Controlling User Access

- Creating Additional Administrative Users
- Managing User Accounts
- Creating User Groups to Control Access to Prime Infrastructure Functions
- Changing Display Preferences
- Using Virtual Domains to Control Access to Sites and Devices
- 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 Access to Prime Infrastructure Functions
- Changing Password Policy

Viewing Active User Sessions

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

Step 1 In Lifecycle 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
- 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. Prime Infrastructure supports external user authentication using these access restrictions and authenticates the users against the TACACS+ and RADIUS servers.

Step 1 Choose **Administration > Users, Roles & AAA > 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 groups to which this user belongs by selecting the checkbox next to each group name.

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**.

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.

Step 3 Click **Save**.

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.

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.

Changing User Passwords

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 Topic

- Creating Additional Administrative Users

Changing User Access to Prime Infrastructure Functions

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

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

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

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

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

Changing Password Policy

Prime Infrastructure supports various password policy controls, such as minimum length, repeated characters, and so forth.

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

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

Creating User Groups to Control Access to Prime Infrastructure Functions

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 10-1 for the user groups available in Prime Infrastructure.

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

Step 2 Click a group name to change the tasks this group is allowed to perform. Table 10-1 lists the user groups.

Note Not all groups have the same tasks. Groups that allow monitoring privileges only, for example, System Monitoring, will not have administrator-level tasks listed as options.

The Access to the NCS Rest NBI option, available for Admin and User Defined groups only, allows users of the specified group to access the REST-based APIs. (Root and Super User groups have access to these APIs by default.) For more information about the REST-based APIs, click the question mark icon at the top right of any Prime Infrastructure page, then select **Prime Infrastructure REST API**.

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

Table 10-1 Default User Groups

User Group	Description
Admin	Group for Prime Infrastructure Administration.
Config Managers	Group for monitoring and configuration tasks.
Lobby Ambassador	Group to allow Guest user administration only. This group is not editable.
Monitor Lite	Group to allow monitoring of assets only. This group is not editable.
North Bound API	Group to allow access to North Bound APIs. This group is not editable.
Root	Group for root user. This group is not editable.
Super Users	Group to allow all Prime Infrastructure tasks.
System Monitoring	Group for monitoring only tasks.
User Assistant	Group to allow Local Net user administration only. This group is not editable.
User-Defined 1	User definable group.
User-Defined 2	User definable group.
User-Defined 3	User definable group.
User-Defined 4	User definable group.

Changing Display Preferences

You can specify display options in Prime Infrastructure by choosing **Administration > User Preferences**. Table 10-2 lists the options you can adjust.

When non-administrative users log in to Prime Infrastructure and try to modify the user preferences, the "Permission Denied" message appears, which is an expected behavior.

Step 1 Choose **Administration > User Preferences**.

Step 2 Use the Items Per List Page drop-down list to configure the number of entries shown on a given list page (such as alarms, events, AP list, and so on).

Step 3 Specify how often you want the home page refreshed by selecting the **Refresh home page** check box and choosing a time interval from the Refresh home page every drop-down list.

Step 4 If you want to switch back from MSE admin UI to legacy MSE UI, unselect the **Use MSE Admin View** check box. By default, the check box is selected.

Step 5 Select the **Logout idle user** check box and configure the Logout idle user after text box, in minutes, that a user session can be idle before the server cancels the session.

Step 6 If you want the maps and alarms page to automatically refresh when a new alarm is raised by Prime Infrastructure, select the **Refresh Map/Alarms page on new alarm** check box in the Alarms portion of the page.

Step 7 From the Refresh Alarm count in the Alarm Summary every drop-down list choose a time interval to specify how often to reset.

Step 8 If you do not want the alarm acknowledge warning message to appear, select the **Disable Alarm Acknowledge Warning Message** check box.

Step 9 Click **Edit Alarm Categories** to select the alarm categories to display in the Alarm Summary page.

Step 10 In the **Select Alarms** page, choose the default category to display from the drop-down list, and select the alarm categories and subcategories to display from the alarm toolbar. Click **Save** to save the alarm category list. The selected alarm category and subcategories appear in the User Preferences page.

Step 11 Click **Save**.

Table 10-2 User Preference Options

Option	Description
Items Per List	You can set the number of items, such as controllers or access points, to display in pages that list these items. Choose the number of items to display from the Items Per List Page drop-down list.
Use Next Generation Maps	Select the check box if you want to use the Next Generation Maps feature.
Logout idle user	Select the check box if you want to configure the amount of time, in minutes, that a user session can be idle before the server cancels the session. If the Logout idle user check box is unselected, the user session does not time out.
Logout idle user after	Choose the maximum number of minutes that a server waits for an idle user. The valid range is between 15 and 120 minutes. If the Logout idle user check box is unselected, the user session does not time out.

