User Permissions and Device Access

User Interfaces, User Types, and How To Transition Between Them

These topics describe the GUI and CLI interfaces used by Prime Infrastructure, and how to transition between the Prime Infrastructure and Linux CLI interfaces.

User Interfaces and User Types

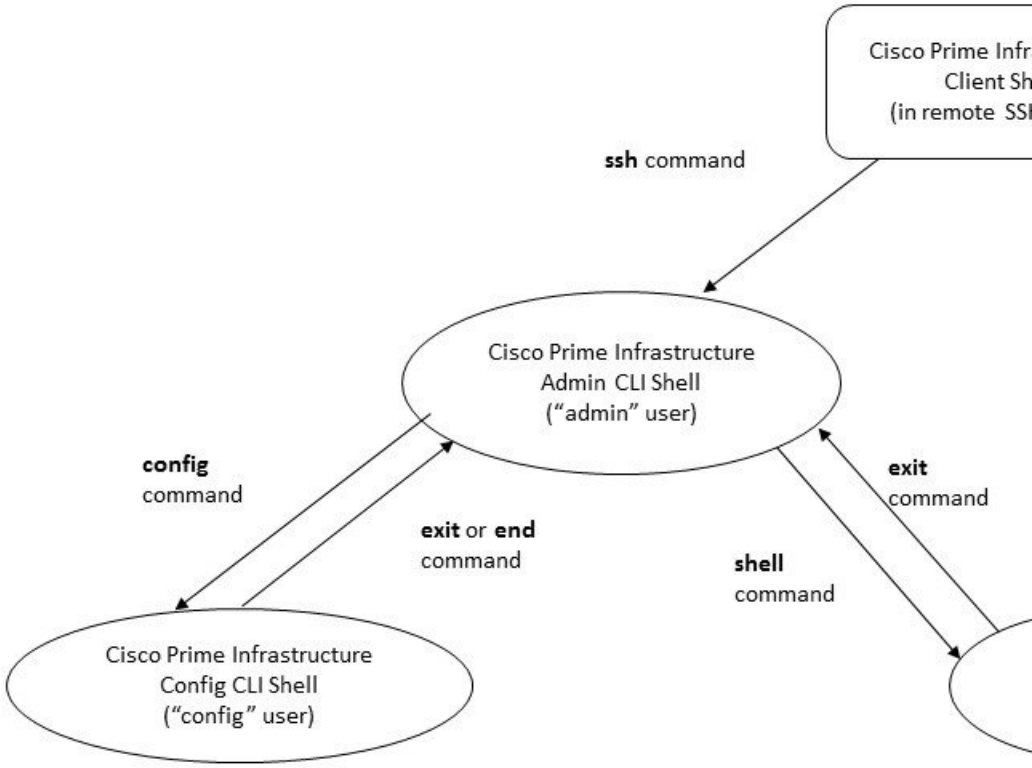
The following table describes the user interfaces employed by Prime Infrastructure , and the types of users that can access each interface.

Prime Infrastructure User Interface	Interface Description	Prime Infrastructure User Types
Prime Infrastructure web GUI	Web interface that facilitates day-to-day and administration operations using the web GUI. These users can have varying degrees of privileges and are classified into role-based access control (RBAC) classes and subclasses. This interface provides a subset of operations that are provided by the Prime Infrastructure CLI admin and CLI config users.	**Prime Infrastructure web GUI everyday users**—Created by web GUI root user . These users have varying degrees of privileges and are classified into role-based access control (RBAC) classes and subclasses called *user groups* (Admin, Super Users, Config Managers, and so forth). For information on the user groups, see Types of User Groups, on page 7. **Prime Infrastructure web GUI root user**—Created at installation and intended for first-time login to the web GUI, and for creating other user accounts. This account should be disabled after creating at least one web GUI user that has Admin privileges—that is, a web GUI user that belongs to the Admin or Super Users user group. See Disable and Enable the Web GUI root User, on page 6. **Note** The Prime Infrastructure web GUI root user is not the same as the Linux CLI root user, nor is it the same as the Prime Infrastructure CLI admin user. .
Prime Infrastructure Admin CLI	Cisco proprietary shell which provides secure and restricted access to the system (as compared with the Linux shell). This Admin shell and CLI provide commands for advanced Prime Infrastructure administration tasks. These commands are explained throughout this guide. To use this CLI, you must have Prime Infrastructure CLI admin user access. You can access this shell from a remote computer using SSH.	**Prime Infrastructure CLI Admin user**—Created at installation time and used for administration operations such as stopping and restarting the application and creating remote backup repositories. (A subset of these administration operations are available from the web GUI). To display a list of operations this user can perform, enter **?** at the prompt. Some tasks must be performed in config mode. To transition to config mode, use the procedure in Transition Between the Prime Infrastructure admin CLI and Prime Infrastructure config CLI, on page 4. The admin CLI user can create other CLI users for a variety of reasons, using the following command: `(config) username username password role {admin|user} password` These users may have admin-like privilege/roles or lower level privileges as defined during creation time. To create a Prime Infrastructure CLI user with admin privileges, run the **username** command with the **admin** keyword; otherwise, use the **user** keyword.
Prime Infrastructure Config CLI	Cisco proprietary shell which is restricted and more secure than the Linux shell. This Config shell and CLI provide commands for Prime Infrastructure system configuration tasks. These commands are explained throughout this guide. To use this CLI, you must have admin-level user access (see the information in the User Types column of this table). You can access this shell from the Admin CLI shell.	

Prime Infrastructure User Interface	Interface Description	Prime Infrastructure User Types
Linux CLI	Linux shell which provides all Linux commands. The Linux shell should only be used by Cisco technical support representatives. Regular system administrators should not use the Linux shell. You cannot reach this shell from a remote computer using SSH; you can only reach it through the Prime Infrastructure admin shell and CLI.	**Linux CLI admin user**—Created at installation time and used for Linux-level administration purposes. This admin user can get root-level privileges by following the procedure in Log In and Out as the Linux CLI root User, on page 5. Tasks that require root-level permissions should only be performed by Cisco Support teams to debug product-related operational issues. For security purposes, the Linux CLI admin and root users should be disabled; see Disable and Enable the Linux CLI Users in Prime Infrastructure, on page 6.

How to Transition Between the CLI User Interfaces in Prime Infrastructure

The following figure illustrates how to transition between the Prime Infrastructure and Linux CLI user interfaces on deployments running Prime Infrastructure.



Transition Between the Prime Infrastructure admin CLI and Prime Infrastructure config CLI

To move from the Prime Infrastructure admin CLI to the Prime Infrastructure config CLI, enter **config** at the admin prompt.

```
(admin)# config
(config)#
```

To move from the config CLI back to the admin CLI, enter **exit** or **end** at the config prompt:

```
(config)# exit
(admin)#
```

Log In and Out as the Linux CLI root User

The Linux CLI has two shell users: One with administrative access (Linux CLI admin user), and another with root access (Linux CLI root user). The diagram in How to Transition Between the CLI User Interfaces in Prime Infrastructure, on page 3 illustrates the flow for logging in and out as the various CLI users.

To log in as the Linux CLI root user, you will have to transition from being the Prime Infrastructure CLI admin user to the Linux CLI admin user to the Linux CLI root user. The following procedure gives you the exact steps you must follow.

Before you begin

If the Linux CLI user is disabled, re-enable it. See Disable and Enable the Linux CLI Users in Prime Infrastructure, on page 6.

Step 1 To log in as the Linux CLI root user:

a) Start an SSH session with the Prime Infrastructure server and log in as the Prime Infrastructure CLI admin user.

b) As the Prime Infrastructure CLI admin user, log in as the Linux CLI admin user:

```
shell
Enter shell access password:  password
```

c) Log in as the Linux CLI root user.

```
sudo -i
```

By default, the Linux CLI shell prompt is the same for the Linux CLI admin and root user. You can use the **whoami** command to check the current user.

Step 2 To exit:

a) Log out as the Linux CLI root user.

```
exit
```

b) Log out as the Linux CLI admin user.

```
exit
```

You are now logged in as the Prime Infrastructure CLI admin user.

What to do next

For security purposes, disable the Linux CLI root user. See Disable and Enable the Linux CLI Users in Prime Infrastructure, on page 6.

Enable and Disable root Access for the Linux CLI and the Prime Infrastructure Web GUI

As described in How to Transition Between the CLI User Interfaces in Prime Infrastructure, on page 3, after installation, you should disable the Prime Infrastructure web GUI **root** user after creating at least one other web GUI user that has Admin or Super Users privileges. See Disable and Enable the Web GUI root User, on page 6.

The Linux CLI root user is disabled after installation time. If you need to re-enable it, follow the procedure in Disable and Enable the Linux CLI Users in Prime Infrastructure, on page 6.

Disable and Enable the Linux CLI Users in Prime Infrastructure

This procedure shows you how to disable and enable the Linux CLI admin shell in deployments running Prime Infrastructure. When you disable the shell, you will no longer be able to log in as the Linux CLI admin or root users. When the shell is enabled, users can log in by following the procedure in How to Transition Between the CLI User Interfaces in Prime Infrastructure, on page 3.

Before you begin

Make sure you have the password for the Linux CLI admin user.

Step 1 Log in to Prime Infrastructure as the Prime Infrastructure CLI admin user. See Establish an SSH Session With the Prime Infrastructure Server.

Step 2 Disable the Linux CLI admin shell (which disables the Linux CLI admin and root users):

```
shell disable
Enter shell access password: passwd
shell access is disabled
```

Step 3 To re-enable the Linux CLI admin shell (you must run this command as the Prime Infrastructure CLI admin user):

```
shell
Shell access password is not set
Configure password for shell access

Password: passwd
Password again: passwd

Shell access password is set
Run the command again to enter shell
```

Disable and Enable the Web GUI root User

Step 1 Log into the Prime Infrastructure web GUI as root, and create another web GUI user that has root privileges—that is, a web GUI user that belongs to the Admin or Super Users user group. See Add Users and Manage User Accounts, on page 32. Once this is done, you can disable the web GUI **root** account.

Step 2 Disable the Prime Infrastructure web GUI root user account. (The web GUI admin account, which remains active, can perform all required CLI functions.)

```
ncs webroot disable
```

Step 3 To re-enable the account:

```
ncs webroot enable
```

Control the Tasks Web Interface Users Can Perform (User Groups)

For Web Interface users, in Prime Infrastructure user authorization is implemented through user groups. A user group contains a list of tasks that control which parts of Prime Infrastructure a user can access and the tasks the user can perform in those parts.

While user groups control what the user can do, *virtual domains* control the devices on which a user can perform those tasks. Virtual domains are described in Create Virtual Domains to Control User Access to Devices, on page 45.

Prime Infrastructure provides several predefined user groups. If a user belongs to a user group, the user inherits all of the authorization settings for that group. A user is normally added to user groups when their account is created.

These topics explain how to manage user authorization:

Types of User Groups

Prime Infrastructure provides the following predefined user groups:

For information about CLI users, see User Interfaces and User Types, on page 1.

User Groups—Web UI

Prime Infrastructure provides the default web GUI user groups listed in the following table. You can assign users to multiple groups, except for users that belong to the Monitor Lite user group (because Monitor Lite is meant for users who should have very limited permissions).

See View and Change the Tasks a Group Can Perform, on page 30 for information on the tasks that pertain to each user group and the default settings.

User Group	Group Task Focus
Root	All operations. The group permissions are not editable. The root web UI user is available after installation and is described in User Interfaces and User Types, on page 1. A best practice is to create other users with Admin or Super Users privileges, and then disable the root web UI user as described in Disable and Enable the Web GUI root User, on page 6.
Super Users	All operations (similar to root). The group permissions are editable.
Admin	Administer the system and server. Can also perform monitoring and configuration operations. The group permissions are editable.
Config Managers	Configure and monitor the network (no administration tasks). The permissions assigned to this group are editable.
System Monitoring	Monitor the network (no configuration tasks). The group permissions are editable.
Help Desk Admin	Only has access to the help desk and user preferences related pages. Members of this user group cannot be members of any other user group. This is a special group which lacks access to the user interface.
Lobby Ambassador	User administration for Guest users only. Members of this user group cannot be members of any other user group.
User–Defined 1–4	these are blank groups and can be edited and customized as needed.
Monitor Lite	View network topology and use tags. The group permissions are not editable. Members of this user group cannot be members of any other user group.
North Bound API	Access to the SOAP APIs. **Note** No acesss restriction for admin owned templates.
User Assistant	Local Net user administration only. Members of this user group cannot be members of any other user group.
mDNS Policy Admin	mDNS policy administration functions. **Note** We recommend you to not use RADIUS, TACACS+ or SSO to create users to be included in the “mDNS Policy Admin” group, because the AAA server do not have the required multicast DNS settings.

