Controlling User Access

This chapter describes how to control and manage the user access provided by Cisco Prime Infrastructure.

- Creating Additional Administrative Users
- Managing User Accounts
- Using User Groups to Control Access
- Changing the Global Session Timeout for Idle Users
- Using Virtual Domains to Control Access
- User Access in Virtual Domains
- Auditing User Access
- Configuring AAA on Prime Infrastructure

Creating Additional Administrative Users

Step 1  Choose Administration > Users, Roles & AAA, then click Users.
Step 2  Choose Select a command > Add User, then click Go.
Step 3  Complete the required fields, then click Admin to give the user administrator privileges.
Step 4  Click Save.
Managing User Accounts

You can perform the following actions on user accounts:

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

Viewing Active User Sessions

All Prime Infrastructure users have basic parameters such as a username and password. Users with administrator privileges can view active user sessions, with details including the

Step 1  In Converged view: Choose Administration > Users, Roles & AAA > Active Sessions.
Step 2  Click the Audit Trail icon for the username for which you want to see the following data:

- User—User login name
- IP Address—IP address of the user’s client device
- 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 associated with this user. Click the Details link for more information on the configuration changes performed by the 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.
Adding Users

You can add a user and assign predefined static roles to that user. Besides complete access, you can give administrative access with differentiated privileges to certain user groups.

User IDs created in Operations Center can log in to Operations Center or any of the Prime Infrastructure 2.2 instances being managed by Operations Center. 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, which also must have the update for Operations Center (see Enabling Prime Infrastructure 2.1.2 for Operations Center Management).

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

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

**Step 3** Enter the username and password, and then confirm the password, for the new user.

**Step 4** Choose the User Groups to which this user belongs by selecting the check box next to each group name (see Using User Groups to Control Access).

**Step 5** Click the Virtual Domains tab to assign a virtual domain to this user (see User Access in Virtual Domains).

**Step 6** Click **Save**.

Disabling the Web Root Account

Prime Infrastructure ships with a default user account called “web 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.

Configuring Guest Account Settings

You can choose to have all expired guest accounts deleted automatically, and restrict Lobby Ambassadors’ control over guest accounts to just those accounts they created.

**Step 1** Choose **Administration > System Settings > Guest Account Settings**.

**Step 2** 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.
Disabling User Accounts

You can disable a user account so that a 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; later, you can 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).

Step 1 Choose Administration > Users, Roles & AAA, then click Users.
Step 2 Select the user whose access you want to disable.
Step 3 Choose Select a command > Lock User(s), then click 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
- Changing Password Policies
- Changing User Passwords

Changing User Passwords

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

Step 1 Choose Administration > Users, Roles & AAA, then click Users.
Step 2 Select the user whose password you want to change.
Step 3 Complete the password fields, then click Save.

Related Topics
- Creating Additional Administrative Users
- Changing Password Policies
Changing Password Policies

Prime Infrastructure supports standard password policies, 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 users, password policies must be set on the AAA server.

Step 1 Choose Administration > Users, Roles & AAA, then click Local Password Policy.
Step 2 Choose the necessary policies, then click Save.

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>
<thead>
<tr>
<th>User Group</th>
<th>Provides access to</th>
<th>Editable?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin</td>
<td>All Prime Infrastructure administration tasks.</td>
<td>Yes</td>
</tr>
<tr>
<td>Config Managers</td>
<td>All monitoring and configuration tasks.</td>
<td>Yes</td>
</tr>
<tr>
<td>Lobby Ambassador</td>
<td>User administration for Guest user only.</td>
<td>No</td>
</tr>
<tr>
<td>Monitor Lite</td>
<td>Monitoring of assets only.</td>
<td>No</td>
</tr>
<tr>
<td>NBI Credential</td>
<td>The Northbound Interface Credential API.</td>
<td>No</td>
</tr>
<tr>
<td>NBI Read</td>
<td>The Northbound Interface Read API.</td>
<td>No</td>
</tr>
</tbody>
</table>
Chapter 11    Controlling User Access

