Logging in and Managing Cisco Extensible Network Controller

This chapter contains the following sections:

Logging in to the Application GUI

You must log into the Cisco XNC GUI using HTTPS.

The default HTTPS web link for the Cisco XNC GUI is `https://Controller_IP:8443`

Step 1 In your web browser, enter the Cisco XNC GUI web link.

Step 2 On the launch page, do the following:

a) Enter your username and password.
The default username and password is admin/admin.

b) Click **Log In**.

Configuring Cisco Extensible Network Controller

Configuring High Availability Clusters

Cisco Extensible Network Controller (XNC) supports high availability clustering in active/active mode with up to five controllers. To use high availability clustering with Cisco XNC, you must edit the `config.ini` file for each instance of Cisco XNC.

Before You Begin

- All IP addresses must be reachable and capable of communicating with each other.
- All switches in the cluster must connect to all of the controllers.
- All controllers must have the same HA clustering configuration information in the `config.ini` files.
- All controllers must have the same information in the `xnc/configuration/startup` directory.
- If using cluster passwords, all controllers must have the same password configured in the `xncjgroups.xml` file. See Password Protecting the High Availability Clusters, on page 3.

Step 1 Ensure that Cisco XNC is not running on any of the instances in the cluster.

Step 2 Open a command window on one of the instances in the cluster.

Step 3 Navigate to the `xnc/configuration` directory that was created when you installed the software.

Step 4 Use any text editor to open the `config.ini` file.

Step 5 Locate the following text:

```
# HA Clustering configuration (colon-separated IP addresses of all controllers that are part of the
 cluster.)
# supernodes=<ip1>:<ip2>:<ip3>:<ipn>
```

Step 6 Remove the comments on the # supernodes line, and replace <ip1>:<ip2><ip3>:<ipn> with the IP addresses for each instance of Cisco XNC in the cluster. You can enter from two to five IP addresses.

Step 7

Example:

```
# HA Clustering configuration (colon-separated IP addresses of all controllers that are part of the
 cluster.)
supernodes=10.1.1.1:10.2.1.1:10.3.1.1:10.4.1.1:10.5.1.1
```

Step 8 Save the file and exit the editor.

Step 9 Repeat Step 3 through Step 7 for each instance of Cisco XNC in the cluster.

Step 10 Restart Cisco XNC.

Password Protecting the High Availability Clusters

You can password protect your HA clusters with the `xncjgroups.xml` file. This file must be exactly the same for each instance of Cisco Extensible Network Controller (XNC).

Step 1 Ensure that Cisco XNC is not running on any of the instances in the cluster.

Step 2 Open a command window on one of the instances in the cluster.

Step 3 Navigate to the `xnc/configuration` directory.

Step 4 Use any text editor to open the `xncjgroups.xml` file.

Step 5 Locate the following text:

```
<!-- <AUTH auth_class="org.jgroups.auth.MD5Token" auth_value="ciscoXNC" token_hash="MD5"></AUTH> -->
```

Step 6 Remove the comments from the AUTH line.

Example:

```
<AUTH auth_class="org.jgroups.auth.MD5Token" auth_value="ciscoXNC" token_hash="MD5"></AUTH>
```

Step 7 (Optional) Change the password in the auth_value attribute.
By default, the cluster is protected with the password "ciscoXNC". You can change this password to whatever value you want, if you make the same change on all machines in the cluster.

Step 8 Save the file and exit the editor.

Step 9 Repeat Step 4 through Step 8 for each instance of Cisco XNC in the cluster.

Step 10 Restart Cisco XNC.

Editing the Configuration Files for Cisco Nexus Switches

The following configuration settings can improve scalability when connecting to Cisco Nexus 3000 or 3100 Series switch.

Step 1 Navigate to the `xnc/configuration` directory that was created when you installed the software.

Step 2 Use any text editor to open the `config.ini` file.

Step 3 Update the following parameters:

Name	Predefined Value	Default Value	Recommended Value
of.messageResponseTimer	10000	2000	60000
of.switchLivenessTimeout	—	60500	120500
of.flowStatsPollInterval	120	10	240
of.portStatsPollInterval	300	5	240

Name	Predefined Value	Default Value	Recommended Value
of.descStatsPollInterval	—	60	240
of.barrierMessagePriorCount	50	100	50
of.discoveryInterval	—	300	300
of.discoveryTimeoutMultiple	—	2	2

Note Predefined values are the values that Cisco includes in the `config.ini` file that is shipped with Cisco XNC. A em dash ("—") in this column of the table means that unless you explicitly update the value, the default value will be used.

Step 4 Save the file and exit the editor.

Step 5 Restart Cisco XNC.

Backing Up or Restoring the Configuration

The backup and restore commands allow you to back up your Cisco Extensible Network Controller (XNC) configurations and restore them.

Step 1 Open a command window where you installed Cisco XNC.

Step 2 Navigate to the `xnc/bin` directory that was created when you installed the software.

Step 3 Back up the configuration by entering the **./xnc config --backup** command.
The **--backup** option creates a backup archive (in .zip format) of the startup configuration in the current `xnc` distribution. The backup archive is stored in `{xncHome}/backup/`. A new archive is created each time that the backup command is entered using a filename with the current timestamp.

Step 4 Restore the configuration by entering the **./xnc config --restore --backupfile** {*zip_filename*} command.
The **--restore** option restores the startup configuration of the current `xnc` distribution from an existing backup archive. The restore action requires the absolute path of the backup archive.

Step 5 If you are restoring a configuration, stop and restart Cisco XNC for the restored configuration to take effect.

Recovering the Administrative Password

The Cisco Extensible Network Controller (XNC) network administrator user can return the administrative password to the factory default.

Note The software may or may not be running when this command is used. If the it is not running, the password reset takes effect the next time that it is run.

Step 1 Open a command window where you installed Cisco XNC.

Step 2 Navigate to the `xnc/bin` directory that was created when you installed the software.

Step 3 Reset the administrative password by entering the **./xnc reset-admin-password** [**--wait-seconds** {*wait_time*} **--password** {*password*}] command.
Resets the admin password to the default or specified password by restarting the user manager.

- The **wait-seconds** is the length of time, in seconds, to wait for the user manager to restart. The minimum is 5 seconds and the maximum is 60 seconds.
- The **password** is the administrative password.

Note
- The password must be from 8 to 256 characters, contain both uppercase and lowercase characters, and have at least one number and one nonalphanumeric character.
- If you leave the password blank, it is reset to the factory default of "admin".
- Each time that you reset the administrative password, make sure that the new password meets these requirements or you will not be able to log in to Cisco XNC.

Uninstalling the Application Software

Before You Begin

Ensure that your Cisco Extensible Network Controller (XNC) application is stopped before proceeding.

Step 1 Navigate to the directory where you created the Cisco XNC installation.
For example, if you installed the controller in `Home/CiscoXNC`, navigate to the `Home` directory.

Step 2 Delete the `CiscoXNC` directory.