User Groups—NBI

Prime Infrastructure Cisco Prime Infrastructure provides the default NBI user groups listed in the following table. The permissions in these groups are not editable.

See View and Change the Tasks a Group Can Perform, on page 30 for information on the tasks that pertain to each user group and the default settings.

User Group	Provides access to:
NBI Credential	The Northbound Interface Credential API
NBI Read	The Northbound Interface Read API.
NBI Write	The Northbound Interface Write API.

View and Change the Tasks a User Can Perform

The tasks a user can perform is controlled by the user groups the user belongs to. Follow these steps to find out which groups a user belongs to and which tasks a user is authorized to perform.

Note If you want to check the *devices* a user can access, see Assign Virtual Domains to Users, on page 51.

Step 1 Choose **Administration** > **Users** > **Users, Roles & AAA** and locate the user name.

Step 2 Locate the user name and check the **Member of** column to find out which user groups the user belongs to.

Step 3 Click a user group hyperlink. The **Group Detail** window lists the tasks that group members can and cannot perform.

- A checked check box means group members have permission to perform that task. If a checked box is greyed-out, it means you cannot disable the task. For example, Prime Infrastructure does not allow you to remove the "View tags" task for the Monitor Lite user group because it is an integral task for that user group.
- A blank check box means group members cannot perform that task. If a blank check box is greyed out, it means you cannot enable the task for the user group.

The web GUI root and Monitor Lite groups, and the NBI groups, are not editable.

Step 4 If you want to change permissions, you have these choices:

Note Be careful. Selecting and deselecting tasks in the Group Detail window will apply your changes to *all group members*.

- Change permissions for all user group members. See View and Change the Tasks a Group Can Perform, on page 30.
- Add the user to a different user group. The predefined user groups are described in User Groups—Web UI, on page 7 and User Groups—NBI, on page 8. Those topics also describe any group restrictions; for example, if a user belongs to the predefined Monitor Lite user group, the user cannot belong to any other groups.
- Remove the user from this group. See View and Change the Groups a User Belongs To, on page 10.
- Use a customized user group and add the user to that group. To find out which customized groups already exist, see View and Change the Tasks a Group Can Perform, on page 30. To create a new customized group, see Create a Customized User Group, on page 28.

View and Change the Groups a User Belongs To

The tasks users can perform is determined by the user groups they belong to. This is normally configured when a user account is created (see Add and Delete Users, on page 34). User groups are described in Types of User Groups, on page 7.

This procedure explains how to view the groups a user belongs to and, if necessary, change the user's group membership.

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

Step 2 In the **User Name**, column, locate and click the user name hyperlink to open the **User Details** window. All user groups are listed under the General tab.

- A checked check box means the user belongs to that group. If a checked box is greyed-out, it means you cannot remove the user from that group. For example, Prime Infrastructure will not allow you to remove the user named **root** from the root user group.
- A blank check box means the user does not belong to that group. If a blank check box is greyed-out, it means you cannot add the user to that group.

(To check the tasks that a group can perform, choose **User Groups** from the left sidebar menu and click a group name.)

Step 3 To change the groups the user belongs to, select and unselect the appropriate groups in the **User Details** window, then click **Save**.

View User Groups and Their Members

Users can belong to multiple groups, unless they belong to a very restricted group such as Monitoring Lite. This procedure explains how to view existing user groups and their members.

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

The User Groups page lists all existing user groups and a short list of their members. For a description of these groups, see Types of User Groups, on page 7.

Step 2 To view all members of a group, click a group hyperlink to open the **Group Details** window, then click the **Members** tab.

Step 3 If you want to make changes to these groups, see:

- View and Change the Tasks a Group Can Perform, on page 30
- View and Change the Groups a User Belongs To, on page 10

User Group Permissions and Task Description

The following table describes user group permissions and task descriptions.

Table 1: User Group Permissions and Task Description

Task Group Name	Task Name	Description
APIC-EM Controller	Apic Controller Read Access	Allows user to read APIC-EM controller details.
	Apic Controller Write Access	Allows user to create or update APIC-EM controller details.
	Apic Global PnP Read Access	Allows user to read the Apic Global PnP/Ztd settings.
	Apic Global PnP Write Access	Allows user to create or update the Apic Global PnP/Ztd settings.
Active Sessions	Force Logout Access	Allows user to force logout other user active sessions.

Task Group Name	Task Name	Description
Administrative Operations	Appliance	Gives the user access to the **Administration > Settings > Appliance** menu.
	Application Server Management Access	Allows user to manage NAM server lists.
	Application and Services Access	Allows user to create, modify, and delete custom applications and services.
	Data Migration	
	Design Endpoint Site Association Access	Allows user to create Assurance site classification rules.
	Device Detail UDF	Allows user to access Device details UDF.
	Export Audit Logs Access	Allows user to access Import Policy Update through Admin Mega menu.
	Health Monitor Details	Allows user to modify Site Health Score definitions.
	High Availability Configuration	Allows user to configure High Availability for pairing primary and secondary servers.
	Import Policy Update	Allow user to manually download and import the policy updates into the compliance and Audit manager engine.
	License Center/Smart License	Allows user to access license center/smart license..
	Logging	Gives access to the menu item which allows user to configure the logging levels for the product.
	Scheduled Tasks and Data Collection	Controls access to the screen to view the background tasks.
	System Settings	Controls access to the **Administration > System Settings** menu.
	Tools	Allows user to access the **Administration > System Settings** menu.

Task Group Name	Task Name	Description
	User Preferences	Controls access to the **Administration > User Preference** menu.
	View Audit Logs Access	Allows user to view Network and System audits.
Alerts and Events	Ack and Unack Alerts	Allows user to acknowledge or unacknowledge existing alarms.
	Alarm Policies	Allows user to access alarm policies.
	Alarm Policies Edit Access	Allows user to edit alarm policies.
	Delete and Clear Alerts	Allows user to clear and delete active alarms.
	Notification Policies Read Access	Allows user to view alarm notification policy.
	Notification Policies Read-Write Access	Allows user to configure alarm notification policy.
	Pick and Unpick Alerts	Allows user to pick and unpick alerts.
	Syslog Policies	Grants access to the Syslog Policies page.
	Syslog Policies Edit Access	Allows creating, modifying and deleting syslog policies.
	Troubleshoot	Allows user to do basic troubleshooting, such as traceroute and ping, on alarms.
	View Alert Condition	Allows user to view alert condition.
	View Alerts and Events	Allows user to view a list of events and alarms.
Configuration Archive	Configuration Archive Read-Only Task	Allows user to view the archived configurations and schedule configuration archive collection jobs.
	Configuration Archive Read-Write Task	Allows user to perform all configuration archive jobs.
Diagnostic Tasks	Diagnostic Information	Controls access to diagnostic page.

Task Group Name	Task Name	Description
Feedback and Support Tasks	Automated Feedback	Allows acess to automatic feedback.
	TAC Case Management Tool	Allows user to open a TAC case.
Global Variable Configuration	Global Variable Access	Allows user to access global variables.
Groups Management	Add Group Members	Allows user to add an entity, such as a device or port, to groups.
	Add Groups	Allows user to create groups.
	Delete Group Members	Allows user to remove members from groups.
	Delete Groups	Allows user to delete groups.
	Export Groups	Allows user to export groups.
	Import Groups	Allows user to export groups.
	Modify Groups	Allows user to edit group attributes such as name, parent, and rules.

Task Group Name	Task Name	Description
Job Management	Approve Job	Allows user to submit a job for approval by another user.
	Cancel Job	Allows user to cancel the running jobs.
	Delete Job	Allows user to delete jobs from job dashboard.
	Edit Job	Allows user to edit jobs from job dashboard.
	Pause Job	Allows user to pause running and system jobs.
	Schedule Job	Allows user to schedule jobs.
	View Job	Allows user to schedule jobs.
	Config Deploy Edit Job	Allows user to edit config delployed jobs.
	Device Config Backup Job Edit Access	Allows user to change the external backup settings such as repository and file encrytion password.
	Job Notification Mail	Allows user to configure notification mails for various job types.
	Run Job	Allows user to run paused and scheduled jobs.
	System Jobs Tab Access	Allows user to view the system jobs.
Maps	Client Location	Allows user to view client locations on Map.
	Maps Read Only	Allows user to view the map in a read-only mode.
	Maps Read Write	Allows user to view and also manipulate elements within the maps such as AP placement.
	Planning Mode	Allows user to launch the planning mode tool.
	Rogue Location	Allows user to view rogue AP locations on Map

Task Group Name	Task Name	Description
Mobility Services	Mobility Service Management	Allows user to edit properties and parameters, view session and Trap destinations,manage user and group accoounts,and monitor status information for mobility services engine.
	View CAS Notifications Only	Allows user to view the CAS notifications

Task Group Name	Task Name	Description
Network Configuration	Add Device Access	Allows user to add devices to Prime Infrastructure.
	Admin Templates Write Access	Check thois check-box for enabling admin templates write access for user defind role.
	Auto Provisioning	Allows access to auto provisioning.
	Compliance Audit Fix Access	Allows user to view, schedule and export compliance fix job/ report.
	Compliance Audit PAS Access	Allows user to view, schedule and export "PSIRT" and "EOX" job/ report
	Compliance Audit Policy Access	Allows user to create, modify, delete, import and export compliance policy.
	Compliance Audit Profile Access	Allows user to view, schedule and export compliance audit job or report view and download violations summary.
	Compliance Audit Profile Edit Access	Allows user to create, modify and delete compliance profiles view and schedule export compliance audit job or report view and download violations summary.
	Configuration Templates Read Access	Allows to access configuration templates in read only mode.
	Configure ACS View Servers	Allows acess to manage ACS View Servers.
	Configure Access Points	Allows users to configure access points.
	Configure Autonomous Access Point Templates	Allows access to configure Autonomous AP Templates on Prime Infrastructure.
	Configure Choke Points	Allows users to Configure Choke Points.
	Configure Config Groups	Allows access to Config Groups.
	Configure Controllers	Allows users to configure the Wireless Controller features.

Task Group Name	Task Name	Description
	Configure Ethernet Switch Ports	Controls access to the config ability when viewing ethernet details in DWC for any device.
	Configure Ethernet Switches	Controls access to the config ability when viewing ethernet details in DWC for any device.
	Configure ISE Servers	Allows users to manage ISE servers on Prime Infrastructure
	Configure Lightweight Access Point Templates	Allows users to configure Lightweight Access Point Templates on Prime Infrastructure
	Configure Mobility Devices	Allows user to configure the CAS,WIPS,Mobile concierge service, location analytics service, and provide the mobility procedures
	Configure Spectrum Experts	Allows users to Configure Spectrum Experts.
	Configure Switch Location Configuration Templates	Allow the user to modify Configuration templates
	Configure Templates	Allow the user to do the CRUD operation of Feature Templates on DWC and configuration Template
	Configure Third Party Controllers and Access Point	Allows users to configure Third Party Controllers and Access Points on Prime Infrastructure.
	Configure WIPS Profiles	Allows users to access WIPS Profiles.
	Configure WiFi TDOA Receivers	Allows users to configure WiFi TDOA Receivers.
	Credential Profile Add_Edit Access	Allows user to Add and edit credential profile.
	Credential Profile Delete Access	Allows user to delete credential profile.
	Credential Profile View Access	Allows user to view credential profile.
	Delete Device Access	Allows user to delete devices from Prime Infrastructure.

Task Group Name	Task Name	Description
	Deploy Configuring Access	Allows user to deploy Configuration and IWAN templates.
	Design Configuration Template Access	Allows user to create Configuration > Shared Policy Object templates and Configuration Group templates.
	Device Bulk Import Access	Allows user to perform bulk import of devices from CSV files.
	Device View configuration Access	Allows user to configure devices in the Device Work Center.
	Edit Device Access	Allows user to edit device credentials and other device details.
	Export Device Access	Allows user to export the list of devices, including credentials, as a CSV file.
	Global SSID Groups	Allows users to configure Global SSID Groups.
	Migration Templates	Allows user to create autonomous AP migration templates
	Network Devices	Allows user to access to the Network devices.
	Network Topology Edit	Allows user to create devices, links and network in the topology map, edit the manually created link to assign the interfaces.
	Scheduled Configuration Tasks	Allows user to create and schedule a configuration template,configuration group,software download task and template.
	TrustSec Readiness Assessment	Access to the TrustSec menu which allows users to configure TrustSec in their network.
	View Compute Devices	Access to Data Center compute servers and virtual elements such as Hosts and Virtual Machines managed in Prime Infrastructure.
	WIPS Service	

Task Group Name	Task Name	Description
		Allows users to configure WIPS Service.
	Wireless Security	Allows user to configure Rogue Policy, Rogur Rule and wIPS profile using Wireless Security Configuration wizard.