Using User Groups to Control Access

Table 11-1    Default User Groups (continued)

<table>
<thead>
<tr>
<th>User Group</th>
<th>Provides access to</th>
<th>Editable?</th>
</tr>
</thead>
<tbody>
<tr>
<td>NBI Write</td>
<td>The Northbound Interface Write API.</td>
<td>No</td>
</tr>
<tr>
<td>North Bound API</td>
<td>All Northbound Interface APIs. This is a special group that lacks access to the Prime Infrastructure user interface; see “North Bound API User Group” in Related Topics.</td>
<td>No</td>
</tr>
<tr>
<td>Root</td>
<td>Superuser access to the web root user.</td>
<td>No</td>
</tr>
<tr>
<td>Super Users</td>
<td>All Prime Infrastructure tasks.</td>
<td>Yes</td>
</tr>
<tr>
<td>System Monitoring</td>
<td>Monitoring tasks only.</td>
<td>Yes</td>
</tr>
<tr>
<td>User Assistant</td>
<td>Local Net user administration only.</td>
<td>No</td>
</tr>
<tr>
<td>User-Defined 1</td>
<td>A user-selectable mix of functions.</td>
<td></td>
</tr>
<tr>
<td>User-Defined 2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>User-Defined 3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>User-Defined 4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>mDNS Policy Admin(^1)</td>
<td>All mDNS policy administration functions only.</td>
<td>No</td>
</tr>
</tbody>
</table>

1. Do not use RADIUS or TACACS+ 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.
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 Table 11-1 for the user groups available in Prime Infrastructure,

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

**Step 2** 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.

**Changing User Group Privileges**

Prime Infrastructure a number of editable User Groups, such as the System Monitoring and Config Managers User Groups (see Table 11-1 for a complete list). You can change the privileges assigned to these editable User Groups as needed.

Use the four “User-Defined” User Groups to define special sets of specific privileges, then assign users to these custom groups as needed using the steps in Changing User Group Memberships

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

**Step 2** Click the Group Name of an editable User Group.

**Step 3** Using the Tasks Permissions tab:

- Select the checkbox next to each task or function you want to provide to this User Group.
- Unselect the checkbox next to each task or function you want remove from this User Group’s privileges.

**Step 4** When you are finished, click Submit.

**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 view the privileges assigned to any User Group by following the steps in Viewing User Group Privileges and Membership

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

---

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

### Step 2
Click on the User Name for the user whose memberships you want to change.

### Step 3
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 4
When you are finished, click Save.

---

### Changing the Global Session Timeout for Idle Users

Prime Infrastructure provides two settings that control when and how idle users are automatically logged out:

- **User Idle Timeout**—Individual users can enable and configure this setting to end their user session when they exceed the timeout. This is enabled by default and is 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.

Administrators can specify the Global Idle Timeout for all users by choosing Administration > User Preferences.

---

### 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. For more information, see the Cisco Prime Infrastructure User Guide.

Before you set up virtual domains, always 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
- Creating Virtual Domains
- Adding Users to Virtual Domains

Understanding Virtual Domains

To manage Virtual Domains, select Administration > Virtual Domains. On 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). In addition, a Search bar is available to search for the required virtual domain.

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. This following section describes 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.

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.

Step 1  Choose Administration > Virtual Domains.
Step 2  In the Virtual Domains sidebar menu, click the parent virtual domain for your new virtual domain and then click the Add New Domain icon.

