CHAPTER 28

Controlling User Access

This chapter contains the following sections:

Managing Users

All Prime Infrastructure 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 Infrastructure 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**.

Managing Lobby Ambassador Accounts

You can use the Cisco Lobby Ambassador to create guest user accounts in Prime Infrastructure. A guest network provided by an enterprise allows access to the Internet for a guest without compromising the host. The web authentication is provided with or without a supplicant or client, so a guest needs to initiate a VPN tunnel to their desired destinations.

Both wired and wireless guest user access is supported. Wired guest access enables guest users to connect to the guest access network from a wired Ethernet connection designated and configured for guest access. Wired guest access ports might be available in a guest office or specific ports in a conference room. Like wireless guest user accounts, wired guest access ports are added to the network using the lobby ambassador feature.

The network administrator must first set up a lobby ambassador account. This allows a nontechnical person to create and manage guest user accounts on the Prime Infrastructure. Guest user accounts are for visitors such as temporary workers who need network access.

This section contains the following topics:

Creating a Lobby Ambassador Account

Note A group that has the SuperUser/administrator privileges (by default) can create a lobby ambassador account.

To create a lobby ambassador account in Prime Infrastructure:

Step 1 Log into Prime Infrastructure user interface as an administrator.

Step 2 Choose **Administration > Users, Roles & AAA**.

Step 3 From the left sidebar menu, choose **Users**.

Step 4 From the Select a command drop-down list, choose **Add User**.

Step 5 Click **Go**.

Step 6 Enter the username.

Step 7 Enter the password. Reenter to confirm the password. Password requirements include the following:

- The password must have a minimum of eight characters.
- The password must include at least three of the following elements: lowercase letters, uppercase letters, numbers, or special characters.

Step 8 In the Groups Assigned to this User section, select the **LobbyAmbassador** check box to access the Lobby Ambassador Defaults tab.

The Lobby Ambassador Defaults tab has the following parameters:

- Profile—The default profile to which the guest users would connect.
- Lifetime—Limited or Unlimited.

  Note By default, the lifetime is limited to eight hours.

- Apply to—From the drop-down list, choose one of the following:
  - **Indoor Area**—Campus, Building, and Floor.
  - **Outdoor Area**—Campus, Outdoor Area.
  - **Controller List**—List of controller(s) on which the selected profile is created.
  - **Config Groups**—Config group names configured on Prime Infrastructure.
- Email ID—The e-mail ID of the host to whom the guest account credentials are sent.
- Description—A brief description of this account.
- Disclaimer—The default disclaimer text.
- Defaults Editable—Select this check box if you want to allow the lobby ambassador to override these configured defaults. This allows the lobby ambassador to modify these Guest User Account default settings while creating Guest Accounts from the Lobby Ambassador portal.

  Note If no default profile is selected on this tab, the defaults are not applied to this Lobby Ambassador. However, the Lobby Ambassador account is created and the Lobby Ambassador can create users with credentials as desired.

- Max User Creation Allowed—Select this check box to set limits on the number of guest users that can be created by the Lobby Ambassador in a given time period. The time period is defined in hours, days, or weeks.

Step 9 Click **Save**. The name of the new lobby ambassador account is listed and the account can be used immediately.

Logging the Lobby Ambassador Activities

The following activities are logged for each lobby ambassador account:

- Lobby ambassador login—The Prime Infrastructure logs the authentication operation results for all users.
- Guest user creation—When a lobby ambassador creates a guest user account, the Prime Infrastructure logs the guest username.
- Guest user deletion—When a lobby ambassador deletes the guest user account, the Prime Infrastructure logs the deleted guest username.
- Account updates—The Prime Infrastructure logs the details of any updates made to the guest user account. For example, increasing the life time.

To view the lobby ambassador activities:

Note You must have administrative permissions to open this window.

Step 1 Log into the Prime Infrastructure user interface as an administrator.

Step 2 Choose **Administration > Users, Roles & AAA > User Groups** from the left sidebar menu to display the User Groups page.

Step 3 On the User Groups page, click the **Audit Trail** icon for the lobby ambassador account you want to view. The Audit Trail page for the lobby ambassador appears.

This page enables you to view a list of lobby ambassador activities over time.

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

Step 4 To clear the audit trail, choose **Clear Audit Trail** from the Select a command drop-down list, and click **Go**.

Managing Guest User Accounts

The lobby ambassador can create the following types of guest user accounts:

- A guest user account with a limited lifetime. After the specified time period, the guest user account automatically expires.

- A guest user account with an unlimited lifetime. This account never expires.
- A guest user account that is activated at a predefined time in the future. The lobby ambassador defines the beginning and the end of the valid time period or configures the account with an unlimited lifetime.

This sections contains the following topics:

Logging in to the Prime Infrastructure User Interface as a Lobby Ambassador

When you log in as a lobby ambassador, you have access to the guest user template page in the Prime Infrastructure. You can then configure guest user accounts (through templates).

To log into the Prime Infrastructure user interface through a web browser:

Step 1 Launch Internet Explorer 7.0 or later on your computer.

Note Some Prime Infrastructure features might not function properly if you use a web browser other than Internet Explorer 7.0 or later on a Windows workstation.