Task Group Name	Task Name	Description
Network Monitoring	Ack and Unack Security Index Issues	Allows users to Acknowledge or Unacknowledge Security Index Violations.
	Admin Dashboard Access	Allows user to access the Admin Dashboard.
	Config Audit Dashboard	Allows users to access Config Audit Dashboard.
	Data Collection Management Access	Allow user to access the Assurance Data Sources page.
	Details Dashboard Access	Allow user to access the Detail dashboards.
	Disable Clients	Allows users to access Disabled Clients page.
	Identify Unknown Users	Allows users to access Identify Unknown Users page.
	Incidents Alarms Events Access	Allows user to access incidents alarms events.
	Latest Config Audit Report	Allows user to view the latest config audit reports.
	Lync Monitoring Access	Allows the user to access and view the Lync monitoring page
	Monitor Access Points	Allows users to view Monitor Access Points page.
	Monitor Chokepoints	Allows users to access Monitor Chokepoints page.
	Monitor Clients	Allows users to access Monitor Clients page.
	Monitor Ethernet Switches	Allows user to monitor ethernet interfaces,VLAN switch port,and VLAN trunk of ethernet switches.
	Monitor Interferers	Allows users to access Monitor Interferers pages.
	Monitor Media Streams	

Task Group Name	Task Name	Description
		Allows user to monitor the media stream configuration information such as name, start and end address ,maximum bandwidth,operational status,average packet size,RRC updates, priority and violation.
	Monitor Mobility Devices	Allows user to monitor mobility group events such as mobility statistics,mobility responder statistics,mobility initiator statistics.
	Monitor Security	Allows user to monitor controller security information such as RADIUS authentication,RADIUS accounting,management frame protection,Rogue AP rules and guest users.
	Monitor Spectrum Experts	Allows users to monitor spectrum experts.
	Monitor Tags	Allows user to monitor tags.
	Monitor Third Party Controllers and Access Point	Allows users to access Monitor Third Party Controllers and Access Point pages.
	Monitor WiFi TDOA Receivers	Allows users to access Monitor WiFi TDOA Receivers pages.
	Monitoring Policies	Allows user to identify the most used rules, troubleshoot a specific rule, and verify hits for the selected rule.
	Network Topology	Allows users to launch the Network Topology map and view the devices and links in the map.
	Packet Capture Access	Allow user to initiate packet captures on NAM and supported routers.
	Performance Dashboard Access	Allow user to access the Performance dashboard.
	PfR Monitoring Access	Allows the user to access and view the PfR Monitoring page
	RRM Dashboard	Allows users to access RRM Dashboard page.

Task Group Name	Task Name	Description
	Remove Clients	Allows users to access Remove Clients page.
	Service Health Access	Allows the user to access and view the Service Health page.
	Site Visibility Access	Allows user to access site visibility.
	Track Clients	Allows users to access Track Clients page.
	View Security Index Issues	Allows users to access Security Index Issues page.
	Voice Diagnostics	Allows users to access Voice Diagnostics information.
	Wireless Dashboard Access	Allows user to view the wireless dashboard.
Operations Center Tasks	Administrative privileges under Manage and Monitor Servers page	Allows for administrative tasks such as Add/Delete/Edit/Activate and deactivate of servers under M&M page.
	Allow report/dashlet use for users with only NBI Read access	Enable this option for users with NBI Read access so they can generate reports and populate all dashlets.
	Manage and Monitor Servers Page Access	Allows access to the Manage & Monitor Servers Page.

Task Group Name	Task Name	Description
Plug n Play Configuration	PnP Deploy History Read Access	Allows user to read provisioned devices status.
	PnP Deploy History Read-Write Access	Allows user to read and delete operations on provisioned devices.
	PnP Preferences Read Access	Allows user to view Plug and Play preferences.
	PnP Preferences Read-Write Access	Allows user to edit Plug and Play preferences.
	PnP Profile Deploy Read Access	Allows user to view Plug and Play provisioning profiles.
	PnP Profile Deploy Read-Write Access	Allow user to create, modify, and delete Plug and Play provisioning profiles.
	PnP Profile Read Access	Allow user to view Plug and Play profiles.
	PnP Profile Read-Write Access	Allow user to create, delete, and modify Plug and Play profiles.
	WorkflowsReadWriteAccess	Allows user to set up configure the cisco IOS switches and access devices
Product Usage	Product Feedback	Allows the user to access the Help Us Improve page.

Task Group Name	Task Name	Description
Reports	Autonomous AP Reports	Allows user to create new Autonomous AP Reports.
	Autonomous AP Reports Read Only	Allows user to view Autonomous AP Reports
	CleanAir Reports	Allows user to create new CleanAir Reports.
	CleanAir Reports Read Only	Allows user to view CleanAir Reports
	Client Reports	Allow user to create Client Reports
	Client Reports Read Only	Allow user to view Client Reports.
	Compliance Reports	Allows user to customize the configuration audit ,network discrepancy,PCI DSS detailed and PCI DSS summary reports,PSIRT detailed and PSIRT summary reports.
	Compliance Reports Read Only	Allows user to configuration audit,network discrepancy,PCI DSS detailed and PCI DSS summary reports,PSIRT detailed and PSIRT summary reports.
	Context Aware Reports	Allows user to run context aware/location-specific reports.
	Context Aware Reports Read Only	Allows user to run context aware/location-specific reports.
	Custom Composite Report	Allow user to create 'custom' report with two or more (upto 5 reports) existing report templates into a single report.
	Custom NetFlow Reports	Allow user to access custom NetFlow reports
	Custom NetFlow Reports Read Only	Allow user to view custom NetFlow reports.
	Device Reports	Allow user to run reports specific to monitoring specific report related to Devices.
	Device Reports Read Only	Allows user to read generated device reports

Task Group Name	Task Name	Description
	Guest Reports	Allow user to create Guest Reports
	Guest Reports Read Only	Allow user to view Guest Reports.
	MSAP Reports	Allows user to run Mobile Concierge reports.
	MSAP Reports Read Only	Allows user to run Mobile Concierge reports.
	Mesh Reports	Allow user to create Mesh Reports.
	Mesh Reports Read Only	Allow user to view Mesh Reports.
	Network Summary Reports	Allows user to create and run network summary reports
	Network Summary Reports Read Only	Allows user to view all Summary reports.
	Performance Reports	Allows user to create performance reports.
	Performance Reports Read Only	Allows user to view performance reports.
	Raw NetFlow Reports	Allows user to view NetFlow reports.
	Raw NetFlow Reports Read Only	Allows user to view Raw NetFlow reports.
	Report Launch Pad	Allows user to access the Report page.
	Report Run History	Allows user to view report history.
	Run Reports List	Allows user to run reports.
	Saved Reports List	Allows user to save reports.
	Saved Reports List Read Only	Allows user to view saved reports.
	Security Reports	Allows user to create Security Reports.
	Security Reports Read Only	Allows users to view wireless security reports related to rogue APs, wIPS etc.
	Virtual Domains List	Allows user to create the Virtual Domain related report.
	Voice Audit Report	

Task Group Name	Task Name	Description
		Allows user to create the Virtual Domain related report
Software Image Management	Add Software Image Management Servers	Allows user to add software imagemanagement servers.
	Software Image Access Privilege	Allows user to access Inventory > Software Images.
	Software Image Activation	Allows user to upgrade and downgrade software versionss to manage devices in their network.
	Software Image Collection	Allows user to collect images from different locations such as from devics, Cisco.com or from URLs.
	Software Image Delete	Allows user to delete an image from the Software Images page, except for images that are included in Plug and Play profiles.
	Software Image Details View	Allows user to view the image details.
	Software Image Distribution	Allows user to distribute software verisons to managed devices in the network.
	Software Image Info Update	Allows the user to edit and save image properties such as minimum RAM, minimum FLASH and minimum boot ROM version.
	Software Image Management Server-Manage Protocols	Allows user to manage protocol
	Software Image Preference Save	Allows user to save preference options on Software Images page.
	Software Image Recommendation	Allows user to recommend images from Cisco.com and from the local repository.
	Software Image Upgrade Analysis	Allows user to analyze software images to determine if the hardware upgrades (boot ROM, flash memory, RAM, and boot flash, if applicable) are required before performing a software upgrade.

Task Group Name	Task Name	Description
User Administration	Audit Trails	Allows user to access the Audit trails on user login and logout.
	RADIUS Servers	Allows user to access the RADIUS Servers menu.
	SSO Server AAA Mode	Allows user to access the AAA menu
	SSO Servers	Allows user to access the SSO menu
	TACACS+ Servers	Allows user to access the TACACS+ Servers menu
	Users and Groups	Allows user to access the Users and Groups menu.
	Virtual Domain Management	Allows user to access the Virtual Domain Management menu.
	Virtual Elements Tab Access	When creating virtual domain or adding members to a virtual domain, allows uses to access the virtual elements tab, so as to allow user to add virtual elements (Datacenters, Clusters and Hosts) to virtual domain.
View Online Help	OnlineHelp	Allows user to access the Prime Infrastructure online help.

Create a Customized User Group

Prime Infrastructure provides a set of predefined user groups that help you control user authorization. These groups are described in Types of User Groups, on page 7 and include four User Defined groups which you can customize to create a user group that is specific to your deployment. The following procedure explains how to create a customized group using one of the four predefined User Defined group templates.

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

Step 2 Locate a User Defined group that has no members, then click its group name hyperlink.

Step 3 Customize the group permissions by checking and unchecking tasks in the **Group Detail** window. If a task is greyed-out, it means you cannot adjust its setting. You cannot change the group name.

Step 4 Click **Save** to save your group settings.

Step 5 If you want to add a new User Defined group Click **Add Groups**. Enter the Group Name, select the required task permissions and click **Save**.

Step 6 If you want to delete any User defined group select the group and click **Delete Groups**. A warning message appears to check whether you want to delete the group. Click **Ok** .

Note You can not delete any predefined groups and groups associated to any user.

Step 7 Add members to your group by editing the relevant user accounts and adding the user to your new group. See Add and Delete Users, on page 34 for information on adjusting user accounts.

Add User with Wireless Persona

You can add a local user with wireless persona so that the user can view only wireless related navigation menu items.

Note You cannot add AAA user or remote user with wireless persona.

Step 1 Log in to Cisco Prime Infrastructure as an administrator.

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

Step 3 From the **Select a command** drop-down list, choose **Add User**, then click **Go**.

Step 4 Configure the user account.

a) Enter a username and password.

b) Control the actions the user can perform by selecting one or more user groups. For descriptions of user groups, see View User Groups and Their Members, on page 10.

c) Control the devices a user can access by clicking the **Virtual Domains** tab and assigning domains to the user. For more information, see Create Virtual Domains to Control User Access to Devices, on page 45.

Step 5 In the **Persona** pane, check the **Wireless** check box. Hover your mouse cursor over the help text question mark to view the menu items that are removed from the navigation.

Step 6 Click **Save**.

Note The following user groups do not support the wireless persona-based menu:

1. Root
2. Lobby Ambassador
3. Lobby Ambassador + NBI Credential
4. Lobby Ambassador + NBI Read
5. Lobby Ambassador + NBI Write
6. Lobby Ambassador + (NBI Credential + NBI Read)
7. Lobby Ambassador + (NBI Read + NBI Write)
8. Lobby Ambassador + (NBI Credential + NBI Write)
9. Lobby Ambassador + (NBI Credential + NBI Read +NBI Write)
10. Help Desk Admin
11. Help Desk Admin + NBI Credential
12. Help Desk Admin + NBI Read
13. Help Desk Admin + NBI Writer
14. Help Desk Admin + (NBI Credential + NBI Read)
15. Help Desk Admin + (NBI Read + NBI Write)
16. Help Desk Admin + (NBI Credential + NBI Write)
17. Help Desk Admin + (NBI Credential + NBI Read +NBI Write)
18. mDNS Policy Admin

View and Change the Tasks a Group Can Perform

Follow these steps to get information about existing user groups and the tasks group members can perform. The predefined user groups are described in View User Groups and Their Members, on page 10.

Note If you want to change *device* access, see Assign Virtual Domains to Users, on page 51.

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

The User Groups page lists all existing user groups.

Step 2 Click a user group hyperlink. The **Group Detail** window lists the group permissions.

- A checked task means group members have permission to perform that task. If a checked box is greyed-out, it means you cannot disable the task.
- A blank check box means group members cannot perform that task. If a blank check box is greyed out, it means you cannot enable the task for the user group.

The web GUI root and Monitor Lite groups, and the NBI groups, are not editable.

Step 3 If you want to change the group permissions—which will affect *all group members*—check and uncheck tasks, then click **Save**.

Note Selecting and deselecting the tasks will affect only that group and not all groups.

