CHAPTER 15

Controlling User Access

This chapter contains the following sections:

- Managing Users, page 15-1
- Changing User Passwords, page 15-2
- Changing User Privileges, page 15-2
- Managing User Groups, page 15-3
- Changing Password Policy, page 15-4
- Setting the AAA Mode, page 15-4
- Changing Virtual Domains, page 15-4
- Auditing Access, page 15-5
- Viewing Audit Logs, page 15-6
- Adding TACACS+ Server, page 15-7
- Adding a RADIUS Server, page 15-7

Managing Users

All Prime NCS (WAN) users have basic parameters such as user name and password. Users with admin privileges can view active user sessions.

To view active sessions:

Step 1 Choose **Administration > Users, Roles & AAA**, then click **Active Sessions**.

Step 2 Click the **Audit Trail** icon to for the username for which you want to see the following data:

- User—User login name
- Operation—Type of operation audited
- Time—Time operation was audited
- Status—Success or failure
- Reason—Failure reason when the user login failed
- Configuration Changes—This field provides a Details link if there are any configuration changes. Click on the Details link for more information on the configuration changes done by an individual user.

Note The audit trail entries could be logged for individual device changes. For example, If a template is applied on multiple switches, then there will be multiple audit entries for each switch to which the template has been applied.

Adding a User

You can add a user and assign predefined static roles. Besides complete access, you can give administrative access with differentiated privileges to certain user groups. Prime NCS (WAN) supports external user authentication using these access restrictions and authenticates the users against the TACACS+ and RADIUS servers.

Step 1 Choose **Administration > Users, Roles & AAA**, then click **Users**.

Step 2 Choose **Add a User**, then click **Go**.

Step 3 Enter the username, password, and confirm password for the new user, then choose the groups to which this user belongs.

Step 4 Click the Virtual Domains tab to assign a virtual domain to this user. See Changing Virtual Domains.

Step 5 Click **Save**.

Changing User Passwords

To change the password for a user:

Step 1 Choose **Administration > Users, Roles & AAA**, then click **Users**.

Step 2 Select the user name who's password you want to change.

Step 3 Complete password fields, then click **Save**.

Changing User Privileges

Prime NCS (WAN) uses a list of tasks to control which part of Prime NCS (WAN) users can access and the functions they can perform in those parts. You change user privileges in Prime NCS (WAN) by changing the User Group to which each user belongs. You use the User Group Task List to change what users in each group are authorized to do and the screens they can access.

You can also assign the sites or devices to which a virtual domains has access.

To edit the task list for a user group:

Step 1 Choose **Administration > Users, Roles & AAA**, then click **User Groups**.

Step 2 Click on a group name to change the tasks this group is allowed to perform.

Step 3 Click the Members tab to view the users of this group.

Managing User Groups

Prime NCS (WAN) has pre-defined user groups as described in. You can change the privileges for the users, but you cannot add additional users. When you create a new user, you assign that user to a group.

Table 15-1 describes the Prime NCS (WAN) default user groups and their privileges.

Table 15-1 Default User Groups

Group Name	Privileges for Users in the Group
System Monitoring	Monitor Prime NCS (WAN) operations.
ConfigManagers	Monitor and configure Prime NCS (WAN) operations.
Admin	Monitor and configure Prime NCS (WAN) operations and perform all system administration tasks except administering Prime NCS (WAN) user accounts and passwords.
SuperUsers	Monitor and configure Prime NCS (WAN) operations and perform all system administration tasks including administering Prime NCS (WAN) user accounts and passwords. Superusers tasks can be changed.
North bound API	Used only with Prime NCS (WAN) Navigator.
User Assistant	Local net user administration only. User assistants cannot configure or monitor devices.
Lobby Ambassador	Guest access for only configuration and managing of user accounts.
Monitor lite	Monitoring of assets location.
Root	Monitor and configure Prime NCS (WAN) operations and perform all system administration tasks including changing any passwords. Only one user can be assigned to this group and is determined upon installation. It cannot be removed from the system, and no task changes can be made for this user.

To view user groups and their associated tasks:

Step 1 Choose **Administration > Users, Roles & AAA**, then click **User Groups**.

Step 2 Click on a group name to change the tasks this group is allowed to perform.

Step 3 Click the Members tab to view the users of this group.

Changing Virtual Domain Access

To edit the sites or devices to which a virtual domains has access:

Step 1 Choose **Administration > Virtual Domains**.

Step 2 Select the domain to which you want to assign sites or devices.

Step 3 Click the **Sites** or **Devices** tab, then move the necessary items from the Available list to the Selected list.

Step 4 Click **Submit**.

To associate users to Virtual Domains, choose **Administration > Users, Roles & AAA**, then click **Users**. See Assigning Users to a Virtual Domain.

Changing Password Policy

Prime NCS (WAN) supports various password policy controls, such as minimum length, repeated characters, etc.

To change password policies:

Step 1 Choose **Administration > Users, Roles & AAA**, then click **Local Password Policy**.

Step 2 Chose the necessary policies, then click **Save**.

Setting the AAA Mode

Prime NCS (WAN) supports local as well as TACACS+ and RADIUS, but you must specify a TACACS+ or RADIUS server first.

