Controlling User Access

This following topics explain how to control and manage user access to Cisco Prime Infrastructure.

Related Topics

- Managing User Accounts
- Using Lobby Ambassadors to Manage Guest User Accounts
- Using User Groups to Control Access
- Using Virtual Domains to Control Access
- Auditing User Access
- Configuring AAA on Prime Infrastructure

Managing User Accounts

The following topics explain how to manage Prime Infrastructure user accounts.

Related Topics

- Viewing Active User Sessions
- Adding User Accounts
- Creating Additional Administrative Users
- Deleting User Accounts
- Configuring Guest Account Settings
- Disabling User Accounts
- Disabling the Web Root Account
- Changing User Passwords
- Changing Password Policies
- Changing the Global Idle Timeout

Viewing Active User Sessions

Administrators can view active Prime Infrastructure user sessions, with details including the user IP address and status.

Step 1 Log in to Prime Infrastructure as an administrator.

Step 2 Choose **Administration > Users > Users, Roles & AAA > Active Sessions**. Prime Infrastructure displays a list of the current active user sessions.

Step 3 Click the **Audit Trail** icon for the username for which you want to see the following data:

- User—User login name
- Client IP Address—IP address of the user's client device.
- Device IP Address—IP address of the device affected by the user operation (if applicable, such as with a device configuration change).
- Description—Description of the operation the user performed (such as login or logout).
- Time—Time operation was audited.

Audit trail entries may 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.

Related Topics

- Adding User Accounts
- Disabling User Accounts
- Changing User Passwords

Adding User Accounts

Administrators can add Prime Infrastructure user accounts and assign predefined static roles to these users. You can also give administrative access with differentiated privileges to certain user groups.

If you are using Operations Center: User accounts created in Operations Center can log in to Operations Center or any of the Prime Infrastructure 2.2 (or later) instances Operations Center is managing. To log into instances of Prime Infrastructure version 2.1.2 from Operations Center, the user ID must exist locally on the 2.1.2 instances. The 2.1.2 instances also must have the required update for Operations Center.

Step 1 Log in to Prime Infrastructure as an administrator.

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

Step 3 Choose **Select a command > Add User > Go**.

Step 4 Enter the username and password, and then confirm the password, for the new user.

Step 5 Choose the user groups to which this user belongs by selecting the check box next to each user group name (see "Using User Groups to Control Access" in Related Topics).

Step 6 Click the Virtual Domains tab to assign this user to a virtual domain (see "User Access in Virtual Domains" in Related Topics).

Step 7 Click **Save**.

Related Topics

- Creating Additional Administrative Users
- Deleting User Accounts
- Disabling User Accounts
- Using Lobby Ambassadors to Manage Guest User Accounts
- Using User Groups to Control Access
- Adding Users to Virtual Domains

Creating Additional Administrative Users

Any Prime Infrastructure administrator with sufficient privileges can create additional administrative user accounts with the same or lower privileges.

Step 1 Log in to Prime Infrastructure as an administrator.

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

Step 3 Choose **Select a command > Add User > Go.**

Step 4 Complete the required fields as you would for any new user account.

Step 5 Click **Admin** to give the new user administrator privileges.

Step 6 Click **Save**.

Related Topics

- Adding User Accounts
- Viewing Active User Sessions
- Disabling User Accounts
- Changing User Passwords

Deleting User Accounts

Administrators need not delete Prime Infrastructure user accounts to deny a user access temporarily. Instead, you can lock the account, then unlock it when the user returns.

Step 1 Log in to Prime Infrastructure as an administrator.

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

Step 3 Select the check box to the left of the name of the user that you want to delete.

Step 4 Choose **Select a command > Delete User(s) > Go.**

Step 5 Click **OK**.

Related Topics

- Adding User Accounts
- Viewing Active User Sessions
- Configuring Guest Account Settings
- Disabling User Accounts
- Changing User Passwords
- Changing Password Policies

Configuring Guest Account Settings

Prime Infrastructure administrators can choose to:

- Force all expired guest accounts to be deleted automatically.
- Limit Lobby Ambassadors' control over guest accounts to just those accounts they have created.

Both of these options impose restrictions on the latitude lobby ambassadors have to manage these temporary guest accounts. For details on using lobby ambassador accounts, see "Using Lobby Ambassadors to Manage Guest User Accounts" in Related Topics.

Step 1 Log in to Prime Infrastructure as an administrator.

Step 2 Choose **Administration > Settings > System Settings > General > Guest Account**.

Step 3 Change radio button selections as follows:

- Select **Automatically remove expired guest accounts** to have guest accounts whose lifetimes have ended moved to the Expired state. Guest accounts in the Expired state are deleted from Prime Infrastructure automatically.
- Select **Search and List only guest accounts created by this lobby ambassador** to restrict Lobby Ambassadors to modifying only the guest accounts that they have created. By default, any Lobby Ambassador can modify or delete any guest account, irrespective of who created that account.

Step 4 Click **Save**.

Related Topics

- Using Lobby Ambassadors to Manage Guest User Accounts
- Using User Groups to Control Access
- Using Virtual Domains to Control Access

Disabling User Accounts

Administrators can disable a user account so that the user cannot log in to Prime Infrastructure. You might want to disable a user account if, for example, a user is on vacation or is temporarily changing job functions. By locking the user account, you disable the user's access to Prime Infrastructure. You can later unlock the user account, enabling access to Prime Infrastructure, without having to re-create the user.

User accounts may be disabled automatically if the password is not changed before expiration. Only an administrator can reset the password in this case (see "Changing User Passwords" and "Changing Password Policies" in Related Topics).

Step 1 Log in to Prime Infrastructure as an administrator.

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

Step 3 Select the user whose access you want to disable.

Step 4 Choose **Select a command > Lock User(s) > Go**.

The next time the user tries to log in to Prime Infrastructure, a message appears saying the login failed because the account is locked.

Related Topics

- Adding User Accounts
- Deleting User Accounts
- Disabling the Web Root Account
- Changing Password Policies
- Changing User Passwords

Disabling the Web Root Account

Prime Infrastructure ships with a default user account called “root”. During Prime Infrastructure installation, a password for the web root account must be entered. This “root” user account and its password are used to log in to the Prime Infrastructure web interface for the first time.

We recommend that you do not use the web root account for normal operations. Instead, create administrative or super- user accounts with all privileges, then disable the web root account that was created when Prime Infrastructure was installed.

To disable the web root account, follow the steps for that account given in “Disabling Root Access” in Related Topics.

Related Topics

- Disabling Root Access
- Disabling User Accounts
- Adding User Accounts
- Viewing Active User Sessions

Changing User Passwords

User passwords are controlled based on the re-use count established when administrators set user password policies.

Step 1 Log in to Prime Infrastructure as an administrator.

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

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

Related Topics

- Managing User Accounts
- Changing Password Policies
- Adding User Accounts

Changing Password Policies

Prime Infrastructure supports standard password policies for its own users, including:

- Controls on password minimum length and re-use.
- Forbidden password content, such as common words and user names.
- Rules on other kinds of character choices, including character classes that must be included, repeated characters and common character substitutions.
- Password expiration periods and user warnings associated with password expiry

These password policies affect the passwords of locally administered users only. If you are using a AAA server to authenticate Prime Infrastructure servers, password policies must be set on the AAA server.

Step 1 Log in to Prime Infrastructure as an administrator.

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

Step 3 Choose the policies you want enforced, then click **Save**.

Related Topics

- Adding User Accounts
- Configuring AAA on Prime Infrastructure

Changing the Global Idle Timeout

Prime Infrastructure automatically logs off idle users. It provides two settings that control when and how this happens:

- User idle timeout—Individual users can enable and configure this setting to end their user session when they exceed the timeout. This user idle timeout is enabled by default and set to 15 minutes.
- Global idle timeout—Users with administrator privileges can enable and configure this setting which affects all users, across the system. The global idle timeout setting overrides the user idle timeout setting. The global idle timeout is enabled by default and set to 15 minutes.

The following steps explain how administrators can change the global idle timeout, or disable it if necessary. For details on changing the user timeout preference, see “Changing Your Idle-User Timeout” in Related Topics.

Step 1 Log in to Prime Infrastructure as an administrator.

Step 2 Choose **Administration > Settings > System Settings > General > Server.**

Step 3 Under **Global Idle Timeout**:

- Change the check status of the checkbox next to **Logout all idle users** to enable or disable the global idle timeout.
- From the **Logout all idle users after** drop-down list, choose one of the idle timeout limits.

Step 4 Click **Save**. You will need to logout and log back in for your changes to take effect.

Related Topics

- Viewing Active User Sessions
- Changing Your Idle-User Timeout

Using Lobby Ambassadors to Manage Guest User Accounts

Lobby ambassador accounts are a special kind of Prime Infrastructure administrative account used to add, manage and retire temporary guest user accounts. Lobby ambassador accounts have very limited network configuration privileges specified in the lobby ambassador profile, and have access only to those Prime Infrastructure functions used to manage guest accounts.

Typically, an enterprise-supplied guest network allows access to the Internet for a guest without compromising the enterprise's hosts. Web authentication is usually provided without a specialized client, so most guests will need to initiate a VPN tunnel to their desired destination.

