be upgraded} --verbose** command.

Note You must provide the location of the XNC directory in the target home. For example, provide the location of the 3.9.2 XNC directory which is /home/3.9.2/xnc.

Step 4 If TLS certification is enabled between NDB server and NXOS switch, copy the tlsTrustStore and tlsKeyStore files to /xnc/configuration from the old xnc backup in the primary and secondary servers.

Step 5 Navigate to the Cisco NDB Release 3.9.2 XNC directory in the primary server and start Cisco NDB using the **./runxnc.sh –start** command.

Step 6 Login to Cisco NDB and verify that the Cisco NDB version is displayed as Release 3.9.2. Verify that the primary configuration and the other configurations are retained.

Step 7 If secondary / cluster NDB server is configured, start the server.

Note If TLS certification is enabled, start the secondary/ cluster using the commands as shown below:

```
./runxnc.sh -tls -tlskeystore ./configuration/tlsKeyStore -tlstruststore
./configuration/tlsTrustStore
cd bin
./xnc config-keystore-passwords --user <NDB_username> --password <NDB_password> --url
https://<Cluster_NDB_IP>:8443 --verbose --prompt --keystore-password <keystore-password>
--truststore-password <truststore-password>
```

GUI Notifications during Install/ Upgrade

Beginning with Release 3.9.2, the GUI behavior has changed while installing or upgrading the NDB controller software. The GUI is in a *read-only* state until the whole installation or upgradation procedure is completed. You will see relevant messages at the top of the NDB GUI indicating the current background process/ event that is in progress. Wait for a *Ready* message to appear at the top of the GUI screen before you make any configuration changes. This change is behavior is to facilitate smooth install and upgrade as NDB is not stabilized while the install or upgrade is in progress. This is applicable to both the upgrades— HA and standalone.

Some of the messages that appear at the top of the screen indicating the completed events or background processes are:

- Message indicating the GUI is ready to accept configuration(s)— *NDB is ready for configuration* .
- (for HA) Message indicating that the primary is loaded and it is time for the members in the cluster— *Primary is ready and bring up the members.*
- During cluster rehashing, when members are joining/ leaving the quorum — *Cluster is rehashing.*

Note Messages are displayed in red until NDB is ready. After NDB is ready, the message, *NDB is ready for configurations* is displayed in green.

For HA upgrade, when the Primary is ready, a small green tick-mark appears at the cluster information (see illustration, below); the corresponding message displayed at the top is, *Primary is Ready, bring up the members* . You can hover over to see the members of the cluster.

Figure 1: GUI enhancement - Primary is Ready Notification

For standalone, wait for the *NDB is ready for configuration* message to be displayed at the top of the screen to perform configurations.

The configuration buttons are either disabled, or are temporarily removed, until the installation / upgradation is complete. Some examples are provided here.

Under **Connections** > **User Connections**, the configuration buttons are temporarily removed.

Figure 2: GUI enhancement - Connections (without configuration buttons)

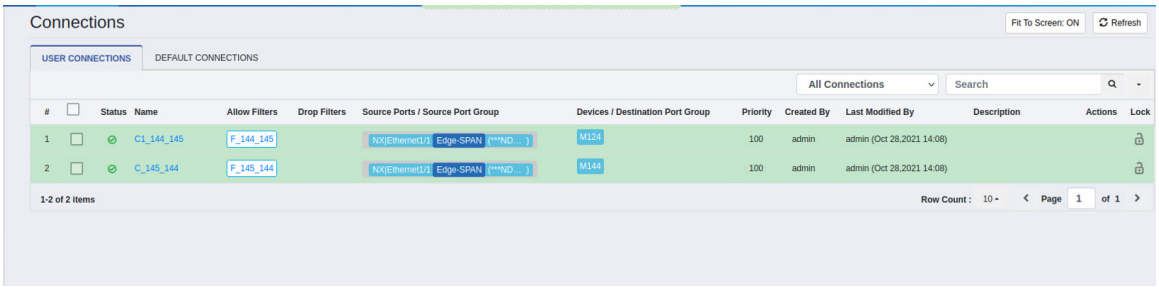
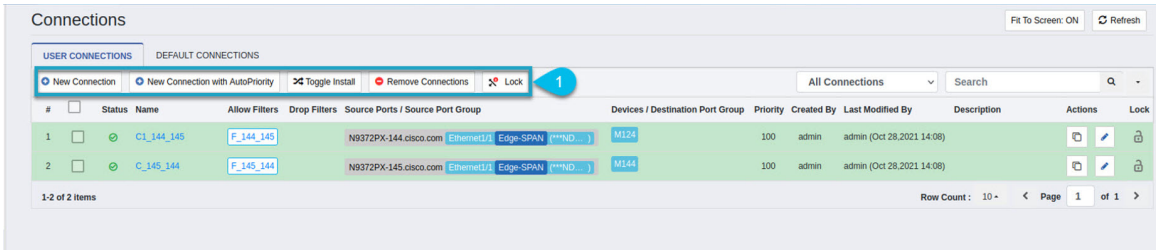


Figure 3: GUI enhancement - Connections (with configuration buttons)



Under **Devices** > **Device Connections**, the configuration buttons are temporarily disabled.