Use Prime Infrastructure User Groups with RADIUS and TACACS+

Your RADIUS or TACACS+ servers must be configured to recognize the user groups that exist in Prime Infrastructure. You can do this using the procedure in Export the Prime Infrastructure User Group and Role Attributes for RADIUS and TACACS+, on page 31.

Note From Prime Infrastructure Release 3.2, Role based based TACACS+ authentication is enabled by default, so it is sufficient to add user roles and virtual domains alone. Tasks will be retrieved from Prime Infrastructure based on the roles given in the ISE/ACS profile.

If you want to use the task based TACACS authentication, you must set the value of the tacsacsServerTaskPref property in the file /opt/CSCOlumos/conf/usermgmt.properties to true and click **Save** in **Administration > Users > Users, Roles & AAA > AAA Mode Settings** Page . When you are copying the custom attributes (role, task and virtual domain) of users belonging to multiple user groups from the **Administration > Users > Users, Roles & AAA > User Groups** page in Prime Infrastructure, and pasting them in ACS, make sure that the custom attributes remain unique in order to avoid duplicate attributes. Also ensure that you paste the currently supported tasks in the ACS and add the Home Menu Access task. It is mandatory.

Export the Prime Infrastructure User Group and Role Attributes for RADIUS and TACACS+

If you are using RADIUS or TACACS+, you must copy all Prime Infrastructure user group and role information into your Cisco Access Control Server (ACS) or Cisco Identity Services Engine (ISE) server. You can do this using the Task List dialog box provided in the Prime Infrastructure web GUI. If you do not export the data into your Cisco ACS or Cisco ISE server, Prime Infrastructure will not allow users to perform their assigned tasks.

The following information must be exported:

- TACACS+—Requires virtual domain and role information (tasks are automatically added).
- RADIUS—Requires virtual domain and role information (tasks are automatically added).

Information in the Task List dialog is preformatted for use with the Cisco ACS server.

Note When you add tasks to the external server, be sure to add the **Home Menu Access** task. It is mandatory for all users.

Before you begin

Make sure you have added the AAA server and configured the AAA mode as explained in Configure External Authentication, on page 54.

Step 1 In Prime Infrastructure:

a) Choose **Administration** > **Users** > **User Groups**.

b) From the User Groups table, copy the role for each user group by clicking the **Task List** hyperlink (at the end of a user group row).

- If you are using RADIUS, right-click the *role0 line* in the RADIUS Custom Attributes field and choose **Copy**.
- If you are using TACACS+, right-click the *role0 line* in the TACACS+ Custom Attributes field and choose **Copy**.

Step 2 Paste the information into your Cisco ACS or Cisco ISE server. These steps show how to add the information to an existing user group in Cisco ACS. If you have not yet added this information to Cisco ACS or Cisco ISE, see:

- Use Cisco ACS With RADIUS or TACACS+ for External Authentication, on page 62
- Use Cisco ISE With RADIUS or TACACS+ for External Authentication , on page 56

a) Navigate to **User or Group Setup**.

b) For the applicable user or group, click **Edit Settings**.

c) Paste the attributes list into the appropriate text box.

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

Add Users and Manage User Accounts

Change User Group Memberships

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

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

Prime Infrastructure will not permit certain combinations of user group membership. For example, a user cannot be a member of the "Root" and "Lobby Ambassador" user groups at the same time (for details, see

the table in “Control the Tasks Users Can Perform (User Groups) ”, in Related Topics). If you are using RADIUS to authenticate Prime Infrastructure users, make sure that you do not insert invalid user-group membership combinations into the RADIUS user attribute/value pairs.

Step 1 Log in to Prime Infrastructure as an administrator.

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

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

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

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

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

Related Topics

Control the Tasks Web Interface Users Can Perform (User Groups), on page 7
View and Change the Tasks a Group Can Perform, on page 30
Create Virtual Domains to Control User Access to Devices, on page 45

Create Web GUI Users with Administrator Privileges

After installation, Prime Infrastructure has a web GUI root account named **root**. This account is used for first-time login to the server to create:

- Web GUI users with Administrator privileges who will manage the product and features
- All other user accounts

You should *not* use the web GUI root account for normal operations. For security purposes, create a new web GUI user with Administrator privileges (and access to all devices), and then disable the web GUI root account.

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

Step 2 Click **Add User**.

Step 3 Enter the username in the **Username** text box.

(Optional) Click the **Generate New Password** button to set a secured system-generated password. On clicking this button, a new password will be displayed in the adjacent text box. The same is also displayed in the **New Password** and **Confirm Password** text boxes. Click the eye icon in the text box to view or hide the password. You can also copy the password to clipboard by clicking the **Copy** button.

Click the Reset button to clear the values in the text box.

Step 4 Enter a password. The new password must satisfy the conditions specified in the password policy. Click the ? icon to view the password policy.

Step 5 In the **General** tab under **Groups Assigned to This User**, click **Admin**.

Step 6 Click the **Virtual Domains** tab to specify which devices the user can access. You should have at least one Admin web GUI user that has access to all devices (ROOT-DOMAIN). For more information on virtual domains, see Create Virtual Domains to Control User Access to Devices, on page 45.

Step 7 Click **Save**.

What to do next

If you have not done so already, for security purposes, disable the web GUI root account as described in Disable and Enable the Web GUI root User, on page 6.

Add and Delete Users

Before you create user accounts, create virtual domains to control device access so you can apply them during account creation. Otherwise you will have to edit the user account to add the domain access. See Create Virtual Domains to Control User Access to Devices, on page 45.

If you want to temporarily disable an account (rather than delete it), see Disable (Lock) a User Account, on page 34.

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

Step 2 Click **Add User**.

Step 3 Configure the user account.

a) Enter a username and password.
b) Enter the first name, last name, and a description for the user.
c) Control the actions the user can perform by selecting one or more user groups. For descriptions of user groups, see View User Groups and Their Members, on page 10.
d) Control the devices a user can access by clicking the **Virtual Domains** tab and assigning domains to the user. (see Create Virtual Domains to Control User Access to Devices, on page 45).

Step 4 Click **Save**.

Step 5 To delete a user account, select a user, . Click **Delete User**.

When you are deleting a stale local user, a popup window opens. Do one of the following:

- Click **Delete/Pause Job(s)**, if you want to delete or pause the jobs associated with the deleted user. The jobs will be displayed in the same page. Select the job(s), click **Pause Job(s)** or **Delete Job(s)** and click **Proceed**.
- Click **Skip** in the popup, if you want to delete the user without deleting or pausing the associated job(s).
- Click **Cancel**, if you do not want to delete the user.

Disable (Lock) a User Account

Disable a user account when you temporarily want to disallow a user from logging in to the Prime Infrastructure GUI. You might want to do this if a user is temporarily changing job functions. If the user tries to log in, Prime Infrastructure displays a message saying the login failed because the account is locked. You can unlock the account later without having to re-create the user. If you want to delete a user account, see Add and Delete Users, on page 34.

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 Change a User's Password, on page 35 and Configure Global Password Policies for Local Authentication, on page 43.

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

Step 2 Select the user whose access you want to disable or enable.

Step 3 From the **Select a command** drop-down list, select **Lock User(s)** (or **Unlock User(s)**), then click **Go**.

Change a User's Password

You can force users to change their passwords on a regular basis using password rules (see Configure Global Password Policies for Local Authentication, on page 43). Users can change their own passwords . If you need to make an immediate change to a user's password, use this procedure.

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

Step 2 Click the username hyperlink.

Step 3 Enter the new password in the password fields, then click **Save**.

Configure Guest Account Settings

Prime Infrastructure administrators can choose to:

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

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

Step 1 Log in to Prime Infrastructure as an administrator.

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

Step 3 Change radio button selections as follows:

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

Step 4 Click **Save**.

Related Topics

Use Lobby Ambassadors to Manage Guest User Accounts, on page 36
Control the Tasks Web Interface Users Can Perform (User Groups), on page 7
Create Virtual Domains to Control User Access to Devices, on page 45

Use Lobby Ambassadors to Manage Guest User Accounts

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

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

Prime Infrastructure permits both wired and wireless guest user access. Wired guest access enables guest users to connect to the guest access network from a wired Ethernet connection designated and configured for guest access. Wired guest access ports may be available via a guest office or through specific ports in a conference room. Like wireless guest user accounts, wired guest access ports are added to the network using the lobby ambassador feature.

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

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

Related Topics

Manage Guest User Accounts: Workflows, on page 36
Save Guest Accounts on a Device, on page 39
Edit Guest User Credentials, on page 40

Manage Guest User Accounts: Workflows

Lobby ambassadors can manage guest user accounts following this workflow

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

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

1. Create lobby ambassador accounts—While logged in as a Prime Infrastructure administrator, create lobby ambassador accounts as needed.

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

Create Lobby Ambassador Accounts, on page 37
Create Guest User Accounts as a Lobby Ambassador, on page 38
Schedule Guest User Accounts, on page 38
Print or Email Guest User Details, on page 38
View Lobby Ambassador Activities, on page 39

Create Lobby Ambassador Accounts

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

Step 1 Log in to Prime Infrastructure as an administrator.

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

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

Step 4 Complete the required fields as follows:

a) In the *Groups Assigned to this User* section, select the **Lobby Ambassador** check box to access the Lobby Ambassador Defaults tab.
b) Complete the required fields on the Lobby Ambassador Defaults tab.
c) Click the Virtual Domains tab to assign a virtual domain for this lobby ambassador account.
d) In the **Available Virtual Domains** list, click to highlight the virtual domain you want this user to access. Then click Add to add it to the Selected Virtual Domains list.

Step 5 Click **Save**.

Related Topics

Manage Guest User Accounts: Workflows, on page 36
Save Guest Accounts on a Device, on page 39
Edit Guest User Credentials, on page 40

Login as a Lobby Ambassador

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

Related Topics

Manage Guest User Accounts: Workflows, on page 36
Save Guest Accounts on a Device, on page 39
Edit Guest User Credentials, on page 40

Create Guest User Accounts as a Lobby Ambassador

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

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

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

See reference guide for field descriptions.

Step 4 Click **Save**.

Related Topics

Manage Guest User Accounts: Workflows, on page 36
Save Guest Accounts on a Device, on page 39
Edit Guest User Credentials, on page 40

Schedule Guest User Accounts

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

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

Step 3 **Configure the required** parameters:

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

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

Step 4 Click **Save**.

Related Topics

Manage Guest User Accounts: Workflows, on page 36
Save Guest Accounts on a Device, on page 39
Edit Guest User Credentials, on page 40

Print or Email Guest User Details

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

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

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

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

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

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

Related Topics

Manage Guest User Accounts: Workflows, on page 36
Save Guest Accounts on a Device, on page 39
Edit Guest User Credentials, on page 40

View Lobby Ambassador Activities

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

Step 1 Log into Prime Infrastructure as an administrator.

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

Step 3 Click the **Audit Trail** icon for the lobby ambassador account you want to view. The Audit Trail page for the lobby ambassador appears. This page enables you to view a list of lobby ambassador activities over time.

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

Related Topics

Manage Guest User Accounts: Workflows, on page 36
Save Guest Accounts on a Device, on page 39
Edit Guest User Credentials, on page 40

Save Guest Accounts on a Device

Step 1 Log into Prime Infrastructure as a lobby ambassador.

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

Related Topics

Manage Guest User Accounts: Workflows, on page 36
Edit Guest User Credentials, on page 40

Edit Guest User Credentials

Step 1 Log in to Prime Infrastructure as an administrator.

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

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

Step 4 Modify the required credentials.

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

Step 5 Click Save.

Related Topics

Manage Guest User Accounts: Workflows, on page 36
Save Guest Accounts on a Device, on page 39

Find Out Which Users Are Currently Logged In

Use this procedure to find out who is currently logged into the Prime Infrastructure server. You can also view a historical list of the actions performed by the user in the current web GUI session and past sessions.

Step 1 Choose **Administration** > **Users** > **Users, Roles & AAA**, then choose **Active Sessions**. Prime Infrastructure lists all users that are currently logged in to the Prime Infrastructure server, including their client machine IP address. If the user performed any actions on managed devices (for example, the user added new devices to Prime Infrastructure), the device IP addresses are listed in the Device IP Address column.

Step 2 To view a historical list of all actions performed by this user, click the Audit Trail icon that corresponds to the user name.

Step 3 If you do not want any particular user to be logged in, select the user and click **Force Log Out** in the upper rigt corner.

Note Force Log Out is not applicable for SSO users.

View the Tasks Performed By Users (Audit Trail)

Prime Infrastructure maintains a history of all actions performed by users in active and past web GUI sessions. Follow these steps to view a historical list of tasks performed by a specific *user* or by all members of a specific *user group*. The audit information includes a description of the task, the IP address of the client from which

the user performed the task, and the time at which the task was performed. If a task affects a managed device (for example, a user adds a new device), the affected device's IP address is listed in the Device IP Address column. If a change is made to multiple devices (for example, a user deploys a configuration template to 10 switches), Prime Infrastructure displays an audit entry for each switch.