Prime Infrastructure permits both wired and wireless guest user access. 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 may be available via a guest office or through 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 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 end of the valid time period.

Any Prime Infrastructure administrator with "SuperUser" or "administrator" privileges can create one or more lobby ambassador accounts, with varying profiles and permissions.

Ensure that you have proper time settings on the devices to see correct lifetimes on guest user accounts after they are discovered.

Related Topics

- Managing Guest User Accounts: Workflows
- Saving Guest Accounts on a Device
- Editing Guest User Credentials

Managing Guest User Accounts: Workflows

Lobby ambassadors can manage guest user accounts following this workflow

1. Create guest user accounts—While logged in as a lobby ambassador, create guest user accounts as needed.
2. Schedule guest user accounts—While logged in as a lobby ambassador, schedule automatic creation of guest user accounts.
3. Print or email guest user details—While logged in as a Lobby Ambassador, print or email the guest user account details to the host or person who will be welcoming the guests.

Prime Infrastructure administrators with full access can manage lobby ambassadors and their work using this workflow:

1. Create lobby ambassador accounts—While logged in as a Prime Infrastructure administrator, create lobby ambassador accounts as needed.
2. View lobby ambassador activities—While logged in as a Prime Infrastructure administrator, supervise the lobby ambassador's activities using the log.

Related Topics

- Creating Lobby Ambassador Accounts
- Creating Guest User Accounts as a Lobby Ambassador
- Scheduling Guest User Accounts
- Printing or Emailing Guest User Details
- Viewing Lobby Ambassador Activities

Creating Lobby Ambassador Accounts

Before you begin creating Lobby Ambassador accounts, you must ensure that you have proper time settings on the devices (if you do not, you will incorrect account lifetimes on Guest User accounts after they are discovered).

Step 1 Log in to Prime Infrastructure as an administrator.

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

Step 3 Choose **Select a command > Add User > Go**.

Step 4 Complete the required fields as follows:

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

b. Complete the required fields on the Lobby Ambassador Defaults tab.

c. Click the Virtual Domains tab to assign a virtual domain for this lobby ambassador account.

d. In the **Available Virtual Domains** list, click to highlight the virtual domain you want this user to access. Then click **Add** to add it to the Selected Virtual Domains list.

Step 5 Click **Save**.

Related Topics

- Managing Guest User Accounts: Workflows
- Saving Guest Accounts on a Device
- Editing Guest User Credentials

Logging in as a Lobby Ambassador

You must use the lobby ambassador username and password to log into the Prime Infrastructure user interface. When you log in as a lobby ambassador, the Guest User page appears and provides a summary of all created Guest Users.

Related Topics

- Managing Guest User Accounts: Workflows
- Saving Guest Accounts on a Device
- Editing Guest User Credentials

Creating Guest User Accounts as a Lobby Ambassador

Step 1 Log in to Prime Infrastructure as a lobby ambassador.

Step 2 Choose **Select a command > Add User Group > Go**.

Step 3 Complete the required fields on the General and Advanced tabs.

Step 4 Click **Save**.

Related Topics

- Managing Guest User Accounts: Workflows
- Saving Guest Accounts on a Device
- Editing Guest User Credentials
- Field Reference for Guest User Pages

Scheduling Guest User Accounts

Step 1 Log in to Prime Infrastructure as a lobby ambassador.

Step 2 Choose **Select a command** > **Schedule Guest User > Go.**

Step 3 Configure the required parameters:

If the **Generate new password on every schedule** and **No days of the week** check boxes are selected, then the user will have one password for the entire time the account is active.

If the **Generate new password on every schedule** and **Any days of the week** check boxes are selected, then the user will have a new password for each day.

Step 4 Click **Save**.

Related Topics

- Managing Guest User Accounts: Workflows
- Saving Guest Accounts on a Device
- Editing Guest User Credentials

Printing or Emailing Guest User Details

The lobby ambassador can print or e-mail the guest user account details to the host or person who welcomes guests. The email or printed sheet will show the following account details:

- Guest user account name.
- Password for the guest user account.
- Start date and time when the guest user account becomes active.
- End date and time when the guest user account expires.
- Profile ID assigned to the guest user. Your administrator can advise which Profile ID to use.
- Disclaimer information for the guest user.

Step 1 Log in to Prime Infrastructure as a lobby ambassador.

Step 2 On the Guest User page, select the check box next to the user name whose account details you want to send.

Step 3 Choose **Select a command > Print/E-mail User Details > Go.** Then proceed as follows:

- If you are printing, click **Print**. From the Print page, select a printer, and click **Print**.
- If emailing, click **Email**. From the Email page, enter the subject-line text and the email address of the recipient, then click **Send**.

Related Topics

- Managing Guest User Accounts: Workflows
- Saving Guest Accounts on a Device
- Editing Guest User Credentials

Viewing Lobby Ambassador Activities

Prime Infrastructure administrators can supervise lobby ambassadors using the Audit Trail feature.

Step 1 Log into Prime Infrastructure as an administrator.

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

Step 3 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 login name
- Type of operation audited
- Time when the operation was audited
- Login success or failure
- Indicates the reason for any login failure (for example, “invalid password”).

Related Topics

- Managing Guest User Accounts: Workflows
- Saving Guest Accounts on a Device
- Editing Guest User Credentials

Saving Guest Accounts on a Device

Step 1 Log into Prime Infrastructure as a lobby ambassador.

Step 2 On the Guest User page, choose **Save Guest Accounts on Device** check box to save guest accounts to a Cisco Wireless LAN Controller (WLC) flash so that they are maintained across WLC reboots.

Related Topics

- Managing Guest User Accounts: Workflows
- Editing Guest User Credentials

Editing Guest User Credentials

Step 1 Log in to Prime Infrastructure as an administrator.

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

Step 3 Click the user name whose credentials you want to edit.

Step 4 Modify the required credentials.

While editing, if the Profile selection is removed (changed to Select a profile), the defaults are removed for this lobby ambassador. The user must reconfigure the defaults to reinforce them.

Step 5 Click **Save**.

Related Topics

- Managing Guest User Accounts: Workflows
- Saving Guest Accounts on a Device

Using User Groups to Control Access

Prime Infrastructure has a list of tasks that control which part of Prime Infrastructure users can access and the functions they can perform when accessing those parts.

To make these access privileges easier to manage, Prime Infrastructure also provides User Groups. User Groups are lists of privileges and a list of users who are members. Any user on the User Group membership list has all of the privileges assigned to that User Group.

You can quickly change any user's privileges by assigning the user to, or removing them from, User Group memberships. If the User Group is editable, you can also use the User Group Task List to change what the users who are members of a specific User Group are authorized to do and the screens they can access.

You can also use any of the four user-defined User Groups to define a special custom set of specific privileges as explained in "Changing User Group Privileges" in Related Topics. You can then assign users to it as needed, as explained in "Changing User Group Memberships".

Prime Infrastructure comes with the set of default User Groups shown in the table below. Note that the functions and privileges of most default User Groups are not editable. You can, however, change the membership of all User Groups, using the steps in "Changing User Group Memberships" in Related Topics.

Table 11-1 Default User Groups

User Group	Provides access to	Editable?
Admin	All Prime Infrastructure administration tasks.	Yes
Config Managers	All monitoring and configuration tasks.	Yes
Lobby Ambassador	User administration for Guest user only.Members of this user group cannot also be members of any other user group.	No
Monitor Lite	Monitoring of assets only. Members of this user group cannot also be members of any other user group.	No
NBI Credential	The Northbound Interface Credential API.	No
NBI Read	The Northbound Interface Read API.	No
NBI Write	The Northbound Interface Write API.	No
North Bound API User	All Northbound InterfaceAPIs. Members of this user group cannot also be members of any other user group. This is a special group that lacks access to the Prime Infrastructure user interface; see "North Bound API User Group" in Related Topics.	No
Root	Superuser access to the web root user. This user group is reserved for the local root user only; no other users should be assigned to this user group.	No
Super Users	All Prime Infrastructure tasks.	Yes
System Monitoring	Monitoring tasks only.	Yes
User Assistant	Local Net user administration only. Members of this user group cannot also be members of any other user group.	No

Table 11-1 Default User Groups (continued)

User Group	Provides access to	Editable?
User-Defined 1	A user-selectable mix of functions.	Yes
User-Defined 2		
User-Defined 3		
User-Defined 4		
mDNS Policy Admin[1]	All mDNS policy administration functions only.	No

1. Do not use RADIUS, TACACS+ or SSO to create users to be included in the "mDNS Policy Admin" group. The AAA server will not have the multicast DNS settings needed to create this type of user.

Related Topics

- Managing User Accounts
- Viewing User Group Privileges and Membership
- Changing User Group Privileges
- Changing User Group Memberships
- North Bound API User Group

North Bound API User Group

Prime Infrastructure's North Bound API user group is a specially privileged group, set up to allow any user who is a member of it to access Prime Infrastructure via its APIs only. Any user assigned to the North Bound API group can issue and get a response for any Prime Infrastructure API, but will not have access to the Prime Infrastructure graphic user interface (GUI). This applies whether the user is also a member of other groups (including the Admin and Super User groups) or not. All other actions and privileges are disabled for members of North Bound API; its members cannot log into the Prime Infrastructure GUI.