Figure 4: GUI enhancement - Devices (configuration buttons are disabled)

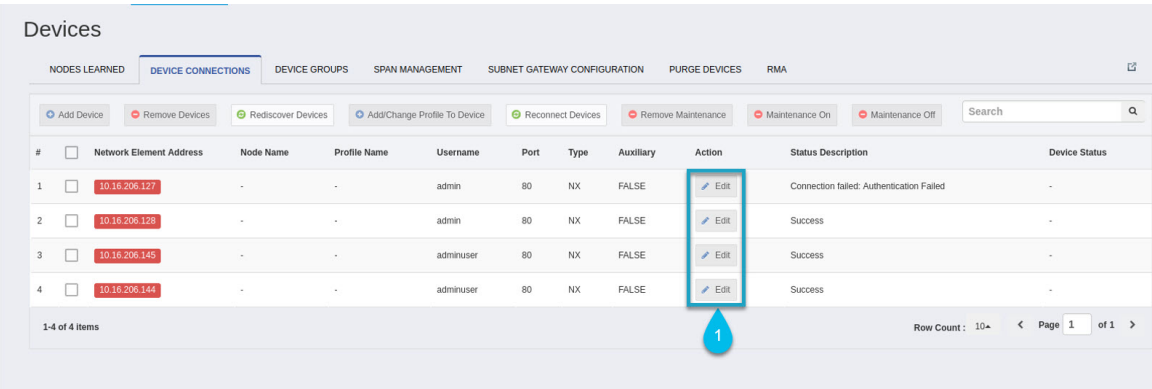
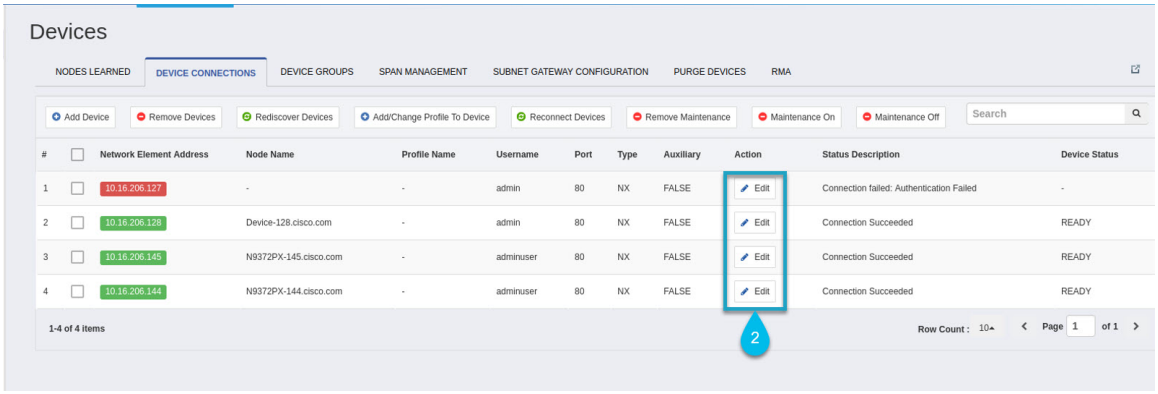


Figure 5: GUI enhancement - Devices (configuration buttons are enabled)



Starting the Application

Note When you are running xnc for the first time, the URL that you need to connect to and the port that it is listening on are displayed on the screen. For example, when you run the ./runxnc.sh script, the following message is displayed on the screen: Web GUI can be accessed using below URL: *[https://<IP_address>:8443]*.

You can use one of the following options:

Option	Description
-jmxport *port_number*	Enables JMX remote access on the specified JVM port.
-debugport *port_number*	Enables debugging on the specified JVM port.
-start	Starts NDB.
-start *port_number*	Starts NDB on the specified port.
-stop	Stops NDB.

Option	Description
-restart	Restarts NDB.
-status	Displays the NDB status with process ID.
-console	Starts NDB with the login console.
-help	Displays the options for the **./runxnc.sh** command.
-tls	To enable TLS, start the controller by entering the **./runxnc.sh -tls -tlskeystore** *keystore_file_location* **-tlstruststore** *truststore_file_location* command.
-osgiPasswordSync	To set the OSGi web console password same as the XNC password if the XNC password is changed. **Note** This step is optional. If the application is started without this option, the OSGi console can be accessed through the default credentials.

Note Use runxnc.sh script to start Cisco Nexus Data Broker. You have to set a path variable named JAVA_HOME. It sets the path variables that are used for startup and launches the OSGi framework with the specified options. If a user attempts to start the Cisco Nexus Data Broker application with Java version lower than 1.7, an error message is displayed and the application aborts. To resolve the issue, upgrade your current Java version and restart Cisco Nexus Data Broker. If the current Java Version used is lower than 1.8.0_45, a warning message is issued before the start that Upgrade to 1.8.0_45 or above is recommended.

Verifying The Application Status

Step 1 Navigate to the `ndb` directory that was created when you installed the software.

Step 2 Verify that the application is running by entering the **./runndb.sh -status** command.

The controller outputs the following, which indicates that the controller is running the Java process with PID 21680:

```
Controller with PID:21680 -- Running!
```

What to do next

Connect the switches to the controller. For more information, see the configuration guide for your switches.