To find out which users are currently logged into the Prime Infrastructure web GUI, see Find Out Which Users Are Currently Logged In, on page 40.

To view audits that are not user-specific, see these topics:

- Audit Actions Executed from the GUI (System Audit)
- Audit Configuration Archive and Software Image Management Changes (Change Audit Dashboard)
- Audit Changes Made By Users (Change Audit)

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

Step 2 To view the tasks performed by a specific user:

a. Choose **Users**.

b. Locate the user name, then click the Audit Trail icon corresponding to that user.

Step 3 To view a historical list of the tasks performed by all members of a user group:

a. Choose **User Groups**.

b. Locate the user group name, then click the Audit Trail icon corresponding to that group.

Configure Job Approvers and Approve Jobs

Use job approval when you want to control jobs that could significantly impact the network. If a job requires approval, Prime Infrastructure sends an e-mail to the users configured as job approvers and does not run the job until one of them approves it. If a job is rejected by an approver, the job is removed from the database. By default, all jobs do not require approval.

If job approval is already enabled and you want to view jobs that need approval, approve a job, or reject a job, choose **Administration** > **Dashboards** > **Job Dashboard**, then click the **Job Approval** link.

Selecting the check box against a job name enables the **Approve** and **Reject** buttons. This page displays information such as, **Job Name**, **Job Type**, **Creation Time**, **Created By**, **Approved By**, and **Status**. You can also view the devices that are scheduled for a particular job by clicking the **>** icon besides a job name. This displays information such as, **Device IP**, **Device Name**, and **Configuration** in a tabular format. You can filter the devices to be deployed based on the device IP and device name attributes by selecting either quick filter or advanced filter options. You can also view the following information by the clicking the **i** icon.

- For a rollback job, it displays the running configuration and start-up configuration details.
- For an overwrite job, it explains the operation to be performed.

The **Discovery** and **Config Archive** options are removed from the **Job Approval** page from Cisco Prime Infrastructure 3.2. If you have chosen the **Discovery** and **Config Archive** options in the previous versions of Cisco Prime Infrastructure, the options will be available in higher versions of Cisco Prime Infrastructure, until you deselect them.

Note Job approval is applicable only for scheduled jobs. When immediate jobs are triggered, the job will be expired on approval.

To enable job approval and configure the jobs that require approval before running:

Step 1 Choose **Administration** > **Settings** > **System Settings**, then choose **General** > **Job Approval**.

Step 2 Check the **Enable Job Approval** check box.

Step 3 Find the jobs you want to configure for approval, and move them from the left field to the right field.

Step 4 Check the **Enable Mail for Job Approval** check box. By default this checkbox is unchecked.

Step 5 Enter the email addresses of the job approvers. By default the email address configured in the **Mail Server Configuration** settings or the pre-configured email addresses will appear in the **Approve Email ID** textbox.

Step 6 Click **Save**.

Configure Job Notification Mail for User Jobs

You can configure Cisco Prime Infrastructure to send job notification mail for every user job if the **Last_Run_Status** shows: **Failure**, **Partial Success**, and **Success**. Use this procedure to configure the job notification mail settings for user jobs.

Step 1 Select **Administration** > **Settings** > **System Settings**, then choose **Mail and Notification** > **Job Notification Mail**.

Step 2 Check the **Enable Job Notification Mail** check box to enable notifications.

Step 3 Enter the email addresses in the **To** text box. By default, the email address configured in the **Mail Server Configuration** settings or the pre-configured email addresses appear in the **To** text box. You can configure an email server by performing the steps explained in Configure Email Server Settings

Step 4 Enter the subject of the job notification mail in the **Subject** text box. The subject is automatically appended by the job name.

Step 5 Select the **Job Status**. You can select either Success, Partial Success, or Failure status options or both the options and provide the recipient address.

Step 6 Select the **Compliance Audit Job** and **Compliance Fix Job** check boxes. The job notification mails are triggered for the selected jobs.

Step 7 Click **Save**. The job notification mail is triggered only for the job status that you select and is sent only after the job completion. You will not receive a job notification mail if the file size exceeds the size specified in the configured mail server.

Configure Global Password Policies for Local Authentication

If you are using local authentication (Prime Infrastructure's authentication mechanism), you control the global password policies from the web GUI. If you are authenticating Prime Infrastructure users using external authentication, the policies are controlled by an external application (see Set Up External AAA Via CLI).

By default, users are not forced to change passwords after any period of time. To enforce password changes and configure other password rules, choose **Administration** > **Users** > **Users, Roles & AAA**, then choose **Local Password Policy**.

Configure the Global Timeout for Idle Users

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

- User Idle Timeout—You can disable or configure this setting, which ends your user session automatically when you exceed the timeout. It is enabled by default and is set to 10 minutes.
- Global Idle Timeout—The Global Idle Timeout setting overrides the User Idle Timeout setting. The Global Idle Timeout is enabled by default and is set to 10 minutes. Only users with administrative privileges can disable the Global Idle Timeout setting or change its time limit.

By default, client sessions are disabled and users are automatically logged out after 15 minutes of inactivity. This is a global setting that applies to all users. For security purposes, you should not disable this mechanism, but you can adjust the timeout value using the following procedure. To disable/change the timeout for an idle user, see Disable Idle User Timeout, on page 44

Step 1 Choose **Administration** > **Settings** > **System Settings**, then choose **General** > **Server**.

Step 2 In the **Global Idle Timeout** area, make sure the **Logout all idle users** check box is selected (this means the mechanism is enabled).

Step 3 Configure the timeout by choosing a value from the **Logout all idle users after** drop-down list.

Step 4 Click **Save**. You will need to log out and log back in for this change to take effect.

What to do next

Irrespective of the customer disabling the "Logout all idle users" in system settings and / Or disabling the "Logout idle user" in the Root user my preference setting, the session will ultimately be timed out once the web-server's session time out is reached. This is essentially to maintain the security posture. For more guidelines on increasing/decreasing the session time out, see https://owasp.org/www-community/Session_Timeout.

Note Session will be timed out only if it is inactive whereas active user sessions are not timed out.

Disable Idle User Timeout

By default, client sessions are disabled and users are automatically logged out after certain period of inactivity. This is a global setting that applies to all users. To avoid being logged out during the installation, it is recommended to disable automatic logout of idle users in the system settings using the following procedure.

Note The Global Idle Timeout setting overrides the User Idle Timeout setting. To configure Global Idle Timeout settings, see *CiscoPrime Infrastructure Administrator Guide*.

Irrespective of the customer disabling the "Logout all idle users" in system settings and / Or disabling the "Logout idle user" in the Root user my preference setting, the session will ultimately be timed out once the web-server's session time out is reached. This is essentially to maintain the security posture. For more guidelines on increasing/decreasing the session time out, see https://owasp.org/www-community/Session_Timeout

Note Session will be timed out only if it is inactive whereas active user sessions are not timed

Step 1 Choose **Administration** > **Settings** > **System Settings**, then choose **General** > **Server**.

Step 2 In the **Global Idle Timeout** area, uncheck the **Logout all idle users** check box and click **Save**.

Step 3 Click ⚙ at the top right of web GUI window and choose **My Preferences**.

Step 4 In the **User Idle Timeout** area, uncheck the **Logout idle user** check box and click **Save**.

If you need to change the idle timeout value, then select **Logout idle user** check box and from the **Logout idle user after** drop-down list, choose one of the idle timeout limits. (But this cannot exceed the value set in the Global Idle Timeout settings.)

Step 5 Click **Save**. You will need to log out and log back in for this change to take effect.

Set Up the Maximum Sessions per User

Use this procedure to configure the maximum sessions per user using the web GUI.

Step 1 Choose **Administration** > **Settings** > **System Settings** > **General** > **Server**.

Step 2 To set the maximum sessions per user, enter the value in the **Max Sessions** text box. You can enter any value from 1 to 50 and the default value is 5.

Step 3 When you are finished, click **Save**.

Step 4 Restart the Cisco Prime Infrastructure server to apply the changes.

Note The session limit is applicable only for Local, RADIUS, and TACACS+ servers. The session limit is not applicable for HA and SSO modes.

Create Virtual Domains to Control User Access to Devices

What Are Virtual Domains?

Virtual domains are logical groupings of devices, sites, and other NEs, and are used to control who has access to those NEs. You choose which elements are included in a virtual domain and which users have access to that virtual domain. Virtual domains can be based on physical sites, device types, user communities, or any other designation you choose. All devices belong to ROOT-DOMAIN, which is the parent domain for all new virtual domains.

Virtual domains work in conjunction with user groups. Virtual domains control the devices a user can access, while user groups determine the actions a user can perform on those devices. Users with access to a virtual domain (depending on their privileges) can configure devices, view alarms, and generate reports for the NEs in their virtual domain.

You can create virtual domains after you have added devices to Prime Infrastructure. Each virtual domain 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 email domain-specific reports.

Users work in one virtual domain at a time. Users can change the current virtual domain by choosing a different one from the Virtual Domain drop-down list .

Before you set up virtual domains, determine which users are responsible for managing particular areas of the network. Then organize your virtual domains according to those needs—for example, by geography, by device type, or by the user community served by the network.

How Virtual Domains Affect Prime Infrastructure Features

Virtual domains are organized hierarchically. The ROOT-DOMAIN domain includes all virtual domains.

Because network elements are managed hierarchically, user views of devices—as well as some associated features and components—are affected by the user's virtual domain. The following topics describe the effects of virtual domains on these features.

Reports and Virtual Domains

Reports only include components that belong to the active virtual domain. A parent virtual domain cannot view reports from its child domains. New components are only reflected in reports that are generated after the components were added.

Search and Virtual Domains

Search results only include components that belong to the active domain. You can only view saved search results if you are in the same domain from which the search was performed and saved. When working in a parent domain, you cannot view the results of searches performed in child domains.

Alarms and Virtual Domains

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, if a network element is added to Prime Infrastructure, and that network element generated alarms before and after it was added, its alarm history would only include alarms generated after it was added.

Note For alarm email notifications, only the ROOT-DOMAIN virtual domain can enable Location Notifications, Location Servers, and Prime Infrastructure email notifications.

Maps and Virtual Domains

Maps only display network elements that are members of the active virtual domain.

Configuration Templates and Virtual Domains

When you create or discover a configuration template in a virtual domain, it can only be applied to network elements in that virtual domain. If you apply a template to a device and then add that device to a child domain, the template is also available to the same device in the child domain.

Note If you create a child domain and then apply a configuration 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 and Virtual Domains

A parent domain can view the network elements in a child domain's configuration groups. The parent domain can also edit the child domain's configuration groups.

Email Notifications and Virtual Domains

Email notifications can be configured per virtual domain.

For *alarm* email notifications, only the ROOT-DOMAIN can enable Location Notifications, Location Servers, and email notifications.

Create New Virtual Domains

To create a new virtual domain, use one of the following procedures depending on the desired hierarchy of the virtual domain.

To create a new virtual domain (*new-domain*) here:	**See this procedure:**
ROOT-DOMAIN > ***new-domain***	Create Virtual Domains Directly Under ROOT-DOMAIN, on page 47
ROOT-DOMAIN > *existing-domain* > ***new-domain***	Create Child Virtual Domains (Subdomains), on page 48
ROOT-DOMAIN > *existing-domain* > *existing-domain* > ***new-domain***	
(etc.)	

Create Virtual Domains Directly Under ROOT-DOMAIN

The following procedure creates an empty virtual domain under ROOT-DOMAIN. You can also create multiple virtual domains at one time by using the procedure in Import a List of Virtual Domains, on page 49.

If a virtual domain already exists under ROOT-DOMAIN, and you want to create a new domain under it (a child domain), see Create Child Virtual Domains (Subdomains), on page 48.

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

Step 2 In the Virtual Domains sidebar menu, click the + icon (Add New Domain).

Step 3 Enter a name in the Name text box. This is required.

Step 4 (Optional) Enter the new domain's time zone, email address and description.

Step 5 Click **Submit** to view a summary of the newly-created virtual domain.

What to do next

Add devices to the virtual domain as described in Add Network Devices to Virtual Domains, on page 49.

Create Child Virtual Domains (Subdomains)

The following procedure creates a child virtual domain (also called a subdomain). A child virtual domain is a domain that is *not* directly under ROOT-DOMAIN; it is under a domain that is under ROOT-DOMAIN.

Do not use this procedure if you want the new virtual domain to appear directly under ROOT- DOMAIN. In that case, see Create Virtual Domains Directly Under ROOT-DOMAIN, on page 47.