The lone exception to this rule is access via the Prime Infrastructure Operations Center GUI. While North Bound API users cannot access an individual Prime Infrastructure server instance, they can still:

- Log in to the Operations Center GUI.
- Add Prime Infrastructure servers to the cluster of servers Operations Center is managing.
- View the status of all the Prime Infrastructure servers in the cluster, and the devices they manage, in a single consolidated report.

Related Topics

- Using User Groups to Control Access

Viewing User Group Privileges and Membership

To simplify managing which users can perform which functions, you can assign users to user groups, and then specify which tasks the users in that group are allowed to perform. See the table in "Using User Groups to Control Access" (in Related Topics, below) for a list of the user groups available in Prime Infrastructure.

Step 1 Log in to Prime Infrastructure as an administrator.

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

Step 3 Click the Group Name of the user group whose privileges and members you want to see:

- The Tasks Permissions tab shows the privileges assigned to this user group.
- The Members tab shows the users assigned to this user group.

Related Topics

- Using User Groups to Control Access
- Changing User Group Privileges
- Changing User Group Memberships

Changing User Group Privileges

Prime Infrastructure offers a several user groups with editable privileges, such as the System Monitoring and Config Managers user groups (see the table in "Using User Groups to Control Access" for a complete list of user groups and their edit status). You can change the privileges assigned to these editable user groups as needed.

You can also use the four User-Defined user groups to define special sets of specific privileges, as explained below. You can then assign users to these custom user groups as explained in "Changing User Group Memberships" in Related Topics.

Step 1 Log in to Prime Infrastructure as an administrator.

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

Step 3 Click the Group Name of an editable user group.

Step 4 Using the Tasks Permissions tab:

- Select the checkbox next to each task or function you want to provide to members of this user group.
- Unselect the checkbox next to each task or function you want remove from this user group's privileges.

Step 5 When you are finished, click **Submit**.

Related Topics

- Using User Groups to Control Access
- Viewing User Group Privileges and Membership

- Changing User Group Memberships

Changing User Group Memberships

You can quickly change a user's privileges in Prime Infrastructure by changing the user groups to which the user belongs.

You can also assign sites or devices to which a virtual domain has access. For details, see "Using Virtual Domains to Control Access" in Related Topics.

Prime Infrastructure will not permit certain combinations of user group membership. For example, a user cannot be a member of the "Root" and "Lobby Ambassador" user groups at the same time (for details, see the table in "Using User Groups to Control Access"). If you are using RADIUS to authenticate Prime Infrastructure users, make sure that you do not insert invalid user-group membership combinations into the RADIUS user attribute/value pairs.

Step 1 Log in to Prime Infrastructure as an administrator.

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

Step 3 Click on the user name for the user whose memberships you want to change. The User Details page appears.

Step 4 On the General tab, under **Groups Assigned to This User**:

- Select the checkbox next to each user group to which you want the user to belong.
- Unselect the checkbox next to each user group from which you want the user to be removed.

Step 5 When you are finished, click **Save**.

Related Topics

- Using User Groups to Control Access
- Viewing User Group Privileges and Membership
- Changing User Group Memberships
- Using Virtual Domains to Control Access

Using Virtual Domains to Control Access

A virtual domain is a logical grouping of sites, devices and access points. You choose which of these elements are included in a virtual domain, and which Prime Infrastructure users have access to that virtual domain.

Users with access to a virtual domain can configure devices, view alarms, and generate reports for the parts of the network included in the virtual domain. Users without this access cannot. Users with access to a virtual domain benefit because they can see just the devices and information they care about.

You can add virtual domains after you have added devices to Prime Infrastructure. Each virtual domain that you add must have a name, and can have an optional description, email address, and time zone. Prime Infrastructure uses the email address and time zone that you specify to schedule and e-mail

domain-specific reports. The scheduled time of the report can be set to the time zone specific to the virtual domain and the scheduled report can be e-mailed to the email address specified for the virtual domain.

Before you set up virtual domains, alway start by determining which Prime Infrastructure users are responsible for managing particular sites, devices and access points in your network. You can then organize your virtual domains according your organization's physical sites, the device types in your network, the user communities the network serves, or any other characteristic you choose.

Related Topics

- Understanding Virtual Domains
- User Access in Virtual Domains
- Creating Virtual Domains
- Adding Users to Virtual Domains

Understanding Virtual Domains

To manage Virtual Domains, select **Administration > Users > Virtual Domains.** In the left pane, the Virtual Domains sidebar menu has both List and Tree views, with the Tree view displayed by default. The menu has two icons, **Add New Domain** and **Import Domain(s)**. Just below these icons, a **Search** bar is available.

Virtual domains are organized hierarchically. Subsets of an existing virtual domain contain the network elements that are contained in the parent virtual domain. The "ROOT-DOMAIN" domain includes all virtual domains.

Hover your mouse cursor over "ROOT-DOMAIN" and a pop-up window appears at the cross-hair icon, displaying a summary of this parent virtual domain. You can create sub domains here.

Because network elements are managed hierarchically, user views of devices and access points, as well as some associated features and components – such as report generation, searches, templates, config groups, and alarms – are affected by the user's virtual domain. The following sections describe the effects of virtual-domain partitioning on the following Prime Infrastructure features:

- Reports
- Search
- Alarms
- Templates
- Config Groups
- Maps
- Access Points
- Controllers
- Email Notification

Reports

Reports only include components assigned to the current virtual domain. For example, if you create a virtual domain with only access points and no controllers assigned, all controllers are not displayed when you generate a controller inventory report.

If you create a virtual domain with only access points and no controllers assigned, you lose some ability to choose controller-based features. For example, some options require you to drill down from controller to access points. Because controllers are not in the virtual domain, you are not able to generate associated reports.

Reports are only visible in the current virtual domain. The parent virtual domain cannot view the reports from its subvirtual domain. Client reports such as Client Count only include clients that belong to the current virtual domain. If new clients are assigned to this partition by the administrator, the previous reports do not reflect these additions. Only new reports reflect the new clients.

Search

Search results only include components that are assigned to the virtual domain in which the search is performed. Search results do not display floor areas when the campus is not assigned to the virtual domain.

The saved searches are only visible in the current virtual domain. The parent virtual domain cannot view these search results. Prime Infrastructure does not partition network lists. If you search a controller by network list, all controllers are returned. Search results do not display floor areas when the campus is not assigned to the virtual domain.

Alarms

When a component is added to a virtual domain, no previous alarms for that component are visible to that virtual domain. Only new alarms are visible. For example, when a new controller is added to a virtual domain, any alarms generated for that controller prior to its addition do not appear in the current virtual domain.

Alarms are not deleted from a virtual domain when the associated controllers or access points are deleted from the same virtual domain.

Alarm Email Notifications—Only the ROOT-DOMAIN virtual domain can enable Location Notifications, Location Servers, and Prime Infrastructure email notification.

Templates

When you create or discover a template in a virtual domain, it is only available to that virtual domain unless it is applied to a controller. If it is applied to a controller and that controller is assigned to a subvirtual domain, the template stays with the controller in the new virtual domain.

Access point templates are visible in the virtual domain in which they were created *only.* You cannot see access points templates in other virtual domains, even if those virtual domains have the same access point added.

If you create a sub (or child) domain and then apply a template to both network elements in the virtual domain, Prime Infrastructure might incorrectly reflect the number of partitions to which the template was applied.

Config Groups

Config groups in a virtual domain can also be viewed by the parent virtual domain. A parent virtual domain can modify config groups for a sub (child) virtual domain. For example, the parent virtual domain can add or delete controllers from a subvirtual domain.

Maps

You can only view the maps that your administrator assigned to your current virtual domain.

- When a campus is assigned to a virtual domain, all buildings in that campus are automatically assigned to the same virtual domain.
- When a building is assigned to a virtual domain, it automatically includes all of the floors associated with that building.
- When a floor is assigned, it automatically includes all of the access points associated with that floor.

If only floors are assigned to a virtual domain, you lose some ability to choose map-based features. For example, some reports and searches require you to drill down from campus to building to floor. Because campuses and buildings are not in the virtual domain, you are not able to generate these types of reports or searches.

Coverage areas shown in Prime Infrastructure are only applied to campuses and buildings. In a floor-only virtual domain, Prime Infrastructure does not display coverage areas. If a floor is directly assigned to a virtual domain, it cannot be deleted from the virtual domain which has the building to which the floor belongs.

Search results do not display floor areas when the campus is not assigned to the virtual domain.

Access Points

When a controller or map is assigned to a virtual domain, the access points associated with the controller or map are automatically assigned as well. Access points can also be assigned manually (separate from the controller or map) to a virtual domain.

If the controller is removed from the virtual domain, all of its associated access points are also removed. If an access point is manually assigned, it remains assigned even if its associated controller is removed from the current virtual domain.

If you create a virtual domain with only access points and no controllers assigned, you lose some ability to choose controller-based features. For example, some options require you to drill down from controller to access points. Because controllers are not in the virtual domain, you are not able to generate associated reports.