Tip  Hover 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 3  Enter the new domain’s name in the Name text box. This field is required.
Step 4  If needed, enter the new domain’s time zone, email address, and description. These are optional fields.
Step 5  Click Submit to view a summary of the newly created virtual domain and your changes to it.
Step 6  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

To add site maps to a virtual domain, follow these steps:

Step 1 Choose Administration > Virtual Domains.
Step 2 From the Virtual Domains sidebar menu, click a virtual domain to which you want to add site maps.
Step 3 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 4 Click Submit to view the summary of the virtual domain.
Step 5 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

To add network devices to a virtual domain, follow these steps:

Step 1 Choose Administration > Virtual Domains.
Step 2 From the Virtual Domains sidebar menu, click a virtual domain to which you want to add a network device.
Step 3 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 4 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 5 Click Submit to view the summary of the virtual domain.
Step 6 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

To add access points to a virtual domain, follow these steps:

Step 1  Choose Administration > Virtual Domains.
Step 2  From the Virtual Domains sidebar menu, click a virtual domain to which you want to add access points.
Step 3  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 4  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 5  Click Submit to view the summary of the virtual domain.
Step 6  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 easier 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  Choose Administration > Virtual Domains.
Step 2  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 3  Click Choose File and navigate to the CSV file you want to import.
Step 4  Click Import to import the CSV file and create the virtual domains you specified.

Related Topics
• Creating Virtual Domains
• Adding Users to 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 Choose Administration > Virtual Domains.
Step 2 In the Virtual Domains sidebar menu, hover your mouse cursor over the name of the virtual domain you want to delete. You will see a cross-hair icon appear next to the domain name.
Step 3 Click the cross-hair icon to display a popup summary of the parent.
Step 4 Click Delete.
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

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”) 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.

Related Topics
- Using Virtual Domains to Control Access
- Creating Virtual Domains
- Adding Users to Virtual Domains
- Changing Virtual Domain Access
- Virtual Domain RADIUS and TACACS+ Attributes
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** Choose Administration > Users, Roles & AAA, then click Users.

**Step 2** 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 3** Click the Virtual Domains tab.

**Step 4** 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.

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

---

Related Topics

- Using Virtual Domains to Control Access
- Understanding 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, and access points. A page with tabs for viewing the currently logged-in virtual domain-available Site Maps, Network Devices, and Access Points is displayed.

The Site Maps, Network Devices and Access Points tabs are used to add or remove components assigned to this virtual domain. You can assign any combination of site maps, network devices, and access points 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** Choose Administration > Virtual Domains.

**Step 2** Choose a virtual domain from the Virtual Domains sidebar menu.

Because all site maps, network devices, and access points 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 3** Click the applicable Site Maps, Network Devices, or Access Points tab.
Step 4  To add elements to the Selected table, click the Add button, check the check boxes of the required elements (Site Maps, Network Devices, or Access Points) 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.

Step 5  The selected elements (Site Maps, Network Devices, or Access Points) are listed in the Selected table.

Step 6  To delete elements from the Selected table, first check the check boxes of the required elements (Site Maps, Network Devices, or Access Points) to select them, and then click the Delete button.

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

Step 8  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.

Related Topics
- Using Virtual Domains to Control Access
- Understanding Virtual Domains
- Creating Virtual Domains
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** Choose Administration > Virtual Domains.

**Step 2** From the Virtual Domain Hierarchy left sidebar menu, choose the virtual domain for which you want to apply the RADIUS and TACACS+ attributes.

Click the Export Custom Attributes button.

**Step 3** Highlight the text in the RADIUS or TACACS+ Custom Attributes list (depending on which one you are currently configuring), go to your browser menu, and choose **Edit > Copy**.

**Step 4** Log in to ACS.

**Step 5** Navigate to 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 6** For the applicable user or group, click **Edit Settings**.

**Step 7** Use your browser’s **Edit > Paste** feature to place the RADIUS or TACACS+ custom attributes into the applicable text box.

**Step 8** 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.

- 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**
In Converged view: Choose **Administration > Users, Roles & AAA > User Groups**.
In Classic view: Choose **Administration > AAA > User Groups**.

**Step 2**
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.

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**
In Converged view: Choose **Administration > System Audit**.

**Step 2**
In the Application Audit Logs page, click to expand the row for which you want to view log details.
For users authenticated via TACACS+/RADIUS, the User Group column will be blank.
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 user deployed a specific template and the date and time the template was deployed.

