Administrative Tasks

This chapter contains the following sections:

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 XNC uses Remote Authentication Dial-In User Service (RADIUS) or Terminal Access Controller Access-Control System Plus (TACACS+) to communicate with a AAA server.

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

Adding an AAA Server

Step 1   On 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.
Server Secret field	The shared secret configured on the AAA server.

Name	Description
Protocol drop-down list	Choose the protocol for the AAA server. This can be one of the following: • **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 theCisco av-pair attribute for a user as show below:

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

Viewing a AAA Server

Step 1   On 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 a AAA Server

Step 1   On 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 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 XNC applications.

- **Network Operator**—Provides read-only privileges to the specified Cisco 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 XNC.

Viewing User Information

Step 1   On 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 On 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	The name that you want to assign to the user. A user name may be between 1 and 32 non-blank alphanumeric characters and contain any special character except a period (.), forward slash (/), pound sign (#), percent sign (%), semi-colon (;), question mark (?), or back slash (\).
Password field	The password for the user. Passwords must be between 8 and 256 characters long, contain upper case and lower case letters, at least one numeric character, and at least one non-alphanumeric character.
Choose Role(s) drop-down list	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: • **Network Administrator**—Provides full administrative privileges to all Cisco XNC applications. • **Network Operator**—Provides read-only privileges to the specified Cisco XNC applications. • **Application User**—Provides privileges that are defined in the specified application. • **Slice User**—Provides access to a specified slice.
Role Name field	If you chose **Application User**, enter the name that you want to assign to the role.
Slices drop-down list	If you chose **Slice User**, choose the slice that you want to assign to the user.
Slice Role drop-down list	If you chose **Slice User**, choose the role that you want to assign to the user. This can be one of the following: • **Administrator**—Provides full administrative privileges to the specified slice. • **Operator**—Provides read-only privileges to the specified slice.
Assign button	Assigns a role to the user.

Step 4   Click **Add User**.

Step 5   In the **User Management** dialog box, click **Close.**

Changing the Password for an Existing User

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

Step 2   In the **User Management** dialog box, click on 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   On the **Admin** drop-down list, choose **Users**.

Step 2   In the **User Management** dialog box, click on 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   On the **Admin** drop-down list, choose **Clusters**.
The **Cluster Management** dialog box lists the IP addresses of all of the Cisco 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 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**. It a brief procedure that guides you in opening the OSGi Web Console and viewing Cisco XNC bundle information.

Step 1   On the Cisco XNC menu bar, click **Admin** and select **OSGi**.
A new browser tab opens.

Step 2   Enter your **User Name** and **Password**, 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**, close the browser tab.