If a manually added access point is removed from a virtual domain but is still associated with a controller or map that is assigned to the same virtual domain, the access point remains visible in the virtual domain. Any alarms associated with this access point are not deleted with the deletion of the access point.

When maps are removed from a virtual domain, the access points on the maps can be removed from the virtual domain.

If you later move an access point to another partition, some events (such as generated alarms) might reside in the original partition location.

Rogue access point partitions are associated with one of the detecting access points (the one with the latest or strongest RSSI value). If there is detecting access point information, Prime Infrastructure uses the detecting controller.
If the rogue access point is detected by two controllers which are in different partitions, the rogue access point partition might be changed at any time.

Controllers

Because network elements are managed hierarchically, controllers might be affected by partitioning. If you create a virtual domain with only access points and no controllers assigned, you lose some ability to choose controller-based features. For example, some options require you to drill down from controller to access points. Because controllers are not in the virtual domain, you are not able to generate associated reports.

If you create a partition with only a few controllers, choose **Configure > Access Points**, and click an individual link in the AP Name column. The complete list of Prime Infrastructure-assigned controllers will be displayed for primary, secondary, and tertiary controllers rather than the limited number specified in the partition.

If a controller configuration is modified by multiple virtual domains, complications can arise. To avoid this, manage each controller from only one virtual domain at a time.

Email Notification

Email notification can be configured per virtual domain. An email is sent only when alarms occur in that virtual domain.

Related Topics

- Using Virtual Domains to Control Access
- User Access in Virtual Domains
- Creating Virtual Domains
- Adding Users to Virtual Domains

User Access in Virtual Domains

A Prime Infrastructure virtual domain consists of a set of Prime Infrastructure devices, maps and access points. The virtual domain restricts the user's view to information relevant to the set of managed objects in that virtual domain.

Using virtual domains, administrators 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 their assigned part of the network *only*.

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 choosing 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-DOMAIN") 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-DOMAIN" 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.

Related Topics

- Using Virtual Domains to Control Access
- Understanding Virtual Domains
- Creating Virtual Domains
- Adding Users to Virtual Domains
- Changing Virtual Domain Access
- Exporting Virtual Domain RADIUS and TACACS+ Attributes

Creating Virtual Domains

When first installed, Prime Infrastructure contains only one virtual domain, called “ROOT-DOMAIN”. All other virtual domains must be created by Prime Infrastructure administrators, and are considered children (also known as “sub domains”) of the parent “ROOT-DOMAIN”.

To create a virtual domain, follow the steps below. Note that you can also create many virtual domains at one time by importing a properly formatted CSV file (for details, see “Importing Virtual Domains” in Related Topics).

Step 1 Log in to Prime Infrastructure as an administrator.

Step 2 Choose **Administration > Users > Virtual Domains.**

Step 3 In the Virtual Domains sidebar menu, click the parent virtual domain for your new virtual domain and then click the **Add New Domain** icon.

You can also create a new child domain of an existing domain by hovering your mouse cursor over the name of the parent virtual domain. You will see a cross-hair icon appear next to the domain name. Click the icon to display a popup summary of the parent, then click **Create Sub Domain** to create a new child domain of that parent.

Step 4 Enter the new domain’s name in the **Name** text box. This field is required.

Step 5 If needed, enter the new domain’s time zone, email address, and description. These are optional fields.

Step 6 Click **Submit** to view a summary of the newly created virtual domain and your changes to it.

Step 7 Click **Save** to confirm the changes.

Virtual domains are useful when you use them to restrict the view of a particular set of users to a specified set of site maps, network devices, and access points. See the Related Topics to continue creating a useful virtual domain.

Related Topics

- Adding Site Maps to Virtual Domains
- Adding Network Devices to Virtual Domains
- Adding Access Points to Virtual Domains
- Adding Users to Virtual Domains
- Importing Virtual Domains

Adding Site Maps to Virtual Domains

Step 1 Log in to Prime Infrastructure as an administrator.

Step 2 Choose **Administration > Users > Virtual Domains.**

Step 3 From the Virtual Domains sidebar menu, click a virtual domain to which you want to add site maps.

Step 4 On the Site Maps tab, click the **Add** button to view the list of available site maps. Select the required site maps and then click **Select** to add these site maps to the Selected Site Maps table.

Step 5 Click **Submit** to view the summary of the virtual domain.

Step 6 Click **Save** to confirm the changes.

Related Topics

- Adding Network Devices to Virtual Domains
- Adding Access Points to Virtual Domains
- Adding Users to Virtual Domains

Adding Network Devices to Virtual Domains

Step 1 Log in to Prime Infrastructure as an administrator.

Step 2 Choose **Administration > Users > Virtual Domains.**

Step 3 From the Virtual Domains sidebar menu, click a virtual domain to which you want to add a network device.

Step 4 On the Network Devices tab, click the **Add** button and the Select Network Devices pop-up appears. Here, a **Filter By** drop-down list is available to filter the network devices based on functionality.

Step 5 From the **Filter By** drop-down list, choose a network device. Select the required devices from the Available Network Devices table and click **Select** to add the devices to the Selected Network Devices table.

Step 6 Click **Submit** to view the summary of the virtual domain.

Step 7 Click **Save** to confirm the changes.

Related Topics

- Adding Site Maps to Virtual Domains
- Adding Access Points to Virtual Domains
- Adding Users to Virtual Domains

Adding Access Points to Virtual Domains

Step 1 Log in to Prime Infrastructure as an administrator.

Step 2 Choose **Administration > Users > Virtual Domains.**

Step 3 From the Virtual Domains sidebar menu, click a virtual domain to which you want to add access points.

Step 4 On the Access Points tab, click the **Add** button and the Add Access Points pop-up appears. Here, a **Filter By** drop-down list is available to filter the access points based on functionality.

Step 5 From the **Filter By** drop-down list, choose an access point group. Select the required access points from the Available Access Points table and click **Select** to add the access points to the Selected Access points table.

Step 6 Click **Submit** to view the summary of the virtual domain.

Step 7 Click **Save** to confirm the changes.

Related Topics

- Adding Site Maps to Virtual Domains
- Adding Network Devices to Virtual Domains
- Adding Users to Virtual Domains

Importing Virtual Domains

If you plan to create many virtual domains, or give them a complex hierarchy, you will find it easer to specify them in a properly formatted CSV file and then import it.

The CSV format allows you to specify the name, description, time zone and email address for each of the virtual domains you create, as well as each domain's parent domain. Adding site maps, network devices, and access points to any one virtual domain must be done separately.

Step 1 Log in to Prime Infrastructure as an administrator.

Step 2 Choose **Administration > Users > Virtual Domains.**

Step 3 Click the **Import Domain(s)** icon. Prime Infrastructure displays the Import popup.

Click the sample CSV format link in the popup to download a sample of the CSV format you must use.

Step 4 Click **Choose File** and navigate to the CSV file you want to import.

Step 5 Click **Import** to import the CSV file and create the virtual domains you specified.

Related Topics

- Creating Virtual Domains
- Adding Users to Virtual Domains

Adding Users to Virtual Domains

After you create a virtual domain, you can associate the virtual domain with specific users. This allows users to view information relevant to them specifically and restricts their access to other areas. Users assigned to a virtual domain can configure devices, view alarms, and generate reports for their assigned virtual domain *only*.

When using external AAA, be sure to add the custom attributes for virtual domains to the appropriate user or group configuration on the external AAA server.

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.

Step 1 Log in to Prime Infrastructure as an administrator.

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

Step 3 Click on the user name of the user you want to add to one or more virtual domains. Prime Infrastructure displays the User Details page for the user you selected.

Step 4 Click the **Virtual Domains** tab.

Step 5 In the “Available Virtual Domains”, click the virtual domain you want this user to access. Then click **Add** to add it to the “Selected Virtual Domains” column.

Except for Root Domain, the child Domains are not automatically included in Users, when their parent Domain is added.

Step 6 When you are finished, click **Save**.

Related Topics

- Adding Virtual Elements to Virtual Domains
- Using Virtual Domains to Control Access
- Understanding Virtual Domains
- User Access in Virtual Domains
- Creating Virtual Domains

Adding Virtual Elements to Virtual Domains

Each virtual domain can contain a subset of elements. For example, you can add additional maps, controllers, and access points to a virtual domain. Similarly you can add virtual elements into a virtual domain.

Virtual elements in PI are datacenters, clusters and hosts.If you select a virtual element as datacenter then user who belongs to this virtual domain will get access of all child elements like clusters, hosts and VMs under this datacenter. Similarly if you added only clusters as virtual elements, the user will get access to only the hosts and respective VMs that belong to that cluster. Selecting a parent element will provide access to all child elements in those virtual domains.

You can view number of virtual elements available in a virtual domain from Virtual Domain's **Quick View**.

To add a virtual element, follow these steps:

Step 1 Log in to Prime Infrastructure as an administrator.

Step 2 Choose **Administration > Users> Virtual Domains**.

Step 3 Click a virtual domain for which you want to add a virtual element.

Step 4 Click the Virtual Elements tab, then click **Add**.