Table 10-2 User Preference Options

Option	Description
Refresh Map/Alarms page on new alarm	Select the check box to refresh map and alarm pages each time a new alarm is generated.
Refresh Alarm count in the Alarm Summary every	Choose the frequency of the Alarm Summary refresh from the drop-down list (every 5, seconds, 15 seconds, 30 seconds, 1 minute, 2 minutes, or 5 minutes).
Display Alarm Category in Alarm Summary page	Choose the alarm category that you want to display in the minimized Alarm Summary (Alarm Summary, Malicious AP, Unclassified AP, Coverage Holes, Security, Controllers, Access Points, Mobility Services, Mesh Links, Prime Infrastructure, or Performance).
Disable Alarm Acknowledge Warning Message	When you acknowledge an alarm, a warning displays as a reminder that a recurrence of the problem does not generate another alarm unless this functionality is disabled. Select this check box to stop the warning message from displaying.
Choose alarms for Alarm Summary Toolbar	To select alarms for the Alarm Summary Toolbar, click **Edit Alarm Categories** and choose the required alarm categories and subcategories.

Using Virtual Domains to Control Access to Sites and Devices

Virtual domains allow you to control who has access to specific sites and devices. After you add devices to Prime Infrastructure, you can configure virtual domains. Virtual domains are logical groupings of devices and are used to control who can administer the group. By creating virtual domains, an administrator allows users to view information relevant to them specifically and restricts their access to other areas. Virtual domain filters allow users to configure devices, view alarms, and generate reports for their assigned part of the network *only*.

The email address and time zone that you specify in the Virtual Domains page (Administration > Virtual Domains) are used when scheduling and e-mailing 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 2.1 User Guide*.

Virtual domains can be based on physical sites, device types, user communities, or any other designation you choose.

Before you set up virtual domains, you should determine which users should have access to which sites and devices in your network.

- Understanding Virtual Domain Hierarchy
- Creating Site-Oriented Virtual Domains

Understanding Virtual Domain Hierarchy

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.

Because network elements are managed hierarchically, some features and components such as report generation, searches, templates, config groups, and alarms are affected.

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

This 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.

Note 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.

Note If you create a subvirtual 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.

Note 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.

Note 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 is displayed for primary, secondary, and tertiary controllers rather than the limited number specified in the partition.

Note If a controller configuration is modified by multiple virtual domains, complications might 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 Site-Oriented Virtual Domains

By default, there is only one virtual domain defined (*root*) in Prime Infrastructure.

When you create a site-oriented virtual domain, you allows users to view information in a specific site and restrict their access to other areas.

The following steps explain how to choose a segment of all the devices at a particular location and make them part of the “Site 1 Routers” virtual domain.

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

Step 2 Click **New**.

By default, only one virtual domain (*root*) is defined in Prime Infrastructure. The selected virtual domain becomes the parent virtual domain of the newly created virtual subdomain.

Step 3 Enter **Site 1 Routers** for the virtual domain name, then click **Submit**.

Step 4 On the Sites tab, move the sites that you want to associate with the virtual domain to the Selected Sites column, then click **Submit**.

Step 5 Click **OK** in the confirmation dialog boxes.

User Access in Virtual Domains

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

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

The administrator specifies for each user a set of allowed virtual domains. Only one of these can be active for that user at login. The user can change the current virtual domain by 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.

- Adding Users to Virtual Domains
- Adding Sites and Devices 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*.

Note 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.

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

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

Step 3 Click the Virtual Domains tab.

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

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

Adding Sites and Devices to Virtual Domains

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

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

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

Changing Virtual Domain Access

Choose a virtual domain from the Virtual Domain Hierarchy on the left sidebar menu to view or edit its assigned maps, controllers, access points, and switches. The Summary page appears. This page includes tabs for viewing the currently logged-in virtual domain-available maps, controllers, access points, and switches.

The Maps, Controllers, Access Points, and Switches tabs are used to add or remove components assigned to this virtual domain. You can assign any combination of site maps, controllers, access points, or wired devices 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 hierarchy from the Virtual Domain Hierarchy left sidebar menu.

Because all maps, controllers, 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 controllers and access points.

Step 3 Click the applicable **Site Maps**, **Controller**, **Access Points**, or **Wired Devices** tab.