Step 2 In the browser address line, enter **https://*PI-ip-address*** (such as https://1.1.1.1), where *PI-ip-address* is the IP address of the computer on which the Prime Infrastructure is installed. Your administrator can provide this IP address.

Step 3 When the Prime Infrastructure user interface displays the Login window, enter your username and password.

Note All entries are case sensitive.

Note The lobby ambassador can only define guest users templates.

Step 4 Click **Submit** to log into the Prime Infrastructure. The Prime Infrastructure user interface is now active and available for use. The Guest Users page is displayed. This page provides a summary of all created Guest Users.

To exit the Prime Infrastructure user interface, close the browser window or click **Logout** in the upper right corner of the page. Exiting a Prime Infrastructure user interface session does not shut down the Prime Infrastructure on the server.

Note When a system administrator stops the Prime Infrastructure server during a Prime Infrastructure session, the session ends, and the web browser displays this message: "`The page cannot be displayed`." Your session does not reassociate to the Prime Infrastructure when the server restarts. You must restart the Prime Infrastructure session.

Adding a New Guest User Account

To create a new guest user account:

Step 1 In the Guest User list page, choose **Add Guest User** from the Select a command drop-down list, and then click **Go**.

Step 2 In the Create a Guest User Account page, complete the fields as described in Table 31-68 and Table 31-69.

Step 3 Click **Save**. The guest user account appears on the Guest User list page.

Scheduling a Guest User Account

To schedule a guest user account:

Step 1 In the Guest User list page, choose **Schedule Guest User** from the Select a command drop-down list, and then click **Go**.

Step 2 Complete the fields as described in Table 31-68 and Table 31-69.

Step 3 Click **Save**.

Printing/Emailing User Details

To print or e-mail user details:

Step 1 In the Guest User list page, select the check box of the guest user whose details you want to print or e-mail.

Step 2 From the Select a command drop-down list, choose **Print/Email User Details**.

Step 3 Click **Go**.

Step 4 Review the credentials for this guest user and click the Email or Print icon, as applicable.

Step 5 Click **Back** to return to the previous page.

Note If the Prime Infrastructure reports a failure in sending e-mail, contact the Prime Infrastructure administrator. The e-mail setting on the Prime Infrastructure may not be configured properly.

Saving Guest Accounts to Device

The Save Guest Accounts to Device feature allows you to save respective guest accounts on the controller flash. When selected, all of the guest accounts on the controller are saved for each of the flash memory of controller. This ensures that the guest accounts are retained on the controllers in case the controllers accidentally reboot.

Note This feature is supported on controller Version 4.2.99.0 and later.

To save guest accounts on the controller flash:

Step 1 In the Guest User list page, choose **Save Guest Accounts on device** from the Select a command drop-down list.

Step 2 Click **Go**. All guest accounts currently present on each of the WLCs are saved.

Configuring User Preferences

The User Preferences page enables you to control the list page display options and idle timeout options in the Prime Infrastructure.

To configure the user preferences:

Step 1 Log into the Prime Infrastructure as a lobby ambassador.

Step 2 From the left sidebar menu, choose **User Preferences**.

Step 3 Enter the following information:

- List Pages
  - Items Per List—You can set the number of guest users to display in the Guest Users list page. Choose the number of items to display from the Items Per List Page drop-down list.
- User Idle Timeout
  - Logout idle user—Select the check box if you want to configure the amount of time, in minutes, that a user session can be idle before the server cancels the session.

Note If the Logout idle user check box is unselected, the user session will not be timed out.

- Logout idle user after—Choose the maximum number of minutes that a server waits for an idle user. The default value is 60 minutes. The minimum value is 15 minutes. The maximum value is 120 minutes.

Step 4 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 Infrastructure uses a list of tasks to control which part of Prime Infrastructure users can access and the functions they can perform in those parts. You change user privileges in Prime Infrastructure 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 Infrastructure 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 28-1 describes the Prime Infrastructure default user groups and their privileges.

Table 28-1 Default User Groups

Group Name	Privileges for Users in the Group
System Monitoring	Monitor Prime Infrastructure operations.
ConfigManagers	Monitor and configure Prime Infrastructure operations.

Table 28-1 Default User Groups

Group Name	Privileges for Users in the Group
Admin	Monitor and configure Prime Infrastructure operations and perform all system administration tasks except administering Prime Infrastructure user accounts and passwords.
SuperUsers	Monitor and configure Prime Infrastructure operations and perform all system administration tasks including administering Prime Infrastructure user accounts and passwords. Superusers tasks can be changed.
North bound API	Used only with Prime Infrastructure 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 Infrastructure 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 Infrastructure 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 Infrastructure 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 Infrastructure Virtual Domain consists of a set of Prime Infrastructure 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 Infrastructure 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 Infrastructure provides two types of audit logs:

- Application Audit logs—Logs events that pertain to the Prime Infrastructure 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.

To view Application Audit Logs:

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

Step 2 In the Application Audit Logs page, click to expand the row for which you want to view details about the log.

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

To view Network Audit Logs:

Step 1 Choose **Operate > Network Audit**.

Step 2 In the Network Audit Logs page, click to expand the row for which you want to view details about the log.

Adding TACACS+ Server

To configure Prime Infrastructure 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 Infrastructure 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 Infrastructure 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 Infrastructure to communicate with the RADIUS server, the shared secret you enter on this page must match the shared secret configured on the RADIUS server.