Step 5 From the list of Available Virtual Elements, select a filter for which you want to view the available virtual elements.

Step 6 Select the required virtual element, then click **Select**.

Step 7 Click **Submit** to view the summary of the virtual domain.

Step 8 Click **Save** to confirm the changes.

Related Topics

- Using Virtual Domains to Control Access
- Understanding Virtual Domains
- User Access in Virtual Domains
- Creating Virtual Domains

Changing Virtual Domain Access

Choose a virtual domain from the Virtual Domains sidebar menu to view or edit its assigned site maps, network devices, access points, and virtual elements. A page with tabs for viewing the currently logged-in virtual domain-available Site Maps, Network Devices, Access Points, and Virtual Elements is displayed.

The Site Maps, Network Devices, Access Points, and Virtual Elements tabs are used to add or remove components assigned to this virtual domain. You can assign any combination of site maps, network devices, access points, and virtual elements to an existing virtual domain.

After assigning elements to a virtual domain and submitting the changes, Prime Infrastructure might take some time to process these changes, depending on how many elements are added.

Step 1 Log in to Prime Infrastructure as an administrator.

Step 2 Choose **Administration > Users > Virtual Domains.**

Step 3 Choose a virtual domain from the Virtual Domains sidebar menu.

Because all site maps, network devices, access points, and virtual elements are included in the partition tree, it can take several minutes to load the complete hierarchy. This time increases if you have a system with a very large number of network devices and access points.

Step 4 Click the applicable **Site Maps**, **Network Devices**, **Access Points,** or **Virtual Elements** tab.

Step 5 To add elements to the Selected table, click the **Add** button, check the check boxes of the required elements (Site Maps, Network Devices, Access Points or Virtual Elements) and click **Select**.

In the **Network Devices** tab, when you click the **Add** button, the Select Network Devices pop-up appears. Here, a **Filter By** drop-down list is available to select the required network devices. From the **Filter By** drop-down list, choose a network device. Select the required devices from the Available Network Devices table and click **Select**.

In the **Access Points** tab, when you click the **Add** button, the Add Access Points pop-up appears. Here, a **Filter By** drop-down list is available to add the required access points. From the **Filter By** drop-down list, choose an access point. Select the required access points from the Available Access Points table and click **Select**.

In **Virtual Element** tab, when you click on **Add** button, Add Virtual Element pop-up appears. Here a **Filter By** drop-down list is available to select the required virtual element. Based on the filter, the selected list will be populated with corresponding virtual elements type. Select the required element from the available virtual elements and click **Select**.

Step 6 The selected elements (Site Maps, Network Devices, Access Points or Virtual Elements) are listed in the Selected table.

Step 7 To delete elements from the Selected table, first check the check boxes of the required elements (Site Maps, Network Devices, Access Points, or Virtual Elements) to select them, and then click the **Delete** button.

Step 8 Click **Submit** to view the summary of the virtual domain.

Step 9 Click **Save** to confirm the changes.

The autonomous AP added through **Administration > Virtual Domains > Network Devices** will be listed under **Administration > Virtual Domains > Access Points**.

If you delete a switch, a controller, or an autonomous AP from the ROOT-DOMAIN, the device is removed from Prime Infrastructure. If the device is explicitly associated with the ROOT-DOMAIN or any other virtual domain that is not the child of the current virtual domain and if you delete the device from the current virtual domain, the device is removed from this virtual domain but it is not removed from Prime Infrastructure.

If a non-root domain user has added any discovery source then all virtual elements associated with discovery source will be available only to the root-domain user. Root-domain user has to give access to other child virtual-domains. The root-domain user can control the access of any virtual element.

Once you get access of virtual elements in your non-root domain you can create other virtual domains and manage the access to all these virtual element for your child virtual domain.

Related Topics

- Using Virtual Domains to Control Access
- Understanding Virtual Domains
- User Access in Virtual Domains
- Creating Virtual Domains

Deleting Virtual Domains

You can delete a virtual domain from the Virtual Domains sidebar menu using the pop-up summary window that appears when you click on the cross-hair icon next to the domain's name.

Deleting a virtual domain does not delete any site map, network device, access point or user assigned to the domain. You cannot delete a virtual domain that has child virtual domains until all of the children have been deleted.

Step 1 Log in to Prime Infrastructure as an administrator.

Step 2 Choose **Administration > Users > Virtual Domains.**

Step 3 In the Virtual Domains sidebar menu, hover your mouse cursor over the information icon (i) next to the name of the virtual domain you want to delete. You will see a a popup summary of the virtual domain and its assigned site maps, access points, network devices and virtual elements.

Step 4 Click the **Delete** link in the popup.

Step 5 You will be prompted to confirm that you want to delete this virtual domain. Click **OK** to confirm.

Related Topics

- Creating Virtual Domains
- Importing Virtual Domains

Exporting Virtual Domain RADIUS and TACACS+ Attributes

The Virtual Domain Custom Attributes page allows you to indicate the appropriate protocol-specific data for each virtual domain. The Export Custom Attributes button on the page preformats the virtual domain RADIUS and TACACS+ attributes. You can copy and paste these attributes into the Access Control Server (ACS) server. This allows you to copy only the applicable virtual domains into the ACS server page and ensures that the users only have access to these virtual domains.

When you create a sub domain for a previously created virtual domain, the sequence numbers for the custom attributes for RADIUS/TACACS are also updated in the existing virtual domain. These sequence numbers are for representation only and do not impact AAA integration.

Step 1 Log in to Prime Infrastructure as an administrator.

Step 2 Choose **Administration > Users > Virtual Domains.**

Step 3 In the left sidebar menu, choose the virtual domain for which you want to apply the RADIUS and TACACS+ attributes.

Step 4 Click the **Export Custom Attributes** link in the upper right corner of the page. The popup Virtual Domain Custom Attributes page displays the list of RADIUS and TACACS+ custom attributes in two separate panes

Step 5 Click and drag your mouse cursor to select the text in the RADIUS or TACACS+ Custom Attributes list (depending on which server you are currently configuring).

Step 6 Using your browser menu, copy the text to your clipboard.

Step 7 Log in to ACS and navigate to the User or Group Setup.

If you want to specify virtual domains on a per-user basis, then you need to make sure you add all of the custom attributes (for example, tasks, roles, virtual domains) information to the User custom attribute page.

Step 8 For the applicable user or group, click **Edit Settings**.

Step 9 Select the check boxes to enable these attributes, then click **Submit + Restart**.

Related Topics

- Using Virtual Domains to Control Access
- Understanding Virtual Domains
- Creating Virtual Domains

Auditing User Access

Prime Infrastructure maintains an audit record of user access, allowing you to check on user access and session activity.

Related Topics

- Accessing the Audit Trail for a User Group
- Viewing Application Logins and Actions
- Viewing User-Initiated Events

Accessing the Audit Trail for a User Group

Step 1 Log in to Prime Infrastructure as an administrator.

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

Step 3 Click the **Audit Trail** icon corresponding to the user group name for which you want to see the audit data. The Configuration Changes field provides a Details link if there are any configuration changes. Click the Details link for more information on the configuration changes done by an individual user.

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.

Related Topics

- Auditing User Access
- Viewing Application Logins and Actions
- Viewing User-Initiated Events

Viewing Application Logins and Actions

Application audit logs log 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. Prime Infrastructure displays the IP address from which the user has logged in to Prime Infrastructure as well as the pages in Prime Infrastructure the user viewed.

Step 1 Log in to Prime Infrastructure as an administrator.

Step 2 Choose **Administration > Settings > System Audit**.

Step 3 In the Application Audit Logs page, click to expand the row for which you want to view log details

For users authenticated via TACACS+ or RADIUS, the User Group column will be blank.

Related Topics

- Auditing User Access

- Viewing User-Initiated Events

Viewing User-Initiated Events

Prime Infrastructure's network audit logs record all events related to the devices in your network, including user-initiated events. For example, you can view the network audit logs to see which Prime Infrastructure user deployed a specific template and the date and time the template was deployed.

Step 1 Log in to Prime Infrastructure as an administrator.

Step 2 Choose **Inventory > Device Management > Network Audit**. The Network Audit Log page displays a list of recent actions, sorted by the name of the device on which the action was performed.

Step 3 Click to expand the row for which you want to view log details.

Related Topics

- Auditing User Access
- Viewing Application Logins and Actions
- Viewing User-Initiated Events

Configuring AAA on Prime Infrastructure

Prime Infrastructure can be configured to communicate with external authentication, authorization, and accounting (AAA) servers. The only user that has permission to configure AAA on Prime Infrastructure is the Root or SuperUser.

Any changes to local user accounts are in effect immediately if you are using Prime Infrastructure internal, or local, AAA mode. If you are using external AAA, such as RADIUS or TACACS+, the user account changes must be copied to the external server. Also note that combinations of Prime Infrastructure user-group memberships that are invalid with local AAA are also invalid when copied to the RADIUS server (even though RADIUS will permit you to create these invalid combinations when you set up RADIUS user attribute/value pairs). For a list of invalid user-group combinations, see the table in "Using User Groups to Control Access".

For information about migrating AAA servers, see the *ACS 5.2 Migration Utility Support Guide* listed in Related Topics.