**Step 1**  In Converged theme: Choose **Inventory > Network Audit**.

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

Configuring AAA on Prime Infrastructure

Prime Infrastructure can be configured to communicate with external authentication, authorization, and accounting (AAA) servers. The only username that has permission to configure Prime Infrastructure AAA is **root** or SuperUser. Any changes to local user accounts are in effect when configured for local mode. If using external authentication, such as RADIUS or TACACS+, the user account changes must be copied to the external server.

For information about migrating AAA servers, see the ACS 5.2 Migration Utility Support Guide.

- Setting the AAA Mode
- Adding TACACS+ Servers
- Adding RADIUS Servers
- Adding SSO Servers
- Configuring SSO Server AAA Mode
- Authenticating AAA Users Through RADIUS Using Cisco Identity Services Engine
- Configuring ACS 5.x

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 alphabets, numbers, and special characters except ‘ (single quote) and “ (double quote) while entering the shared secret key for a third-party TACACS+ or RADIUS server.

To specify a TACACS+ server and then change the AAA mode to TACACS+, follow these steps:

**Step 1**  Add one or more RADIUS or TACACS+ Server. For details, see Adding RADIUS Servers and Adding TACACS+ Servers.

**Step 2**  Select AAA Mode Settings.

**Step 3**  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 4  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 when the external server is unreachable or has network problems or the external AAA server cannot authenticate the user.

For AAA mode, the root user is always locally authenticated.

Step 5  Click **Save**.

---

## Adding TACACS+ Servers

Prime Infrastructure can use a maximum of three AAA servers.

**Step 1**  In Converged Theme: Choose **Administration > Users, Roles & AAA >TACACS+ Servers**.

In Classic view: Choose **Administration > AAA > TACACS+ Servers**.

**Step 2**  Choose **Select a command >Add TACACS+ Server**, then click **Go**.

**Step 3**  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 virtual IP address as the Local Interface IP.

---

**Related Topics**

- How High Availability Works
- Virtual IP Addressing
- Required TACACS+/RADIUS Configurations After Prime Infrastructure IP Address Changes
Adding RADIUS Servers

Prime Infrastructure can use a maximum of three AAA servers. Please note that ISE FIPS mode is not supported in Prime Infrastructure 2.2.

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

In Classic view: Choose **Administration > AAA > RADIUS Servers**.

**Step 2** Choose **Select a command > Add Radius Server**, then click **Go**.

**Step 3** Enter the RADIUS server information, then 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 Topic**

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

**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**

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**.

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 user “root” 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.
Adding SSO Servers

This section describes how to add Single Sign-On Authentication (SSO) servers to Prime Infrastructure. You can enable SSO in Prime Infrastructure. SSO allows you to enter your credentials only once, when you navigate across multiple SSO-enabled Prime Infrastructure applications. SSO makes it easier for you 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. For information about configuring SSO Server AAA Mode, see Configuring SSO Server AAA Mode.

Step 1
In Converged view: Choose Administration > Users, Roles & AAA > SSO Servers.
In Classic view: Choose Administration > AAA > SSO Servers.

Step 2
Choose Select a command > Add SSO Server, then click Go.

Step 3
Enter the SSO server information, then click Save.

The number of retries allowed for the SSO server authentication request is from 0 to 3.

Configuring SSO Server AAA Mode

Single Sign-On Authentication (SSO) is used to authenticate and manage users in a multiuser, multirepository environment and to store and retrieve the credentials that are used for logging in to disparate systems. You can set up Prime Infrastructure as the SSO server for other instances of Prime Infrastructure.

As Prime Infrastructure does not support CA certificates and self-signed certificates in Java, SSO requires accurate DNS configuration. You must define the DNS with fully qualified domain name (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 fully qualified domain name (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. For instructions on regenerating the certificate, see the Cisco Prime Infrastructure Server Hardening section of the Cisco Prime Infrastructure Classic View Configuration Guide for Wireless Devices, Release 2.1.