Step 4 In the Available (Site Maps, Controllers, Access Points, or Wired Devices) column, click to highlight the new component(s) you want to assign to the virtual domain.

Step 5 Click **Add** to move the selected elements to the Selected (Site Maps, Controllers, Access Points, or Wired Devices) column.

Step 6 To remove a component from the virtual domain, click to highlight the component in the Selected (Site Maps, Controllers, Access Points, or Wired Devices) column, and click **Remove**. The component returns to the Available column.

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.

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

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 button on the Virtual Domain Hierarchy left sidebar menu 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.

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.

Step 3 Click **Export**.

Step 4 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 5 Log in to ACS.

Step 6 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 7 For the applicable user or group, click **Edit Settings**.

Step 8 Use your browser's Edit > Paste feature to place the RADIUS or TACACS+ custom attributes into the applicable text box.

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

Note For more information on adding RADIUS and TACACS+ attributes to the ACS server, see Adding Prime Infrastructure User Groups into ACS for TACACS+ or Adding Prime Infrastructure User Groups into ACS for RADIUS.

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 Lifecycle 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.

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

Viewing 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 Lifecycle 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 Lifestyle view: Choose **Operate > 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 permissions to configure Prime Infrastructure AAA is *root* or SuperUser. Any changes to local users accounts are in effect when configured for local mode. If using external authentication, such as RADIUS or TACACS+, the user 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 4.x
- 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 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 a TACACS+ Server. For more information, see Adding TACACS+ Servers.

Step 2 Select **AAA Mode**.

Step 3 Select **TACACS+**.

Step 4 Select the **Enable Fallback to Local** check box if you want to use the local database when the external AAA server is down. You then need to specify the conditions under which the fallback to local Prime Infrastructure user accounts 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.

Step 5 Click **Save**.

Adding TACACS+ Servers

Prime Infrastructure can use a maximum of three AAA servers.

Step 1 In Lifestyle view: 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.

Related Topic

- 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 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