Related Topics

- Setting the AAA Mode
- Adding TACACS+ Servers
- Adding RADIUS Servers
- Adding SSO Servers
- Configuring SSO Server AAA Mode
- Authenticating AAA Users Through RADIUS Using ISE: Workflow
- Configuring ACS 5.x for Prime Infrastructure: Workflow
- *ACS 5.2 Migration Utility Support Guide*

- Using User Groups to Control Access

Setting the AAA Mode

Prime Infrastructure supports local authentication as well as TACACS+ and RADIUS AAA, but you must specify a TACACS+ or RADIUS server first.

If you add more than one external AAA server, users are authenticated on the second server only if the first server is not reachable or has network problems.

You can use any alphabetical, numerical or special character (except for the single and double quote characters) while entering the shared secret key for a third-party TACACS+ or RADIUS server.

Step 1 Add one or more RADIUS or TACACS+ servers. For details, see "Adding RADIUS Servers" and "Adding TACACS+ Servers" in Related Topics.

Step 2 Log in to Prime Infrastructure as SuperUser.

Step 3 Select **Administration > Users > Users, Roles & AAA > AAA Mode Settings**.

Step 4 Select **RADIUS** or **TACACS+**. The **Enable Fallback to Local** check box is automatically selected, enabling use of the local database when the external AAA server is down.

Step 5 With the **Enable Fallback to Local** check box selected, specify the conditions under which the fallback to local Prime Infrastructure user account authentication occurs:

- **ONLY on no server response:** Only when the external server is unreachable or has network problems.
- **on authentication failure or no server response**: Either **w**hen the external server is unreachable or has network problems *or* the external AAA server cannot authenticate the user.

For AAA mode, SuperUser is always locally authenticated.

Step 6 Click **Save**.

Related Topics

- Adding TACACS+ Servers
- Adding RADIUS Servers

Adding TACACS+ Servers

Prime Infrastructure can use a maximum of three AAA servers.

Step 1 Log in to Prime Infrastructure as SuperUser.

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

Step 3 Choose **Select a command >Add TACACS+ Server (IP or DNS) > Go.**

Step 4 Enter the TACACS+ server information, then click **Save**.

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.

If you have enabled Prime Infrastructure High Availability and configured a virtual IP feature, the **Local Interface IP** field will offer you a choice between the virtual IP address and the physical IP address of the primary server. Be sure to select the physical IP address as the Local Interface IP.

Related Topics

- How High Availability Works
- Using Virtual IP Addressing with HA
- Required TACACS+/RADIUS Configurations After Prime Infrastructure IP Address Changes

Adding RADIUS Servers

Prime Infrastructure can use a maximum of three AAA servers.

Step 1 Log in to Prime Infrastructure as SuperUser.

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

Step 3 Choose **Select a command >Add Radius Server(IP or DNS) > Go.**

Step 4 Enter the RADIUS server information.

Step 5 Select the authentication type.

The authentication types available are:

- PAP—Password-based authentication is the protocol where two entities share a password in advance and use the password as the basis of authentication.
- CHAP—Challenge-Handshake Authentication Protocol requires that both the client and server know the plain text of the secret, although it is never sent over the network. CHAP provides greater security than Password Authentication Protocol (PAP).
- EAP_TLS—Extensible Authentication Protocol - Transport Layer Security is a secure protocol as it supports certificate-based mutual authentication. When EAP-TLS is selected as the authentication type, the generated key must be added to Cisco Prime Infrastructure keystore using **ncs key importsignedcert** admin CLI and the certificate chains must be present in RADIUS server. This does not require Cisco Prime Infrastructure services restart.

Step 6 Click **Save**.

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.

Related Topics

- Required TACACS+/RADIUS Configurations After Prime Infrastructure IP Address Changes
- Renewing AAA Settings After Installing a New Prime Infrastructure Version

Required TACACS+/RADIUS Configurations After Prime Infrastructure IP Address Changes

If you change the IP address of the Prime Infrastructure server after you add a TACACS+ or RADIUS server, you must manually configure the TACACS+ or RADIUS server with the new IP address of the Prime Infrastructure server. Prime Infrastructure stores in cache the local interface on which the RADIUS or TACACS+ requests are sent, and you need to manually edit the RADIUS or TACACS+ server configurations to make sure the Prime Infrastructure IP address is updated.

Related Topics

- Adding TACACS+ Servers
- Adding RADIUS Servers
- Renewing AAA Settings After Installing a New Prime Infrastructure Version

Renewing AAA Settings After Installing a New Prime Infrastructure Version

If you were using external RADIUS or TACACS+ user authentication before migrating your existing data to a new version of Prime Infrastructure, you must transfer the expanded Prime Infrastructure user task list to your AAA server. After you upgrade Prime Infrastructure, you must re-add any permissions on the TACACS+ or RADIUS server and update the roles in your TACACS server with the tasks from the Prime Infrastructure server. For information, see “Setting the AAA Mode” in Related Topics.

If you changed the IP address of the Prime Infrastructure server during the upgrade process, you will need to log in to Prime Infrastructure as SuperUser and follow the instructions given in “Required TACACS+/RADIUS Configurations After Prime Infrastructure IP Address Changes” before other users will be able to log in.

Related Topics

- Adding TACACS+ Servers
- Adding RADIUS Servers
- Setting the AAA Mode
- Required TACACS+/RADIUS Configurations After Prime Infrastructure IP Address Changes

Adding SSO Servers

You can enable Single Sign-On Authentication (SSO) in Prime Infrastructure.

SSO allows Prime Infrastructure users to enter their credentials just once before navigating across multiple SSO-enabled Prime Infrastructure applications. SSO makes it easier for users to perform cross-launch operations or use dashlets with content that comes from separate applications.

You must have administrator-level privileges to set up SSO.

Before setting up SSO, you must have an SSO-configured server and know its basic IP information. You must also configure the SSO server's AAA mode. For details on the latter task, see "Configuring SSO Server AAA Mode" in Related Topics.

Step 1 Log in to Prime Infrastructure as an administrator.

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

Step 3 Choose **Select a command >Add SSO Server > Go**.

Step 4 Enter the SSO server information, then click **Save**.

The maximum number of retries allowed for SSO server authentication requests is three.

The default Port Number is 443, which refers to the port on which the HTTPS is configured. You need to change the Port Number if you configure HTTPS on the Prime Infrastructure SSO Server on a different port.

Related Topics

- Configuring SSO Server AAA Mode
- Configuring AAA on Prime Infrastructure

Configuring High Availability for SSO

You can configure High Availability on the SSO client in the following ways:

- Adding multiple SSO servers. Configure all the SSO servers with the same set of external AAA servers to ensure that they have the same authentication and authorization credentials.The Prime Infrastructure SSO clients will attempt to use the SSO servers in the order in which they were defined, as displayed in the list of SSO servers on the Prime Infrastructure SSO servers page. For example: If the first SSO server is unavailable, the SSO client will fall back to the second SSO server in the list and use it. If the second is unavailable, the SSO client will fall back to the third SSO server — and so on, to the limit of the SSO servers you have defined.
- Create an HA pair for the SSO server: Configure a virtual IP address for the HA primary and secondary servers. For more information on High Availability see "Configuring High Availability" (in Related Topics, below). The Prime Infrastructure SSO clients will be configured with an SSO server with the configured Virtual IP address.

Related Topics

- Configuring High Availability

Configuring SSO Server AAA Mode

Single Sign-On Authentication (SSO) is used to authenticate and manage users in multi-user, multi-repository environments. SSO servers store and retrieve the credentials that are used for logging into disparate systems. You can set up Prime Infrastructure as the SSO server for other instances of Prime Infrastructure.

Prime Infrastructure supports CA and self-signed certificates as long as the Common Name (CN) field of the certificate contains the Fully Qualified Domain Name (FQDN) of the server on both the SSO client and the SSO server. The server must be capable of name resolution from the IP address to the FQDN. In addition, the hostname must match the left-most component of the FQDN.

For example, the **nslookup** command and expected data when configuring DNS with FQDN is:

```
hostname CUSTOMER_PI_HOSTNAME
nslookup CUSTOMER_PI_HOSTNAME
Server: ..
Address: ...
Name: CUSTOMER_PI_HOSTNAME.example.com
Address:  ….
```

For SSO operation, Prime Infrastructure requires that the SSL/TLS certificate hold the FQDN in the Common Name (CN) field. To verify that the certificate used by your Prime Infrastructure server has the FQDN in the CN field, use your browser to view the certificate. If the certificate does not contain the FQDN in the CN field, you must regenerate the certificate. After you regenerate the SSL/TLS certificate, add the SSO server to any or all the SSO clients. The SSO functionality distributes the certificate when the SSO server is added to the SSO client.

To add the SSO server, follow these steps:

Step 1 Log in to Prime Infrastructure as an administrator.

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

Step 3 Choose which SSO Server AAA mode you want to use. You can select only one at a time.

Any changes to local user accounts are effective only when you are configured for local mode. If you use remote authentication, changes to the credentials are made on a remote server. The two remote authentication types are RADIUS and TACACS+. RADIUS requires separate credentials for different locations (East and West Coast). TACACS+ is an effective and secure management framework with a built-in failover mechanism.

