



Administrative Tasks

This chapter contains the following sections:

- [About AAA Servers, page 1](#)
- [Users and Roles, page 3](#)
- [Viewing Cluster Management Information, page 5](#)
- [Viewing the OSGi Console, page 6](#)
- [Viewing the Northbound API Content, page 7](#)

About AAA Servers

AAA enables the security appliance to determine who the user is (authentication), what the user can do (authorization), and what the user did (accounting). Cisco Extensible Network Controller (XNC) uses Remote Authentication Dial-In User Service (RADIUS) or Terminal Access Controller Access-Control System Plus (TACACS+) to communicate with an AAA server.

Remote authentication and authorization is supported using the AAA server. To authenticate each user, Cisco Extensible Network Controller (XNC) uses both the login credentials and an attribute-value (AV) pair that assigns the authorized role for the user as part of the user administration. After successful authentication, the Cisco AV pair is returned to Cisco Extensible Network Controller (XNC) for resource access authorization.

Adding an AAA Server

Step 1 From the **Admin** drop-down list, choose **AAA**.

Step 2 In the **AAA Configuration** dialog box, click **Add Server**.

Step 3 In the **Add AAA Server** dialog box, complete the following fields:

Name	Description
Server Address field	The IP address of the AAA server.

Name	Description
Server Secret field	The shared secret configured on the AAA server.
Protocol drop-down list	Choose the protocol for the AAA server. This can be one of the following: <ul style="list-style-type: none"> • Radius+ • TACACS+

Step 4 Click **Save**.

What to Do Next

If you chose RADIUS as the protocol for the AAA server, you need to configure user authentication for RADIUS.

Configuring User Authentication for RADIUS Server

User authorization on a RADIUS server must conform to the Cisco Attribute-Value (av-pair) format.

In the RADIUS server, configure the Cisco av-pair attribute for a user as follows:

```
shell:roles="Network-Admin Slice-Admin"
```

Viewing an AAA Server

-
- Step 1** From the **Admin** drop-down list, choose **AAA**.
- Step 2** In the **AAA Configuration** dialog box, click a server address.
- Step 3** After viewing the server information in the **Remove AAA Configuration** dialog box, click **Close**.
- Step 4** In the **AAA Configuration** dialog box, click **Close**.
-

Deleting an AAA Server

-
- Step 1** From the **Admin** drop-down list, choose **AAA**.
- Step 2** In the **AAA Configuration** dialog box, click a server address.
- Step 3** In the **Remove AAA Configuration** dialog box, click **Remove**.
- Step 4** In the **AAA Configuration** dialog box, click **Close**.
-

Users and Roles

Cisco Extensible Network Controller (XNC) uses users and roles to manage user access. You can assign more than one role to a user. This can be one of the following:

- **Network Administrator**—Provides full administrative privileges to all Cisco Extensible Network Controller (XNC) applications.
- **Network Operator**—Provides read-only privileges to the specified Cisco Extensible Network Controller (XNC) applications.
- **Application User**—Provides privileges that are defined in the specified application.
- **Slice User**—Provides access to a specified slice.

Each user is assigned a role, which determines the permissions that they have. Slice users are assigned to both a role and a slice. The Admin user with the Network Administrator role is created by default when you install Cisco Extensible Network Controller (XNC).

Viewing User Information

-
- Step 1** From the **Admin** drop-down list, choose **Users**.
- Step 2** In the **User Management** dialog box, you can do the following:
- View a list of usernames and the roles assigned to each user.
 - Click an existing user to delete the user or change the password for the user.
 - Click **Add User** to create a new user.
- Step 3** When you are finished, click **Close**.
-

Adding a User

After creating a user, you can change the password, but you cannot change the roles assigned to the user.

Step 1 From the **Admin** drop-down list, choose **Users**.

Step 2 In the **User Management** dialog box, click **Add User**.