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

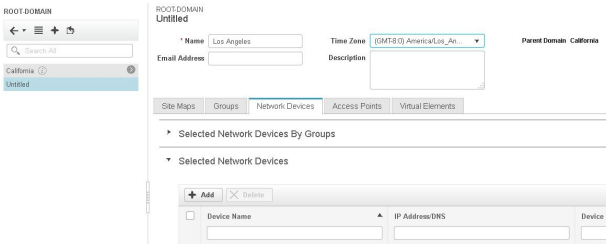
Step 2 In the Virtual Domains sidebar menu:

a) Locate the domain under which you want to create a new child domain. (This is called the parent domain.) In this example, the parent domain is **California**.

b) Click the information (**i**) icon next to the domain name. This opens a data popup window.

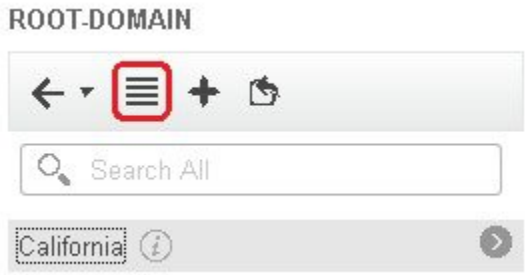
c) In the popup window, click **Create Sub Domain**. The navigation pane switches to the list view, with the parent domain **California** displayed above **Untitled**.

Step 3 Enter a name in the Name text box. This is required. In this example, the new child domain is named **Los Angeles**. (The name in the navigation pane will not change from **Untitled** to **Los Angeles** until you save the new child domain.)

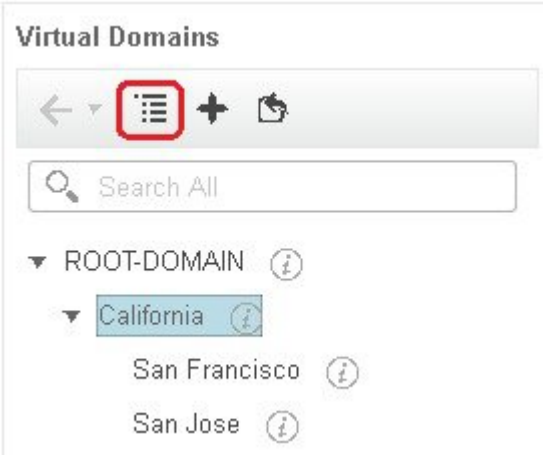


Step 4 (Optional) Enter the new domain's time zone, email address and description.

Step 5 Click **Submit** and confirm the creation of the new child domain. To revert back to the hierarchical view, click the view toggle button at the top of the navigation pane.



The view reverts to the hierarchical view.



What to do next

Add devices to the virtual domain as described in Add Network Devices to Virtual Domains, on page 49.

Import a List of 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 a name, description, time zone, and email address for each virtual domain you create, as well as each domain's parent domain. Adding network elements to the virtual domains must be performed separately.

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

Step 2 Click the **Import Domain(s)** icon, download a sample CSV file from the link provided in the popup, and prepare the CSV file.

Step 3 Click **Choose File** and navigate to your CSV file.

Step 4 Click **Import** to import the CSV and create the virtual domains you specified.

What to do next

Add devices to the virtual domains as explained in Add Network Devices to Virtual Domains, on page 49.

Add Network Devices to Virtual Domains

Use this procedure to add network devices to a virtual domain. When you add a new network device to an existing virtual domain, the device becomes immediately accessible to users with access to that domain (users do not have to restart the web GUI).

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

Step 2 From the Virtual Domains sidebar menu, click the virtual domain to which you want to add network devices.

Step 3 Click **Network Devices** tab. You can either add network devices by group or add a network device to a specific location group.

Step 4 To add devices from groups, in the **Selected Network Devices by Group** section, click **Add**, and the **Add Group** pop-up appears, which lists the applicable location and user-defined groups. Select the group to which you need to add the device and click **Select** to add the groups to the Selected Network Devices by Group table. These groups will not have create, read, update and delete privileges.

Step 5 In the **Selected Network Devices** section, click **Add** 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 6 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. These devices will not have create, read, update and delete privileges.

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

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

What to do next

Give users access to the virtual domain as described in Assign Virtual Domains to Users, on page 51.

Add Groups to Virtual Domains

Use this procedure to add device groups to a virtual domain.

Step 1 Log in to Prime Infrastructure as an administrator.

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

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

Step 4 On the **Groups** tab, click **Add** to view the list of available location and user-defined groups.

The **Add Group** window appears.

Step 5 The **Add Group** window lists only those groups that are applicable to you, which can be added to the virtual domains. Select the required group check box under All Locations, and click **Select** to add the devices to the Selected Groups table.

Note If the selected group is a parent group, all of its child groups gets automatically added to the virtual domain.

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

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

These groups added from the **Groups** tab will have create, read, update and delete privileges.

Step 8 Proceed to create Users accounts.

Assign Virtual Domains to Users

Once a virtual domain is assigned to a user account, the user is restricted to viewing and performing operations on the devices in their assigned domain(s).

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. See Use Prime Infrastructure Virtual Domains with RADIUS and TACACS+, on page 52.

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

Step 2 Select the user to whom you want to grant device access.

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

Step 4 Use the **Add** and **Remove** buttons to make your assignment changes, then click **Save**.

Edit a Virtual Domain

To adjust a virtual domain, choose it from the Virtual Domain Hierarchy on the left sidebar menu to view or edit its assigned network devices. You cannot edit any of the settings for ROOT-DOMAIN.

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

Step 2 Click the virtual domain you want to edit in the Virtual Domains sidebar menu.

Step 3 To adjust the name, email address, time zone, or description, enter your changes in the text boxes.

Step 4 To adjust device members:

- To add devices, click **Add** and follow the instructions in Add Network Devices to Virtual Domains, on page 49.
- To delete devices, select the devices using their check boxes, then click **Delete**.

Step 5 Click **Submit**, then check the summary of your changes.

Step 6 Click **Save** to apply and save your edits.

Delete a Virtual Domain

Use this procedure to delete a virtual domain from Prime Infrastructure. This procedure only deletes the virtual domain; it does not delete the network elements from Prime Infrastructure (the network elements will continue to be managed by Prime Infrastructure).

Before you begin

You can only delete a virtual domain if:

- The virtual domain does not contain any network elements and does not have any child domains.

- It is not the only domain a user can access. In other words, if a Prime Infrastructure user has access to *only* that domain, you cannot delete it.
- No users are logged into the domain.

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

Step 2 In the Virtual Domains sidebar menu, click the information (**i**) icon next to the virtual domain name. This opens a data popup window.

Step 3 In the popup window, click **Delete**.

Step 4 Click **OK** to confirm deleting the virtual domain.

Use Prime Infrastructure Virtual Domains with RADIUS and TACACS+

Your RADIUS or TACACS+ servers must be configured to recognize the virtual domains that exist in Prime Infrastructure. You can do this using the procedure in Export the Prime Infrastructure Virtual Domain Attributes for RADIUS and TACACS+, on page 52.

If your RADIUS or TACACS+ server does not have any virtual domain information for a user, the following occurs, depending on the number of virtual domains that are configured in Prime Infrastructure:

- If Prime Infrastructure has only one virtual domain (ROOT-DOMAIN), the user is assigned the ROOT-DOMAIN by default.
- If Prime Infrastructure has multiple virtual domains, the user is prevented from logging in.

Export the Prime Infrastructure Virtual Domain Attributes for RADIUS and TACACS+

If you are using RADIUS or TACACS+, you must copy all Prime Infrastructure virtual domain information into your Cisco ACS or Cisco ISE server. You can do this using the Virtual Domains Custom Attributes dialog box provided in the Prime Infrastructure web GUI. If you do not export the data into your Cisco ACS or Cisco ISE server, Prime Infrastructure will not allow users to log in.

The following information must be exported, depending on the protocol you are using:

- TACACS+—Requires virtual domain, role, and task information.
- RADIUS—Requires virtual domain and role information (tasks are automatically added).

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

Information in the Virtual Domains Custom Attributes dialog is preformatted for use with Cisco ACS server.

Note When you add tasks to the external server, be sure to add the **Home Menu Access** task. It is mandatory for all users.

Before you begin

Make sure you have added the AAA server and configured the AAA mode as explained in Configure External Authentication, on page 54.

Step 1 In Prime Infrastructure:

a) Choose **Administration** > **Users** > **Virtual Domains**.

b) Click **Export Custom Attributes** at the top right of the window. This opens the Virtual Domain Custom Attributes dialog.

c) Copy the attributes list.

- If you are using RADIUS, right-click *all of the text* in the RADIUS Custom Attributes field and choose **Copy**.
- If you are using TACACS+, right-click *all of text* in the TACACS+ Custom Attributes field and choose **Copy**.

Step 2 Paste the information into your Cisco ACS or Cisco ISE server. If you have not yet added this information to Cisco ACS or Cisco ISE, see:

- Use Cisco ACS With RADIUS or TACACS+ for External Authentication, on page 62
- Use Cisco ISE With RADIUS or TACACS+ for External Authentication , on page 56

Configure Local Authentication

Prime Infrastructure uses local authentication by default, which means that user passwords are stored and verified from the Prime Infrastructure database. To check the authentication mode that is being used, choose **Administration** > **Users** > **Users, Roles & AAA**, then choose **AAA Mode Settings**. The selection is displayed on the AAA Mode Settings page. If you are using local authentication, be sure to configure strong password policies. See Configure Global Password Policies for Local Authentication, on page 43.

If you want to use SSO with local authentication, see Use SSO With Local Authentication, on page 53.

For information on external authentication, see Configure External Authentication, on page 54.

Use SSO With Local Authentication

To use SSO with local authentication, you must add the SSO server and then configure Prime Infrastructure to use SSO in local mode.

Prime Infrastructure does not support localization on the SSO sign-in page.

The following topics describe how to configure SSO for external authentication, but you can use the same procedures to configure SSO for local authentication. The only difference is that when you configure the SSO mode on the Prime Infrastructure server, choose **Local** mode (not RADIUS or TACACS+).

- Add the SSO Server, on page 68
- Configure SSO Mode on the Prime Infrastructure Server, on page 68

Configure External Authentication

Users with web GUI root user or SuperUser privileges can configure Prime Infrastructure to communicate with external RADIUS, TACACS+, and SSO servers for external authentication, authorization, and accounting (AAA). If you choose to configure external authentication, the user groups, users, authorization profiles, authentication policies, and policy rules must be created in the external server through which all access requests to Prime Infrastructure will be routed.

You can use a maximum of three AAA servers. Users are authenticated on the second server only if the first server is not reachable or has network problems.

If you want to configure external authentication from the CLI, see Set Up External AAA Via CLI.

See the following topics for more information.

- Use RADIUS or TACACS+ for External Authentication, on page 54
- Use Cisco ISE With RADIUS or TACACS+ for External Authentication , on page 56
- Use Cisco ACS With RADIUS or TACACS+ for External Authentication, on page 62
- Use SSO with External Authentication, on page 68

Integrate Prime Infrastructure with an LDAP Server

Prime Infrastructure supports external authentication using an LDAP server. If you are interested in this configuration, contact your Cisco representative.

Use RADIUS or TACACS+ for External Authentication

These topics explain how to configure Prime Infrastructure to use RADIUS or TACACS+ servers.

- Add a RADIUS or TACACS+ Server to Prime Infrastructure, on page 54
- Configure RADIUS or TACACS+ Mode on the Prime Infrastructure Server, on page 55

Add a RADIUS or TACACS+ Server to Prime Infrastructure

TACACS uses three way handshake packet approach to authenticate and authorize the login credentials. As per TACACS+ RFC standard it is expected to have 2 authentication packet/1 authorization packet for PAP mode and 1 authentication packet/1 authorization packet for CHAP mode.

To add a RADIUS or TACACS+ server to Prime Infrastructure:

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

Step 2 Select the type of server you want to add.

- For RADIUS, choose **RADIUS Servers**. From the **Select a command** drop-down list, choose **Add RADIUS Server**, then click **Go**.
- For TACACS+, choose **TACACS+ Servers**. From the **Select a command** drop-down list, choose **Add TACACS+ Server**, then click **Go**.

Note You can use Move Up and Move Down arrow to reorder the available IP address.

Step 3 Enter the required information—IP address, DNS Name, and so forth. For Prime Infrastructure to communicate with the external authentication server, the shared secret you enter on this page must match the shared secret configured on the RADIUS or TACACS+ server. 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.

Step 4 Select the authentication type.

- PAP—Password-based authentication is the protocol where two entities share a password in advance and use the password as the basis of authentication.
- CHAP—Challenge-Handshake Authentication Protocol requires that both the client and server know the plain text of the secret, although it is never sent over the network. CHAP provides greater security than Password Authentication Protocol (PAP).