Step 4 Click **OK**.

Related Topics

- Configuring AAA on Prime Infrastructure
- Setting Up SSL Certification
- Configuring AAA on Prime Infrastructure

Authenticating AAA Users Through RADIUS Using ISE: Workflow

You can integrate Prime Infrastructure with Cisco Identity Services Engine (ISE). This section explains Prime Infrastructure user authentication through RADIUS protocol using ISE.

Only RADIUS server authentication is supported in ISE.

Step 1 Add Prime Infrastructure as a AAA client in ISE. For details, see “Adding Prime Infrastructure as an AAA Client in ISE” in Related Topics.

Step 2 Create a new User group in ISE. For details, see “Creating a New User Group in ISE”.

Step 3 Create a new User in ISE and add that User to the User group created in ISE. For details, see “Creating a New User” and “Adding to a User Group in ISE”.

Step 4 Create a new Authorization profile. For details, see “Creating a New Authorization Profile in ISE”.

Step 5 Create an Authorization policy rule. For details, see “Creating an Authorization Policy Rule in ISE”.

Step 6 Create an Authentication policy. For details, see “Creating a Simple Authentication Policy in ISE” or “Creating a Rule-Based Authentication Policy in ISE”.

Step 7 Configure AAA in Prime Infrastructure. For details, see “Configuring AAA in Prime Infrastructure”.

Related Topics

- Adding Prime Infrastructure as an AAA Client in ISE
- Creating a New User Group in ISE
- Creating a New User and Adding to a User Group in ISE
- Creating a New Authorization Profile in ISE
- Creating a Simple Authentication Policy in ISE
- Creating a Rule-Based Authentication Policy in ISE
- Configuring AAA on Prime Infrastructure

Adding Prime Infrastructure as an AAA Client in ISE

Step 1 Log in to ISE.

Step 2 Choose **Administration** > **Network Devices**.

Step 3 From the left sidebar menu, click the arrow next to Network Devices to expand that option.

The expanded list shows the already added devices.

Step 4 Click any device to view its details.

Step 5 From the left sidebar menu, click the arrow next to the  icon, then choose the **Add new device** option.

Step 6 In the right pane, enter the required details.

Step 7 Enter the Shared key in the Shared Secret text box.

Step 8 Click **Save** to add the device.

Related Topics

- Authenticating AAA Users Through RADIUS Using ISE: Workflow
- Creating a New User Group in ISE
- Creating a New User and Adding to a User Group in ISE
- Creating a New Authorization Profile in ISE
- Creating a Simple Authentication Policy in ISE
- Creating a Rule-Based Authentication Policy in ISE
- Configuring AAA on Prime Infrastructure

Creating a New User Group in ISE

You can create a new user group in ISE. This helps you to classify different privileged Prime Infrastructure users and also create authorization policy rules on user groups.

Step 1 Choose **ISE** > **Administration** > **Groups**.

Step 2 From the left sidebar menu, choose **User Identity Groups**, then click **Add**.

Step 3 Enter the name and description for the group, then click **Save**.

Related Topics

- Authenticating AAA Users Through RADIUS Using ISE: Workflow
- Adding Prime Infrastructure as an AAA Client in ISE
- Creating a New User and Adding to a User Group in ISE
- Creating a New Authorization Profile in ISE
- Creating a Simple Authentication Policy in ISE
- Creating a Rule-Based Authentication Policy in ISE
- Configuring AAA on Prime Infrastructure

Creating a New User and Adding to a User Group in ISE

You can create a new user in ISE and map that user to a user group.

Step 1 Choose **ISE** > **Administration** > **Identity Management** > **Identities**.

Step 2 From the left sidebar menu, choose **Identities** > **Users**, then click **Add**.

Step 3 Enter the username and password and reenter the password for the user.

Step 4 Choose the required user group from the **User Group** drop-down list, then click **Save**.

You can also integrate ISE with external sources such as Active Directory and Lightweight Directory Access Protocol (LDAP).

Related Topics

- Authenticating AAA Users Through RADIUS Using ISE: Workflow
- Adding Prime Infrastructure as an AAA Client in ISE
- Creating a New User Group in ISE
- Creating a New Authorization Profile in ISE
- Creating a Simple Authentication Policy in ISE
- Creating a Rule-Based Authentication Policy in ISE
- Configuring AAA on Prime Infrastructure

Creating a New Authorization Profile in ISE

Step 1 Choose **ISE** > **Policy** > **Policy Elements** > **Results**.

Step 2 From the left sidebar menu, choose **Authorization** > **Authorization Profiles**, then click **Add**.

Step 3 Enter the name and description for the profile.

Step 4 Choose **ACCESS_ACCEPT** from the Access Type drop-down list.

Step 5 In the Advanced Attribute Settings area, add Prime Infrastructure user group RADIUS custom attributes one after another along with the virtual domain attributes at the end.

User group RADIUS custom attributes are located in Prime Infrastructure at **Administration > Users > Users, Roles & AAA > User Groups**. Click **Task List** for the group with appropriate permissions.

a. Select **cisco - av - pair** and paste Prime Infrastructure user group RADIUS custom attribute next to it. Keep adding one after another.

b. Add the Virtual Domain attribute at the end of the last RADIUS custom attribute for each group (for RADIUS custom attributes, see “Exporting Virtual Domain RADIUS and TACACS+ Attributes”).

Step 6 Save the authorization profile.

Related Topics

- Exporting Virtual Domain RADIUS and TACACS+ Attributes
- Authenticating AAA Users Through RADIUS Using ISE: Workflow

- Adding Prime Infrastructure as an AAA Client in ISE
- Creating a New User Group in ISE
- Creating a New User and Adding to a User Group in ISE
- Creating a Simple Authentication Policy in ISE
- Creating a Rule-Based Authentication Policy in ISE
- Configuring AAA on Prime Infrastructure

Creating an Authorization Policy Rule in ISE

Step 1 Choose **ISE** > **Policy** > **Authorization**.

Step 2 From the Authorization Policy page, choose **Insert New Rule Above** from the Actions drop-down list.

Create a rule to be used for Prime Infrastructure user login.

Step 3 Enter a name for the rule in the Rule Name text box.

Step 4 Choose the required identity group from the Identity Groups drop-down list.

For example, choose **Prime Infrastructure-SystemMonitoring-Group**.

Step 5 Choose a permission from the Permissions drop-down list. The permissions are the Authorization profiles.

For example, choose **Prime Infrastructure-SystemMonitor authorization profile**.

In this example, we define a rule where all users belonging to Prime Infrastructure System Monitoring Identity Group receive an appropriate authorization policy with system monitoring custom attributes defined.

Step 6 Click **Save** to save the authorization rule.

You can also monitor successful and failed authentication using the ISE > Monitor > Authentications option.

Related Topics

- Authenticating AAA Users Through RADIUS Using ISE: Workflow
- Adding Prime Infrastructure as an AAA Client in ISE
- Creating a New User Group in ISE
- Creating a New User and Adding to a User Group in ISE
- Creating a New Authorization Profile in ISE
- Creating a Simple Authentication Policy in ISE
- Creating a Rule-Based Authentication Policy in ISE
- Configuring AAA on Prime Infrastructure

Creating a Simple Authentication Policy in ISE

The procedure for configuring a simple authentication policy includes defining an allowed protocols service and configuring a simple authentication policy.

To perform the following task, you must be a Super Admin or System Admin.

Step 1 Choose **Policy** > **Authentication**.

Step 2 Click **OK** on the message that appears.

Step 3 Enter the values as required.

Step 4 Click **Save** to save your simple authentication policy.

Related Topics

- Simple Authentication Policies in the *Cisco Identity Services Engine User Guide, Release 1.2*
- Authenticating AAA Users Through RADIUS Using ISE: Workflow
- Adding Prime Infrastructure as an AAA Client in ISE
- Creating a New User Group in ISE
- Creating a New User and Adding to a User Group in ISE
- Creating a New Authorization Profile in ISE
- Creating a Rule-Based Authentication Policy in ISE
- Configuring AAA on Prime Infrastructure

Creating a Rule-Based Authentication Policy in ISE

You can edit the default identity source that you want Cisco ISE to use in case none of the identity sources defined in this rule match the request.

The last row in the policy page is the default policy that will be applied if none of the rules match the request. You can edit the allowed protocols and identity source selection for the default policy.

You cannot specify the “UserName” attribute when configuring an authentication policy when the EAP-FAST client certificate is sent in the outer TLS negotiation. We recommend using certificate fields like “CN” and “SAN,” for example.

It is a good practice to choose Deny Access as the identity source in the default policy if the request does not match any of the other policies that you have defined.

To perform the following task, you must be a Super Admin or System Admin.

Step 1 Choose **Policy** > **Authentication**.

Step 2 Click the **Rule-Based** radio button.

Step 3 Click **OK** on the message that appears.

Step 4 Click the action icon and click I**nsert new row above** or **Insert new row below** based on where you want the new policy to appear in this list. The policies will be evaluated sequentially.

Each row in this rule-based policy page is equivalent to the simple authentication policy. Each row contains a set of conditions that determine the allowed protocols and identity sources.