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 Lifecycle 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:  ….
```

Step 1 In Lifecycle view: Choose **Administration > Users, Roles & AAA >SSO Server AAA Mode**.

In Classic view: Choose **Administration > AAA> SSO Server AAA Mode**.

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 From Prime Infrastructure, get the custom attributes that you want to add to the ISE authorization profile:

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

b. Select the user group whose permissions you want to copy into the ISE Authorization Profile.

c. Click **Task List**.

d. Copy the line for the desired role for the RADIUS version (for example, **NCS:role0=System Monitoring**).

Note If the ISE authorization profile will match the Prime Infrastructure User Group permissions exactly, you need to copy the *role* lines only. To create a customized authorization profile, you can select a set of individual *task* lines. However, keep in mind that RADIUS imposes an overall length limit of 4096 bytes for RADIUS attributes.

Step 2 Create an ISE Authorization Profile in ISE by choosing **ISE > Policy > Policy Elements > Results**.

Step 3 From the left sidebar menu, choose **Authorization > Authorization Profiles**, then click **Add**.

Step 4 Enter the name and description for the profile.

Step 5 Choose **ACCESS_ACCEPT** from the Access Type drop-down list.

Step 6 In the Advanced Attribute Settings area, add Prime Infrastructure User Group RADIUS custom attributes along with the virtual domain attributes at the end.

a. Select **cisco - av - pair** and paste the Prime Infrastructure User Group RADIUS custom attribute next to it, for example **NCS:role0=System Monitoring**. You can copy and paste specific *tasks* (instead of *roles*) if you want to specify more granular access control. However, keep in mind that RADIUS imposes an overall length limit of 4096 bytes for RADIUS attributes.

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). Click the link at the bottom of the Task List page to view the virtual domain custom attributes.

Step 7 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. Cisco recommends 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*

Configuring AAA in Prime Infrastructure

Step 1 Log in to Prime Infrastructure as *root*, then choose **Administration > 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 > AAA > AAA Mode Settings**.

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

Step 5 Log off of Prime Infrastructure.

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

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

For more information about creating users in ISE, see Creating a New User and Adding to a User Group in ISE.

Configuring ACS 4.x

This section provides instructions for configuring ACS 4.x to work with Prime Infrastructure.

To import tasks into Cisco Secure ACS server, you must add Prime Infrastructure to an ACS server (or non-Cisco ACS server):

- Adding Prime Infrastructure to an ACS Server for Use with TACACS+ Server
- Adding Prime Infrastructure User Groups into ACS for TACACS+
- Adding Prime Infrastructure to an ACS Server for Use with RADIUS
- Adding Prime Infrastructure User Groups into ACS for RADIUS
- Adding Prime Infrastructure to a Non-Cisco ACS Server for Use with RADIUS

Adding Prime Infrastructure to an ACS Server for Use with TACACS+ Server

Note The instructions and illustrations in this section pertain to ACS Version 4.1 and might vary slightly for other versions or other vendor types. See the Cisco Secure ACS documentation or the documentation for the vendor you are using.

Step 1 Click **Add Entry** in the Network Configuration page of the ACS server.

Step 2 In the AAA Client Hostname text box, enter the Prime Infrastructure hostname.

Step 3 Enter the Prime Infrastructure IP address in the AAA Client IP Address text box.

Ensure that the interface that you use for ACS is the same as the interface specified in Prime Infrastructure and that the interface is reachable.

Step 4 In the Shared Secret text box, enter the shared secret that you want to configure on both Prime Infrastructure and ACS servers.

Step 5 Choose **TACACS+** in the Authenticate Using drop-down list.

Step 6 Click **Submit + Apply**.

Step 7 From the left sidebar menu, choose **Interface Configuration**.

Step 8 In the Interface Configuration page, click the **TACACS+ (Cisco IOS)** link.

The TACACS+ (Cisco IOS) Interface Configuration page appears.

Step 9 In the New Services portion of the page, add NCS in the Service column heading.

Step 10 Enter **HTTP** in the Protocol column heading.

Note HTTP must be in uppercase.

Step 11 Select the check box in front of these entries to enable the new service and protocol.

Note The ACS 4.x configuration is complete only when you specify and enable NCS service with HTTP protocol.

Step 12 Click **Submit**.

Adding Prime Infrastructure User Groups into ACS for TACACS+

Step 1 Log in to Prime Infrastructure.

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

Step 3 Click the Task List link of the user group that you want to add to ACS. The Export Task List page appears.

Step 4 Highlight the text inside of the TACACS+ Custom Attributes, go to your browser menu, and choose **Edit > Copy**.

Step 5 Log in to ACS.

Step 6 Go to Group Setup. The Group Setup page appears.

Step 7 Choose which group to use, and click **Edit Settings**. Prime Infrastructure HTTP appears in the TACACS+ setting.

Step 8 Use Edit > Paste in your browser to place the TACACS+ custom attributes from Prime Infrastructure into this text box.

Note When 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.

Step 9 Select the check boxes to enable these attributes.

Step 10 Click **Submit + Restart**. You can now associate ACS users with this ACS group.

To enable TACACS+ in Prime Infrastructure, see Adding TACACS+ Servers.

Note You must add a virtual domain in ACS when exporting the task list to ACS. This might be the ROOT-DOMAIN virtual domain. For more information on virtual domains, see Using Virtual Domains to Control Access to Sites and Devices.

Adding Prime Infrastructure to an ACS Server for Use with RADIUS

If you have a non-Cisco ACS server, see Adding Prime Infrastructure to a Non-Cisco ACS Server for Use with RADIUS.

Step 1 Go to Network Configuration on the ACS server.

Step 2 Click **Add Entry**.

Step 3 In the AAA Client Hostname text box, enter Prime Infrastructure hostname.

Step 4 In the AAA Client IP Address text box, enter Prime Infrastructure IP address.

Note Ensure the interface that you use for ACS is the same you specified in Prime Infrastructure and it is reachable.

Step 5 In the Shared Secret text box, enter the shared secret that you want to configure on both Prime Infrastructure and ACS servers.

Step 6 Choose **RADIUS (Cisco IOS/PIX 6.0)** from the Authenticate Using drop-down list.

Step 7 Click **Submit + Apply**. You can now associate ACS users with this ACS group.

To enable RADIUS in Prime Infrastructure, see Adding RADIUS Servers.

Note From Prime Infrastructure Release 1.0 and later, you are required to add a virtual domain in ACS when exporting the task list to ACS. This might be the ROOT-DOMAIN virtual domain. For more information on virtual domains, see Using Virtual Domains to Control Access to Sites and Devices.

Adding Prime Infrastructure User Groups into ACS for RADIUS

Step 1 Log in to Prime Infrastructure.

Step 2 Choose **Administration > Users, Roles & AAA > User Groups**. The All Groups page appears.

Step 3 Click the Task List link of the user group that you want to add to ACS. The Export Task List page appears.

Step 4 Highlight the text inside of the RADIUS Custom Attributes, go to the menu of your browser, and choose **Edit > Copy**.

Note When you upgrade Prime Infrastructure, any permissions on the TACACS+ or RADIUS server must be readded.

Step 5 Log in to ACS.

Step 6 Go to Group Setup. The Group Setup page appears.

Step 7 Choose which group to use, and click **Edit Settings**. Find [009\001]cisco-av-pair in the **Cisco IOS/PIX 6.x RADIUS Attributes** area.

Step 8 Use Edit > Paste in your browser to place the RADIUS custom attributes from Prime Infrastructure into this text box.

Note When you upgrade Prime Infrastructure, any permissions on the TACACS+ or RADIUS server must be readded.

Step 9 Select the check boxes to enable these attributes.

Step 10 Click **Submit + Restart**. You can now associate ACS users with this ACS group.

To enable RADIUS in Prime Infrastructure, see Adding RADIUS Servers.

For information on adding Prime Infrastructure virtual domains into ACS for TACACS+, see Virtual Domain RADIUS and TACACS+ Attributes.

Note You must add a virtual domain in ACS when exporting the task list to ACS. This might be the ROOT-DOMAIN virtual domain. For more information on virtual domains, see Using Virtual Domains to Control Access to Sites and Devices.

Adding Prime Infrastructure to a Non-Cisco ACS Server for Use with RADIUS

When you use a RADIUS server to log in to Prime Infrastructure, the AAA server sends back an access=accept message with a user group and a list of available tasks, after the username and password were verified. The access=accept message comes back as a fragmented packet because of the large number of tasks in some user groups. You can look in the following file to see the tasks associated with a given user group: C:\Program Files\Prime Infrastructure\webnms\webacs\WEB-INF\security\usergroup-map.xml. The tasks are passed back as a vendor specific attribute (VSA), and Prime Infrastructure requires authorization information using the VSA (IETF RADIUS attribute number 26). The VSA contains Prime Infrastructure RADIUS task list information.

The content of the VSA is as follows:

- Type = 26 (IETF VSA number)
- Vendor Id = 9 (Cisco vendor ID)
- Vendor Type = 1 (Custom attributes)
- Vendor Data = Prime Infrastructure task information (for example Prime Infrastructure: task0 = Users and Group)

Each line from Prime Infrastructure RADIUS task list should be sent in its own RADIUS VSA.

In the data portion of the access=access packet, the truncated output sometimes shows only one role sent back for an Admin user group login. The tasks associated with the role start with task0 and increment with task1, task2, and so on. Table 10-3 defines what these attributes in the access=access packet example signify.