Step 3 In the **Add User** dialog box, complete the following fields:

Name	Description
Username field	<p>The name that you want to assign to the user.</p> <p>A username can be between 1 and 32 alphanumeric characters and contain any special character except a period ("."), forward slash ("/"), pound sign ("#"), percent sign ("%"), semicolon (";"), question mark ("?"), or backslash ("\").</p>
Password field	<p>The password for the user.</p> <p>Passwords must be between 8 and 256 characters long, contain uppercase and lowercase characters, have at least one numeric character, and have at least one nonalphanumeric character.</p>
Choose Role(s) drop-down list	<p>Choose the role that you want to assign to the user. You can assign more than one role. This can be one of the following:</p> <ul style="list-style-type: none"> • Network Administrator—Provides full administrative privileges to all Cisco Extensible Network Controller (XNC) applications. • Network Operator—Provides read-only privileges to the specified Cisco Extensible Network Controller (XNC) applications. • Application User—Provides privileges that are defined in the specified application. • Slice User—Provides access to a specified slice.
Role Name field	<p>If you chose Application User, enter the name that you want to assign to the role.</p>
Slices drop-down list	<p>If you chose Slice User, choose the slice that you want to assign to the user.</p>
Slice Role drop-down list	<p>If you chose Slice User, choose the role that you want to assign to the user. This can be one of the following:</p> <ul style="list-style-type: none"> • Administrator—Provides full administrative privileges to the specified slice. • Operator—Provides read-only privileges to the specified slice.
Assign button	<p>Assigns a role to the user.</p>

- Step 4** Click **Add User**.
- Step 5** In the **User Management** dialog box, click **Close**.
-

Changing the Password for an Existing User

- Step 1** From the **Admin** drop-down list, choose **Users**.
- Step 2** In the **User Management** dialog box, click the user that you want to modify.
- Step 3** In the **Edit User** dialog box, click **Change Password**.
- Step 4** In the **Change Password** dialog box, enter the new password and then enter it a second time to verify.
- Step 5** Click **Submit**.
- Step 6** In the **User Management** dialog box, click **Close**.
-

Deleting a User

If you are signed in as a particular user, you cannot delete that user.

-
- Step 1** From the **Admin** drop-down list, choose **Users**.
- Step 2** In the **User Management** dialog box, click the user that you want to modify.
- Step 3** In the **Edit User** dialog box, click **Remove User**.
- Step 4** In the **User Management** dialog box, click **Close**.
-

Viewing Cluster Management Information



Note The cluster management dialog boxes are read-only.

Before You Begin

You must have configured high availability clustering in order to view the cluster management information. See the *Cisco Extensible Network Controller Deployment Guide*.

-
- Step 1** From the **Admin** drop-down list, choose **Clusters**.
The **Cluster Management** dialog box lists the IP addresses of all of the Cisco Extensible Network Controller (XNC) instances in the cluster. Clusters can be denoted by one of the following icons:
- The * icon indicates the cluster node that is currently being viewed.
 - The C icon indicates that the cluster node is the coordinator.
- Step 2** In the **Cluster Management** dialog box, choose a cluster.
The **Connected Nodes** dialog box lists all of the nodes in the selected cluster.
- Step 3** In the **Connected Nodes** dialog box, click **Close**.
- Step 4** In the **Cluster Management** dialog box, click **Close**.
-

Viewing the OSGi Console

You can view all of Cisco Extensible Network Controller (XNC) bundles that comprise the application by viewing the OSGi Web Console.



Note This procedure does not provide a step-by-step guide to everything you can do in the OSGi Web Console for **Cisco XNC Bundles** list. It guides you in opening the OSGi Web Console and viewing Cisco XNC bundle information.

-
- Step 1** From the **Admin** drop-down list, choose **OSGi**.
A new browser tab opens.
- Step 2** Enter your username and password, and then press **Enter**.
The **Cisco – XNC Bundles** list is displayed. In this page you can view all of the active packages, filter on the package name to specify bundle names, and complete other tasks.
- Step 3** When you are finished viewing the **Cisco XNC Bundles** list, close the **Cisco XNC – Bundles** browser tab.
-

Viewing the Northbound API Content

You can view all of Cisco Extensible Network Controller (XNC) northbound API content for the application by opening a browser tab using the **Northbound API** tool (book icon) in the menu bar.

Step 1

From the menu bar, click the **Northbound API** button.

A new browser tab (Swagger UI) is opened and the complete list of northbound API content used in Cisco XNC is displayed.

From this tab, you can do the following:

- Show or hide the operations for an API.
- List the operations for an API.
- Expand the operations for an API.

Step 2

When you are finished viewing northbound API content, close the browser tab.