To specify a TACACS+ server and then change the AAA mode to TACACS+:

Step 1 Choose **Administration > Users, Roles & AAA**, then click **TACACS+**.

Step 2 From the command pull-down menu, choose Add TACACS+ Server, then click **Go**.

Step 3 Enter the TACACS+ server parameters, then click **Save**.

Step 4 Click **AAA Mode**.

Step 5 Select TACACS+ and specify whether to enable fallback to the local condition.

Step 6 Click **Save**.

Changing Virtual Domains

A Prime NCS (WAN) Virtual Domain consists of a set of Prime NCS (WAN) devices and/or maps and restricts a user view to information relevant to these managed objects.

Through a virtual domain, an administrator can ensure that users are only able to view the devices and maps for which they are responsible. In addition, because of the virtual domain filters, users are able to configure, view alarms, generate reports for *only* their assigned part of the network.

The administrator specifies for each user a set of allowed virtual domains. Only one of these can be active for that user at login. The user can change the current virtual domain by selecting a different allowed virtual domain from the Virtual Domain drop-down list at the top of the page. All reports, alarms, and other functionality are now filtered by that virtual domain.

If there is only one virtual domain defined ("root") in the system AND the user does not have any virtual domains in the custom attributes fields in the TACACS+/RADIUS server, the user is assigned the "root" virtual domain by default. If there is more than one virtual domain, and the user does not have any specified attributes, then the user is blocked from logging in.

To add sites and devices to a virtual domain:

Step 1 Choose **Administration > Virtual Domains**.

Step 2 From the left Virtual Domain Hierarchy sidebar menu, click the virtual domain to which you want to add a site or device.

Step 3 Move the sites and devices from the Available to the Selected column, then click **Submit**.

To add a user to a virtual domain:

Step 1 Choose **Administration > Users, Roles & AAA**, then click **Users**.

Step 2 Click on the user you want to add to a virtual domain.

Step 3 Click the Virtual Domains tab.

Step 4 Move the virtual domain to which you want to add the user from the Available Virtual Domains column to the Selected Virtual Domains column, then click **Save**.

Note Each virtual domain may contain a subset of the elements included with its parent virtual domain. When a user is assigned a virtual domain, that user can view the devices that are assigned to its virtual domain.

Auditing Access

Prime NCS (WAN) maintains an audit record of user access.

To access the audit trail for a user or user's active sessions:

Step 1 Choose **Administration > Users, Roles & AAA**, then click **Active Sessions**.

Step 2 Click the **Audit Trail** icon to for the username for which you want to see the following data:

- User—User login name
- Operation—Type of operation audited
- Time—Time operation was audited
- Status—Success or failure

- Configuration Changes—This field provides a Details link if there are any configuration changes. Click on the Details link for more information on the configuration changes done by an individual user.

Note The audit trail entries could be logged for individual device changes. For example, If a template is applied on multiple switches, then there will be multiple audit entries for each switch to which the template has been applied.

To access the audit trail for a user group:

Step 1 Choose **Administration > Users, Roles & AAA**, then click **User Groups**.

Step 2 Click the **Audit Trail** icon to for the username for which you want to see the following data:

- User—User login name
- Operation—Type of operation audited
- Time—Time operation was audited
- Status—Success or failure
- Configuration Changes—This field provides a Details link if there are any configuration changes. Click on the Details link for more information on the configuration changes done by an individual user.

Note The audit trail entries could be logged for individual device changes. For example, If a template is applied on multiple switches, then there will be multiple audit entries for each switch to which the template has been applied.

Viewing Audit Logs

Prime NCS (WAN) provides two types of audit logs:

- Application Audit logs—Logs events that pertain to the Prime NCS (WAN) features. For example, you can view the application audit log to see when a particular user logged in and what actions were taken.
- Network Audit logs—Logs events related to the devices in your network. For example, you can view the network audit logs to see which user deployed a specific template and the date and time the template was deployed.

Step 1 Choose **Administration > Audit Logs**.

Step 2 Click the **Application Audit** or **Network Audit** tab.

Note For Application Audit, the User Group column is blank for TACACS+/RADIUS users.

Step 3 To view details about the log, click to expand the row for which you want to view details.

Adding TACACS+ Server

To configure Prime NCS (WAN) so it can communicate with the TACACS+ server:

Step 1 Choose **Administration > Users, Roles & AAA**, then click **TACACS+**.

Step 2 Choose Add TACACS+ Server, then click **Go**.

Step 3 Enter the TACACS+ server information, then click **Save**.

Note For Prime NCS (WAN) to communicate with the TACACS+ server, the shared secret you enter on this page must match the shared secret configured on the TACACS+ server.

Adding a RADIUS Server

To configure Prime NCS (WAN) so it can communicate with the RADIUS server:

Step 1 Choose **Administration > Users, Roles & AAA**, then click **RADIUS Servers**.

Step 2 Choose Add Radius Server, then click **Go**.

Step 3 Enter the RADIUS server information, then click **Save**.

Note For Prime NCS (WAN) to communicate with the RADIUS server, the shared secret you enter on this page must match the shared secret configured on the RADIUS server.