```
0000 06 6d 0e 59 07 3d 6a 24 02 47 07 35 d2 12 a4 eb .m.Y.=j$G.5...
0010 a2 5a fa 84 38 20 e4 e2 3a 3a bc e5 1a 20 00 00 .Z..8..:::..
0020 00 09 01 1a 57 69 72 65 6c 65 73 73 2d 57 43 53 ....Prime Infrastructure
0030 3a 72 6f 6c 65 30 3d 41 64 6d 69 6e 1a 2b 00 00 :role0=Admin.+...
0040 00 09 01 25 57 69 72 65 6c 65 73 73 2d 57 43 53 ...%Prime Infrastructure
0050 3a 74 61 73 6b 30 3d 55 73 65 72 73 20 61 6e 64 :task0=Users and
0060 20 47 72 6f 75 70 73 1a 27 00 00 00 09 01 21 57 Groups.”....!W
0070 69 72 65 6c 65 73 73 2d 57 43 53 3a 74 61 73 6b Prime Infrastructure:task
0080 31 3d 41 75 64 69 74 20 54 72 61 69 6c 73 xx xx 1=Audit Trails.*
```

Table 10-3 Access=Access Packet Example

Attribute	Description
1a (26 in decimal)	Vendor attribute
2b (43 bytes in decimal)	Length as the total number of bytes to skip and still reach the next TLV (for task0, Users and Groups)
4-byte field	Vendor Cisco 09
01	Cisco AV pair - a TLV for Prime Infrastructure to read
25 (37 bytes in decimal)	Length
hex text string	Prime Infrastructure:task0=Users and Groups
	The next TLV until the data portion is completely processed
255.255.255.255	TLV: RADIUS type 8 (framed IP address)
Type 35 (0x19)	A class, which is a string
Type 80 (0x50)	Message authenticator

To troubleshoot, perform the following tasks:

- Verify if the RADIUS packet is an access accept.
- Verify the task names for the user group in the access accept.
- Look at the different length fields in the RADIUS packet.

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

Step 1 Choose **Network Resources > Network Devices and AAA Clients**.

Step 2 Enter an IP address.

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**.