Step 5 If you have enabled the High Availability feature and configured a virtual IP address for the **Local Interface IP**, choose either the virtual IP address or the physical IP address of the primary server. See Cisco Prime Infrastructure Quick Start Guide.

Note The IP address configured in the external authentication server must match the **Local Interface IP**.

Step 6 Click **Test** to check the connectivity of the AAA server. The connectivity test will pass only if the port, authentication type and shared key you have entered matches with the TACACS or RADIUS server.

Note Only server reachability is tested for RADIUS server.

Step 7 Click **Save**.

Configure RADIUS or TACACS+ Mode on the Prime Infrastructure Server

Step 1 Log in to Prime Infrastructure as Super User.

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

Step 3 Select **TACACS+** or **RADIUS**.

Note We recommend you to set the value as "true" for the field **AAARemoteAddressEnabled** in the /opt/CSCOlumos/conf/ usermgmt.properties file through CLI, in order to display the client IP or System IP as the value of **Remote Address** under TACACS reports in the ACS server.

Step 4 Check the Enable Fallback to Local check box to enable the use of the local database when the external AAA server is down.

Step 5 If you want to revert to local authentication if the external RADIUS or TACACS+ server goes down, perform the following steps:

a) Select **Enable Fallback to Local**. If you disable this option Prime Infrastructure will read only the first server and the users added in the first server will be authenticated.

b) 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.If you select this option, you will be able to login as AAA user only.
- **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. If you select this option, you will be able to login as both local user and AAA user.

For AAA mode, SuperUser is always locally authenticated.

Step 6 Click **Save**.

Note Cisco Prime Infrastructure supports only Cisco ACS and ISE servers in the AAA mode.

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

Add a RADIUS or TACACS+ Server to Prime Infrastructure, on page 54
Renew AAA Settings After Installing a New Prime Infrastructure Version, on page 56

Renew 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.

Related Topics

Add a RADIUS or TACACS+ Server to Prime Infrastructure, on page 54
Required TACACS+/RADIUS Configurations After Prime Infrastructure IP Address Changes, on page 56

Use Cisco ISE With RADIUS or TACACS+ for External Authentication

Cisco Identity Services Engine (ISE) uses the RADIUS or TACACS+ protocols for authentication, authorization, and accounting (AAA). You can integrate Prime Infrastructure with Cisco ISE to authenticate the Prime Infrastructure users using the RADIUS or TACACS+ protocols. When you use external authentication, the details such as users, user groups, passwords, authorization profiles, authorization policies, and policy rules that are required for AAA must be stored and verified from the Cisco ISE database.

Complete the following tasks to use Cisco ISE with the RADIUS or TACACS+ protocol for external authentication:

Tasks to be completed to use Cisco ISE for external authentication	For information, see:
Make sure you are using a supported version of Cisco ISE	Supported Versions of Cisco ISE in Prime Infrastructure, on page 57
Add Prime Infrastructure as an AAA client in Cisco ISE	Add Prime Infrastructure as a Client in Cisco ISE, on page 57

Create a user group in Cisco ISE	Create a User Group in Cisco ISE, on page 58
Create a user in Cisco ISE and add the user to the user group that is created in Cisco ISE	Create a User and Add the User to a User Group in Cisco ISE, on page 58
(If using RADIUS) Create an authorization profile for network access in Cisco ISE, and add the RADIUS custom attributes with user roles and virtual domains created in Prime Infrastructure **Note** For RADIUS, you do not need to add the attributes for user tasks. They are automatically added based on the user roles.	Create an Authorization Profile for RADIUS in Cisco ISE, on page 58
(If using TACACS+) Create an authorization profile for network access in Cisco ISE, and add the TACACS+ custom attributes with user roles and virtual domains created in Prime Infrastructure **Note** For TACACS+, you need not add the attributes for user tasks. They are automatically added based on the user roles.	Create an Authorization Profile for TACACS+ in Cisco ISE, on page 59
Create an authorization policy in Cisco ISE and associate the policy with the user groups and authorization profile created in Cisco ISE	Configure an Authorization Policy for RADIUS in Cisco ISE, on page 61Configure an Authorization Policy for TACACS in Cisco ISE, on page 61
Create an authentication policy to define the protocols that Cisco ISE must use to communicate with Prime Infrastructure, and the identity sources that it uses for authenticating users to Prime Infrastructure	Create an Authentication Policy in Cisco ISE, on page 62
Add Cisco ISE as a RADIUS or TACACS+ server in Prime Infrastructure	Add a RADIUS or TACACS+ Server to Prime Infrastructure, on page 54
Configure the RADIUS or TACACS+ mode on the Prime Infrastructure server	Configure RADIUS or TACACS+ Mode on the Prime Infrastructure Server, on page 55

Supported Versions of Cisco ISE in Prime Infrastructure

Prime Infrastructure supports Cisco ISE from 2.1 Release onwards.

Add Prime Infrastructure as a Client in Cisco ISE

Step 1 Log in to Cisco ISE as the admin user.

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

Step 3 In the **Network Devices** page, click **Add**.

Step 4 Enter the device name and IP address of the Prime Infrastructure server.

Step 5 Check the **Authentication Settings** check box, and then enter the shared secret.

Note Ensure that this shared secret matches the shared secret you enter when adding the Cisco ISE server as the RADIUS server in Prime Infrastructure.

Step 6 Click **Submit**.

Create a User Group in Cisco ISE

Step 1 Log in to Cisco ISE as the admin user.
Step 2 Choose **Administration** > **Identity Management** > **Groups**.
Step 3 In the **User Identity Groups** page, click **Add**.
Step 4 In the **Identity Group** page, enter the name and description of the user group.
Step 5 Click **Submit**.

Create a User and Add the User to a User Group in Cisco ISE

Step 1 Log in to Cisco ISE as the admin user.
Step 2 Choose **Administration** > **Identity Management** > **Identities**.
Step 3 In the **Network Access Users** page, click **Add**.
Step 4 From the **Select an item** drop-down list, choose a user group to assign the user to.
Step 5 Click **Submit**.

Create an Authorization Profile for RADIUS in Cisco ISE

You create authorization profiles to define how different types of users are authorized to access the network. For example, you can define that a user attempting to access the network over a VPN connection is treated more strictly than a user attempting to access the network through a wired connection.

When you create an authorization profile for device administration, you must add the RADIUS custom attributes that are associated with user roles, tasks, and virtual domains created in Prime Infrastructure.

Note For RADIUS, you can add the user role attributes without adding the task attributes. The tasks are automatically added with the user roles.

For more information about Cisco ISE authorization profiles, see the information on managing authorization policies and profiles in the Cisco Identity Services Engine Administrator Guide.

To create an authorization profile for RADIUS in Cisco ISE:

Before you begin

Make sure you have the complete list of the following Prime Infrastructure custom attributes for RADIUS. You will need to add this information to Cisco ISE in this procedure.

- Prime Infrastructure user roles and tasks—see Export the Prime Infrastructure User Group and Role Attributes for RADIUS and TACACS+, on page 31
- Prime Infrastructure virtual domains—see Export the Prime Infrastructure Virtual Domain Attributes for RADIUS and TACACS+, on page 52

Step 1 Log in to Cisco ISE as the admin user.

Step 2 Choose **Policy** > **Policy Elements** > **Results**.

Step 3 From the left sidebar, choose **Authorization** > **Authorization Profiles**.

Step 4 In the **Standard Authorization Profiles** page, click **Add**.

Step 5 In the **Authorization Profile** page, enter the name and description of the authorization profile.

Step 6 From the **Access Type** drop-down list, choose **ACCESS_ACCEPT**.

Step 7 In the **Advanced Attributes Settings** area, paste in the complete list of RADIUS custom attributes for:

- User roles
- Virtual domains

Note If you do add user tasks, be sure to add the Home Menu Access task. It is mandatory.

Note For Operations Center, you must export NBI Read and NBI Write attributes.

Step 8 Click **Submit**.

Create an Authorization Profile for TACACS+ in Cisco ISE

You create authorization profiles to define how different types of users are authorized to access the network. For example, you can define that a user attempting to access the network over a VPN connection is treated more strictly than a user attempting to access the network through a wired connection.

When you create an authorization profile for device administration, you must add the TACACS+ custom attributes that are associated with user roles and virtual domains created in Prime Infrastructure.

Note

- For TACACS+, you need not add the attributes for user tasks. They are automatically added based on the user roles.
- In Release 8.5.135.0, the creation of Authorization server is deprecated. To create an Authorization server, you must create an Authentication server and duplicate it as an Authorization server. Due to this change in functionality, an alarm is generated in Cisco Prime Infrastructure 3.2 as follows:

  ```
  1.Successfully created Authentication server. 2.Failed to create
  authorization server:SNMP operation to Device failed: Set Operation
  not allowed for TACACS authorization server.1.Successfully created
  Accounting server.
  ```

  The workaround on Cisco Prime Infrastructure is to uncheck the Authorization server on the template. For more information, see CSCvm01415.

For more information about Cisco ISE authorization profiles, see the information on managing authorization policies and profiles in the Cisco Identity Services Engine Administrator Guide.

To create an authorization profile for TACACS+ in Cisco ISE:

Step 1 Log in to Cisco ISE as the admin user.

Step 2 Choose **Work Centers** > **Device Administration** > **Policy Elements** > **Results**.

Step 3 From the left sidebar, choose **TACACS Profiles**.

Step 4 In the **TACACS Profiles** page, click **Add**.

Step 5 In the **TACACS Profile** page, enter the name and description of the authorization profile.

Step 6 In the **Raw View** area, paste in the complete list of TACACS+ custom attributes for:

- User roles, including the tasks
- Virtual domains

Note

- From Prime Infrastructure Release 3.2 role based TACACS+ authentication is enabled by default.
- It is sufficient to add User roles and Virtual domains alone. If you do add user tasks, be sure to add the Home Menu Access task.
- You must set the value of the tacsacsServerTaskPref property in the file /opt/CSCOlumos/conf/usermgmt.properties to true and click **Save** in **Administration > Users > Users, Roles & AAA > AAA Mode Settings** Page, in order to enable task based TACACS authentication.

Note For Operations Center, you must export NBI Read and NBI Write attributes.

Step 7 Click **Submit**.

Configure an Authorization Policy for RADIUS in Cisco ISE

An authorization policy consists of a rule or a set of rules that are user-defined and produce a specific set of permissions, which are defined in an authorization profile. Based on the authorization profile, access requests to Prime Infrastructure are processed.

There are two types of authorization policies that you can configure:

- Standard—Standard policies are intended to be stable and are created to remain in effect for long periods of time, to apply to a larger group of users, devices, or groups that share a common set of privileges.
- Exception—Exception policies are created to meet an immediate or short-term need, such as authorizing a limited number of users, devices, or groups to access network resources. An exception policy lets you create a specific set of customized values for an identity group, condition, or permission that are tailored for one user or a subset of users.

For more information about authorization policies, see the "Manage Authorization Policies and Profiles" chapter in the Cisco Identity Services Engine Administrator Guide.

To create an authorization policy in Cisco ISE:

Step 1 Log in to Cisco ISE as the admin user.

Step 2 Choose **Policy** > **Authorization**.

Step 3 In the **Standard** area, click the down arrow on the far right and select either **Insert New Rule Above** or **Insert New Rule Below**.

Step 4 Enter the rule name and choose identity group, condition, attribute, and permission for the authorization policy.

For example, you can define a user group as Prime Infrastructure-SystemMonitoring-Group and choose this group from the Identity Groups drop-down list. Similarly, define an authorization profile as Prime Infrastructure-SystemMonitoring-authorization profile and choose this profile from the Permissions drop-down list. Now, you have defined a rule where all users belonging to the Prime Infrastructure System Monitoring identity group receive an appropriate authorization policy with system monitoring custom attributes defined.

Step 5 Click **Done**, and then click **Save**.

Configure an Authorization Policy for TACACS in Cisco ISE

To create an authorization policy for TACACS in Cisco ISE:

Step 1 Log in to Cisco ISE as the admin user.

Step 2 Choose **Device Work Centers** > **Device Administration** > **Device admin Policy Sets**.

Step 3 Choose **Default** in the left side pane.

Step 4 In the **Authorization Policy** area, click the down arrow on the far right and select either **Insert New Rule Above** or **Insert New Rule Below**.

Step 5 Enter the rule name and choose identity group, condition, Shell Profile for the authorization policy.

For example, you can define a user group as Prime Infrastructure-SystemMonitoring-Group and choose this group from the Identity Groups drop-down list. Similarly, define an authorization profile as Prime Infrastructure-SystemMonitoring-authorization profile and choose this profile from the Permissions drop-down list. Now,

you have defined a rule where all users belonging to the Prime Infrastructure System Monitoring identity group receive an appropriate authorization policy with system monitoring custom attributes defined.