Enter the values as required to create a new authentication policy.

Step 5 Click **Save** to save your rule-based authentication policies.

Related Topics

- Rule-Based Authentication Policies in the *Cisco Identity Services Engine User Guide, Release 1.2*
- Authenticating AAA Users Through RADIUS Using ISE: Workflow
- Adding Prime Infrastructure as an AAA Client in ISE
- Creating a New User Group in ISE
- Creating a New User and Adding to a User Group in ISE
- Creating a New Authorization Profile in ISE
- Creating a Simple Authentication Policy in ISE
- Configuring AAA on Prime Infrastructure

Configuring AAA in Prime Infrastructure

Step 1 Log in to Prime Infrastructure as *root*, then choose **Administration > Users > Users, Roles & AAA > RADIUS Servers**.

Step 2 Add a new RADIUS server with the ISE IP address, then click **Save**.

Step 3 Log in to ISE, then choose **Administration > Users > Users, Roles & AAA > AAA Mode Settings**.

Step 4 Select **RADIUS** as the AAA mode, then click **Save**.

Step 5 Log out of Prime Infrastructure.

Step 6 Log in again to Prime Infrastructure as an AAA user that is already defined in ISE.

For example, log in as user *ncs-sysmon*.

Related Topics

- Authenticating AAA Users Through RADIUS Using ISE: Workflow
- Adding Prime Infrastructure as an AAA Client in ISE
- Creating a New User Group in ISE
- Creating a New User and Adding to a User Group in ISE
- Creating a New Authorization Profile in ISE
- Creating a Simple Authentication Policy in ISE
- Creating a Rule-Based Authentication Policy in ISE

Configuring ACS 5.x for Prime Infrastructure: Workflow

If you are configuring ACS 5.x to work with Prime Infrastructure, you will follow this workflow:

1. Create ACS network devices and AAA clients.
2. Add ACS groups.
3. Add ACS users.
4. Create ACS policy elements or authorization profiles for RADIUS or TACACS+, as appropriate.
5. Create ACS service selection rules for RADIUS or TACACS+, as appropriate.
6. Configure ACS access services for RADIUS or TACACS+, as appropriate.

Related Topics

- Creating ACS Network Devices and AAA Clients
- Adding ACS Groups
- Adding ACS Users
- Creating ACS Policy Elements or Authorization Profiles for RADIUS
- Creating ACS Policy Elements or Authorization Profiles for TACACS+
- Creating ACS Service Selection Rules for RADIUS
- Creating ACS Service Selection Rules for TACACS+
- Configuring ACS Access Services for RADIUS
- Configuring ACS Access Services for TACACS+

Creating ACS Network Devices and AAA Clients

Step 1 Log in to the ACS 5.x server and choose **Network Resources** > **Network Devices and AAA Clients**.

Step 2 Enter an IP address.

Related Topics

- Configuring ACS 5.x for Prime Infrastructure: Workflow
- Adding ACS Groups

Adding ACS Groups

Step 1 Log in to the ACS 5.x server and choose **Users and Identity Stores** > **Identity Groups**.

Step 2 Create a group.

Related Topics

- Configuring ACS 5.x for Prime Infrastructure: Workflow
- Creating ACS Network Devices and AAA Clients
- Adding ACS Users

Adding ACS Users

Step 1 Log in to the ACS 5.x server and choose **Users and Identity Stores > Internal Identity Stores > Users**.

Step 2 Add a user, and then map a group to that user.

Related Topics

- Configuring ACS 5.x for Prime Infrastructure: Workflow
- Adding ACS Groups
- Creating ACS Policy Elements or Authorization Profiles for RADIUS
- Creating ACS Policy Elements or Authorization Profiles for TACACS+

Creating ACS Policy Elements or Authorization Profiles for RADIUS

Step 1 Log in to the ACS 5.x server and choose **Policy Elements** > **Authorization and Permissions** > **Network Access** > **Authorization Profiles**, then click **Create**.

Step 2 Enter the required information, then click **Submit**.

The **Export Custom Attributes** button preformats the virtual domain RADIUS and TACACS+ attributes. You can copy and paste these attributes into the Access Control Server (ACS) server. This allows you to copy only the applicable virtual domains into the ACS server page and ensures that users have access to these virtual domains only.

Related Topics

- Configuring ACS 5.x for Prime Infrastructure: Workflow
- Adding ACS Users
- Creating ACS Service Selection Rules for RADIUS
- Configuring ACS Access Services for RADIUS

Creating ACS Policy Elements or Authorization Profiles for TACACS+

Before you begin, ensure that you add the relevant Menu Access task so that the ACS submenus are displayed in Prime Infrastructure. For example, if you add a submenu under the Administration menu, you must first add the Administration Menu Access task so that the submenu is visible under the Administration menu in Prime Infrastructure.

Step 1 Retrieve the appropriate User Group task list attribute/value pairs from Prime Infrastructure:

a. Log in to Prime Infrastructure as an administrator and choose **Administration > Users > Users, Roles & AAA > User Groups**. Prime Infrastructure displays the list of User Groups.

b. Display the task list for the user group whose authorizations you want to send to ACS.

For example, if you want to send Admin user group authorizations to ACS: In the **Group Name** column, find the **Admin** group at the top of the list, then click the **Task List** link at the far right, opposite the "Admin" entry. Prime Infrastructure displays separate lists of custom task attributes for TACACS+ and RADIUS.

c. Copy and save the TACACS+ custom attributes to your desktop.

d. Repeat these steps as needed for all the user groups whose tasks you want to add to ACS.

Step 2 Log in to the ACS Admin GUI, and choose P**olicy Elements > Authentication and Permissions > Device Administration > Shell Profiles**.

Step 3 Click **Create** to create a new ACS shell profile for Prime Infrastructure

Step 4 Choose the **Custom Attributes** tab, then click **Bulk Edit**.

Step 5 Copy and paste all the attribute/value pairs you retrieved in Step 1 into the new shell profile.

Step 6 When you are finished, click **Submit** to create an attribute-based role for Prime Infrastructure.

Related Topics

- Configuring ACS 5.x for Prime Infrastructure: Workflow
- Adding ACS Users
- Creating ACS Service Selection Rules for TACACS+
- Configuring ACS Access Services for TACACS+

Creating ACS Service Selection Rules for RADIUS

Step 1 Log in to the ACS 5.x server and choose **Access Policies** > **Access Services** > **Service Selection Rules**.

Step 2 Click **Create**.

Step 3 Enter the required information, then click **OK**.

Related Topics

- Configuring ACS 5.x for Prime Infrastructure: Workflow
- Creating ACS Policy Elements or Authorization Profiles for RADIUS
- Creating ACS Service Selection Rules for RADIUS

- Configuring ACS Access Services for RADIUS

Creating ACS Service Selection Rules for TACACS+

Step 1 Log in to the ACS 5.x server and choose **Access Policies** > **Access Services** > **Service Selection Rules**\.

Step 2 Click **Create**.

Step 3 Enter the required information, then click **OK**.

Related Topics

- Configuring ACS 5.x for Prime Infrastructure: Workflow
- Creating ACS Policy Elements or Authorization Profiles for TACACS+
- Configuring ACS Access Services for TACACS+

Configuring ACS Access Services for RADIUS

Step 1 Log in to the ACS 5.x server and choose **Access Policies** > **Access Services** > **Default Network Access**.

Step 2 On the General tab, click the policy structure you want to use. By default, all the three policy structures are selected.

Step 3 From the Allowed Protocols, click the protocols you want to use.

You can retain the defaults for identity and group mapping.

Step 4 To create an authorization rule for RADIUS, choose **Access Policies** > **Access Services** > **Default Network Access** > **Authorization**, then click **Create**.

Step 5 In Location, click **All Locations** or you can create a rule based on the location.

Step 6 In Group, select the group that you created earlier.

Step 7 In Device Type, click **All Device Types** or you can create a rule based on the Device Type.

Step 8 In Authorization Profile, select the authorization profile created for RADIUS, click **OK**, then click **Save**.

Related Topics

- Configuring ACS 5.x for Prime Infrastructure: Workflow
- Creating ACS Service Selection Rules for RADIUS

Configuring ACS Access Services for TACACS+

Step 1 Log in to the ACS 5.x server and choose **Access Policies** > **Access Services** > **Default Device Admin**.

Step 2 On the General tab, click the policy structure you want to use. By default, all the three are selected. Similarly, in Allowed Protocols, click the protocols you want to use.

You can retain the defaults for identity and group mapping.

Step 3 To create an authorization rule for TACACS+, choose **Access Policies** > **Access Services** > **Default Device Admin** > **Authorization**, then click **Create**.

Step 4 In Location, click **All Locations**, or you can create a rule based on the location.

Step 5 In Group, select the group that you created earlier.

Step 6 In Device Type, click **All Device Types**, or you can create a rule based on the Device Type.

Step 7 In Shell Profile, select the shell profile created for TACACS+, click **OK**, then click **Save**.

Related Topics

- Configuring ACS 5.x for Prime Infrastructure: Workflow
- Creating ACS Service Selection Rules for TACACS+