Note
After you regenerate the SSL/TLS certificate, you must redistribute the new certificate to all users that have the old certificate.

Step 1
In Converged view: Choose Administration > Users, Roles & AAA > SSO Server AAA Mode.
In Classic view: Choose Administration > AAA > SSO Server AAA Mode.
Chapter 11 Controlling User Access

Configuring AAA on Prime Infrastructure

Step 2 Choose which SSO Server AAA mode you want to use. Only one can be selected 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 3 Select the Enable Fallback to Local check box if you want the administrator to use the local database when the external SSO AAA server is down.

This check box is unavailable if Local was selected as the SSO Server AAA Mode type.

Step 4 Click OK.

Authenticating AAA Users Through RADIUS Using Cisco Identity Services Engine

You can integrate Prime Infrastructure with 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 more information, see Adding Prime Infrastructure as an AAA Client in ISE.

Step 2 Create a new User group in ISE. For more information, 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 more information, see Creating a New User and Adding to a User Group in ISE.

Step 4 Create a new Authorization profile. For more information, see Creating a New Authorization Profile in ISE.

Step 5 Create an Authorization policy rule. For more information, see Creating an Authorization Policy Rule in ISE.

Step 6 Create an Authentication policy. For more information, 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 more information, see Configuring AAA in 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.

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.

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).
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, 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 Virtual Domain RADIUS and TACACS+ Attributes).

Step 6  Save the authorization profile.

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.
For more information about creating Identity User Groups, see Creating a New User Group in ISE.
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.
For more information about creating authorization profiles, see Creating a New Authorization Profile in ISE.
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.
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

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 Insert 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
Chapter 11  Controlling User Access

Configuring AAA in Prime Infrastructure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Log in to Prime Infrastructure as root, then choose Administration &gt; Users, Roles &amp; AAA &gt; RADIUS Servers.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Add a new RADIUS server with the ISE IP address, then click Save.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Log in to ISE, then choose Administration &gt; AAA &gt; AAA Mode Settings.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Select RADIUS as the AAA mode, then click Save.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Log off of Prime Infrastructure.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Log in again to Prime Infrastructure as an AAA user defined in ISE.</td>
</tr>
<tr>
<td></td>
<td>For example, log in as user ncs-sysmon.</td>
</tr>
<tr>
<td></td>
<td>For more information about creating users in ISE, see Creating a New User and Adding to a User Group in ISE.</td>
</tr>
</tbody>
</table>

Configuring ACS 5.x

This section provides instructions for configuring ACS 5.x to work with Prime Infrastructure:

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

Creating Network Devices and AAA Clients

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Choose Network Resources &gt; Network Devices and AAA Clients.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Enter an IP address.</td>
</tr>
</tbody>
</table>
Adding Groups

Step 1  Choose Users and Identity Stores > Identity Groups.
Step 2  Create a group.

Adding Users

Step 1  Choose Users and Identity Stores > Internal Identity Stores > Users.
Step 2  Add a user, and then map a group to that user.

Creating Policy Elements or Authorization Profiles for RADIUS

Step 1  Choose Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles, then click Create.
Step 2  Enter the required information, then click Submit.

Creating Policy Elements or Authorization Profiles for TACACS+

Before You Begin
Ensure that you add the relevant Menu Access task so that the 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  Choose Policy Elements > Authorization and Permissions > Device Administration > Shell Profiles, then click Create.
Step 2  Enter the required information, then click Submit.

Creating Service Selection Rules for RADIUS

Step 1  Choose Access Policies > Access Services > Service Selection Rules, then click Create.
Step 2  Enter the required information, then click OK.
Creating Service Selection Rules for TACACS+

Step 1  Choose Access Policies > Access Services > Service Selection Rules, then click Create.
Step 2  Enter the required information, then click OK.

Configuring 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.

Configuring Access Services for TACACS+

Step 1  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.