Step 6 Click **Save**.

Create an Authentication Policy in Cisco ISE

Authentication policies define the protocols that Cisco ISE uses to communicate with Prime Infrastructure, and the identity sources that it uses for authenticating users to Prime Infrastructure. An identity source is an internal or external database where the user information is stored.

You can create two types of authentication policies in Cisco ISE:

- Simple authentication policy - In this policy, you can choose the allowed protocols and identity sources to authenticate users.
- Rule-based authentication policy - In this policy, you can define conditions that allow Cisco ISE to dynamically choose the allowed protocols and identity sources.

For more information about authentication policies, see the "Manage Authentication Policies" chapter in the Cisco Identity Services Engine Administrator Guide.

To create an authentication policy in Cisco ISE:

Step 1 Log in to Cisco ISE as the Super Admin or System Admin user.

Step 2 Choose **Policy** > **Authentication**.

Step 3 Choose the Policy Type as **Simple** or **Rule-Based** to create the required authentication policy.

Step 4 Enter the required details based on the policy type selected.

Step 5 Click **Save**.

Use Cisco ACS With RADIUS or TACACS+ for External Authentication

Cisco Secure Access Control System (ACS) uses RADIUS and TACACS+ protocol for authentication, authorization, and accounting (AAA).You can integrate Prime Infrastructure with Cisco ACS to authenticate the Prime Infrastructure users using the RADIUS or TACACS+ protocol. When you use an external authentication, the details such as users, user roles, passwords, authorization profiles, authorization policies, and policy rules that are required for AAA must be stored and verified from the Cisco ACS database.

Complete the following tasks to use Cisco ACS with the RADIUS or TACACS+ protocol for external authentication:

Tasks to be completed to use Cisco ACS for external authentication	For information, see:
Make sure you are using a supported version of Cisco ACS	Supported Versions of Cisco ACS in Prime Infrastructure, on page 63
Add Prime Infrastructure as an AAA client in Cisco ACS	Add Prime Infrastructure as a Client in Cisco ACS, on page 63

Create a user group in Cisco ACS	Create a User Group in Cisco ACS, on page 64
Create a user in Cisco ACS and add the user to the Cisco ACS user group	Create a User and Add the User to a User Group in Cisco ACS, on page 64
(If using RADIUS) Create an authorization profile for network access in Cisco ACS, and add the RADIUS custom attributes for user roles and virtual domains created in Prime Infrastructure. **Note** For RADIUS, you do not need to add the attributes for user tasks. They are automatically added based on the user roles.	Create an Authorization Profile for RADIUS in Cisco ACS, on page 64
(If using TACACS+) Create an authorization profile for device administration in Cisco ACS, and add the TACACS+ custom attributes with user roles and virtual domains created in Prime Infrastructure. **Note** For TACACS+, you need not add the attributes for user tasks. They are automatically added based on the user roles.	Create an Authorization Profile for TACACS+ in Cisco ACS, on page 65
Create an access service in Cisco ACS and define a policy structure for the access service.	Create an Access Service for Prime Infrastructure in Cisco ACS, on page 66
Create an authorization policy rule in Cisco ACS, and map the authorization or shell profile based on the access type (network access or device administration).	Create an Authorization Policy Rule in Cisco ACS, on page 67
Configure a service selection policy in Cisco ACS and assign an access service to an incoming request.	Configure a Service Selection Policy in Cisco ACS, on page 67
Add Cisco ACS as a RADIUS or TACACS+ server in Prime Infrastructure.	Add a RADIUS or TACACS+ Server to Prime Infrastructure, on page 54
Configure the RADIUS or TACACS+ mode on the Prime Infrastructure server.	Configure RADIUS or TACACS+ Mode on the Prime Infrastructure Server, on page 55

Supported Versions of Cisco ACS in Prime Infrastructure

Prime Infrastructure supports Cisco ACS 5.*x* releases.

Add Prime Infrastructure as a Client in Cisco ACS

Step 1 Log in to Cisco ACS as the admin user.

Step 2 From the left sidebar, choose **Network Resources** > **Network Devices** > **Network Devices and AAA Clients**.

Step 3 In the **Network Devices** page, click **Create**.

Step 4 Enter the device name and IP address of the Prime Infrastructure server.

Step 5 Choose the authentication option as **RADIUS** or **TACACS+**, and enter the shared secret.

Note Ensure that this shared secret matches the shared secret you enter when adding the Cisco ACS server as the RADIUS or TACACS+ server in Prime Infrastructure.

Step 6 Click **Submit**.

Create a User Group in Cisco ACS

Step 1 Log in to Cisco ACS as the admin user.
Step 2 From the left sidebar, Choose **Users and Identity Stores** > **Identity Groups**.
Step 3 In the **Identity Groups** page, click **Create**.
Step 4 Enter the name and description of the user group.
Step 5 Select a network device group parent for the user group.
Step 6 Click **Submit**.

Create a User and Add the User to a User Group in Cisco ACS

Step 1 Log in to Cisco ACS as the admin user.
Step 2 From the left sidebar, Choose **Users and Identity Stores** > **Internal Identity Stores** > **Users**.
Step 3 In the **Internal Users** page, click **Create**.
Step 4 Enter the required details.
Step 5 In the **Identity Group** field, click **Select** to choose a user group to assign the user to.
Step 6 Click **Submit**.

Create an Authorization Profile for RADIUS in Cisco ACS

You create authorization profiles to define how different types of users are authorized to access the network. For example, you can define that a user attempting to access the network over a VPN connection is treated more strictly than a user attempting to access the network through a wired connection.

When you create an authorization profile for device administration, you must add the RADIUS custom attributes that are associated with user roles, tasks, and virtual domains created in Prime Infrastructure.

Note For RADIUS, you can add the user role attributes without adding the task attributes. The tasks are automatically added with the user roles.

For more information about Cisco ACS authorization profiles and policies, see chapters on managing policy elements and access policies in the User Guide for Cisco Secure Access Control System.

To create an authorization profile for RADIUS in Cisco ACS:

Before you begin

Make sure you have the complete list of the following Prime Infrastructure custom attributes for RADIUS. You will need to add this information to Cisco ACS in this procedure.

- Prime Infrastructure user roles and tasks—see Export the Prime Infrastructure User Group and Role Attributes for RADIUS and TACACS+, on page 31
- Prime Infrastructure virtual domains—see Export the Prime Infrastructure Virtual Domain Attributes for RADIUS and TACACS+, on page 52

Step 1 Log in to Cisco ACS as the admin user.

Step 2 From the left sidebar, choose **Policy Elements** > **Authorizations and Permissions** > **Network Access** > **Authorization Profiles**.

Step 3 Click **Create**.

Step 4 On the **General** tab, enter the name and description of the authorization profile.

Step 5 Click the **RADIUS Attributes** tab, and paste in the complete list of RADIUS custom attributes for:

- User roles
- Virtual domains

Note If you do add user tasks, be sure to add the Home Menu Access task. It is mandatory.

Note For Operations Center, you must export NBI Read and NBI Write attributes.

Step 6 Click **Submit**.

Create an Authorization Profile for TACACS+ in Cisco ACS

When you create an authorization profile for device administration, you must add the TACACS+ custom attributes that are associated with user roles and virtual domains created in Prime Infrastructure.

Note For TACACS+, you need not add the attributes for user tasks. They are automatically added based on the user roles.

For more information about Cisco ACS authorization profiles and policies, see chapters on managing policy elements and access policies in the User Guide for Cisco Secure Access Control System.

To create an authorization profile for TACACS+ in Cisco ACS:

Before you begin

Make sure you have the complete list of the following Prime Infrastructure custom attributes. You will need to add this information to Cisco ACS in this procedure.

- Prime Infrastructure user roles and tasks—see Export the Prime Infrastructure User Group and Role Attributes for RADIUS and TACACS+, on page 31
- Prime Infrastructure virtual domains—see Export the Prime Infrastructure Virtual Domain Attributes for RADIUS and TACACS+, on page 52.

Step 1 Log in to Cisco ACS as the admin user.

Step 2 From the left sidebar, choose **Policy Elements** > **Authorizations and Permissions** > **Device Administration** > **Shell Profiles**.

Step 3 Click **Create**.

Step 4 On the **General** tab, enter the name and description of the authorization profile.

Step 5 Click the **Custom Attributes** tab, and paste in the complete list of TACACS+ custom attributes for:

- User roles, including the tasks
- Virtual domains

Step 6 Click **Submit**.

Create an Access Service for Prime Infrastructure in Cisco ACS

Access services contain the authentication and authorization policies for access requests. You can create separate access services for different use cases; for example, device administration (TACACS+), network access (RADIUS), and so on.

When you create an access service in Cisco ACS, you define the type of policies and policy structures that it contains; for example, policies for device administration, network access, and so on.

Note You must create access services before you define service selection rules, although you do not need to define the policies in the services.

To create an access service for Prime Infrastructure requests:

Step 1 Log in to Cisco ACS as the admin user.

Step 2 From the left sidebar, choose **Access Policies** > **Access Services**.

Step 3 Click **Create**.

Step 4 Enter the name and description of the access service.

Step 5 Choose one of the following options to define a policy structure for the access service:

- **Based on service template**—Creates an access service containing policies based on a predefined template.
- **Based on existing service**—Creates an access service containing policies based on an existing access service. However, the new access service does not include the existing service's policy rules.
- **User selected service type**—Provides you the option to select the access service type. The available options are Network Access (RADIUS), Device Administration (TACACS+), and External Proxy (External RADIUS or TACACS+ servers).

Step 6 Click **Next**.

Step 7 Choose the authentication protocols that are allowed for the access service.

Step 8 Click **Finish**.

Create an Authorization Policy Rule in Cisco ACS

Step 1 Log in to Cisco ACS as the admin user.

Step 2 From the left sidebar, choose **Access Policies** > **Access Services** > **service** > **Authorization**.

Step 3 Click **Create**.

Step 4 Enter the name of the rule and then choose the rule status.

Step 5 Configure the required conditions for the rule.

For example, you can create a rule based on the location, device type, or user group that you have created.

Step 6 If you are creating an authorization policy rule for network access (RADIUS), choose the required authorization profile(s) to map to the authorization policy rule.

Alternatively, if you are creating an authorization policy rule for device administration (TACACS+), choose the required shell profile(s) to map to the authorization policy rule.

Note If you are using multiple authorization profiles or shell profiles, make sure you order them in priority.

Step 7 Click **OK**.

Configure a Service Selection Policy in Cisco ACS

A service selection policy determines which access service applies to an incoming request. For example, you can configure a service selection policy to apply the device administration access service to any access request that uses the TACACS+ protocol.

You can configure two types of service selection policy:

- Simple service selection policy—Applies the same access service to all requests.
- Rule-based service selection policy—Contains one or more conditions and a result, which is the access service that will be applied to an incoming request.

To configure a service selection policy:

Step 1 Log in to Cisco ACS as the admin user.

Step 2 From the left sidebar, choose **Access Policies** > **Access Services** > **Service Selection Rules**.

Step 3 If you want to configure a simple service selection policy, click the **Single result selection** radio button, and then choose an access service to apply to all requests.

Alternatively, if you want to configure a rule-based service selection policy, click the **Rule based result selection** radio button, and then click **Create**.

Step 4 Enter the name of the rule and then choose the rule status.

Step 5 Choose either **RADIUS** or **TACACS+** as the protocol for the service selection policy.

Step 6 Configure the required compound condition, and then choose an access service to apply to an incoming request.

Step 7 Click **OK**, and then click **Save Changes**.

Use SSO with External Authentication

To set up and use SSO (with or without a RADIUS or TACACS+ server), see these topics:

- Add the SSO Server, on page 68
- Configure SSO Mode on the Prime Infrastructure Server, on page 68

Prime Infrastructure does not support localization on the SSO sign-in page.

Add the SSO Server

Prime Infrastructure can be configured with a maximum of three AAA servers.

Step 1 Choose **Administration** > **Users** > **Users, Roles & AAA**, then choose **SSO Servers**.

Step 2 From the **Select a command** drop-down list, choose **Add SSO Servers**, then click **Go**.

Step 3 Enter the SSO information. The maximum number of server retries for an SSO server authentication request is 3.

Step 4 Click **Save**.

Note If you want the hostname to appear in the Prime Infrastructureserver URL, you must configure SSO using FQDN after logging in to Prime Infrastructure with the hostname.

Configure SSO Mode on the Prime Infrastructure Server

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

Note If you are using this procedure to configure SSO but are using local authentication, choose **Local** in Step 2.

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

Step 2 Select the SSO Server AAA Mode you want to use. The options are: **Local**, **RADIUS**, or **TACACS+**.

Step 3 Click **Save**.