



User Permissions and Device Access

- [User Interfaces, User Types, and How To Transition Between Them, on page 1](#)
- [Enable and Disable root Access for the Cisco EPN Manager Web GUI, on page 4](#)
- [Control the Tasks Web Interface Users Can Perform, on page 4](#)
- [Add Users and Manage User Accounts, on page 25](#)
- [Find Out Which Users Are Currently Logged In, on page 28](#)
- [View the Tasks Performed By Users \(Audit Trail\), on page 29](#)
- [Configure Job Approvers and Approve Jobs, on page 29](#)
- [Configure Global Password Policies for Local Authentication, on page 30](#)
- [Configure Number of Parallel Sessions Allowed, on page 30](#)
- [Configure the Global Timeout for Idle Users, on page 31](#)
- [Create Virtual Domains to Control User Access to Devices, on page 32](#)
- [Configure Local Authentication, on page 39](#)
- [Configure External Authentication, on page 40](#)

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

These topics describe the GUI and CLI interfaces used by Cisco Evolved Programmable Network Manager, and how to transition between the Cisco Evolved Programmable Network Manager and Linux CLI interfaces.

- [User Interfaces and User Types, on page 1](#)
- [How to Transition Between the CLI User Interfaces in Cisco Evolved Programmable Network Manager, on page 3](#)

User Interfaces and User Types

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

Cisco EPN Manager User Interface	Interface Description	CEPMM User Types
Cisco EPN Manager web GUI	<p>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.</p> <p>This interface provides a subset of operations that are provided by the Cisco EPN Manager CLI admin and CLI config users.</p>	<p>Cisco Evolved Programmable Network Manager 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 <i>user groups</i> (Admin, Super Users, Config Managers, and so forth). For information on the user groups, see Types of User Groups, on page 5.</p> <p>Cisco Evolved Programmable Network Manager 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 4.</p> <p>Note The Cisco EPN Manager web GUI root user is not the same as the Linux CLI root user, nor is it the same as the Cisco EPN Manager CLI admin user.</p>
North Bound Interface (NBI) REST API	<p>NBI is REST Application Programming Interface that allows a client system to talk to Cisco EPN Manager to carry out day-to-day and administration operations. Special privileged service account users are assigned to a client system to allow talking to Cisco EPN Manager using this interface.</p> <p>These NBI users can also have varying degrees of privileges and are also classified into role-based access control (RBAC) classes and subclasses.</p>	Cisco EPN Manager NBI users—Created by web GUI root user. These users have three different types of privileges and are classified into role-based access control (RBAC) classes and subclasses called NBI user groups (NBI Read and NBI Write). For information on the user groups, see section User Groups—NBI, on page 6

Cisco EPN Manager User Interface	Interface Description	CEPNM User Types
CEPNM 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 Cisco EPN Manager administration tasks. These commands are explained throughout this guide. To use this CLI, you must have Cisco EPN Manager CLI admin user access. You can access this shell from a remote computer using SSH.	<p>Cisco EPN Manager 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 is available in the web GUI.)</p> <p>To display a list of operations this user can perform, enter <code>?</code> at the prompt.</p> <p>Some tasks must be performed in config mode. To transition to config mode, use the procedure in Transition Between the Cisco Evolved Programmable Network Manager admin CLI and Cisco Evolved Programmable Network Manager config CLI, on page 3.</p>
CEPNM Config CLI	Cisco proprietary shell which is restricted and more secure than the Linux shell. This Config shell and CLI provide commands for Cisco EPN Manager 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 in the Admin CLI shell.	<p>The admin CLI user can create other CLI users for various reasons, using the following command:</p> <pre>(config) username <i>username</i> password <i>role</i> {<i>admin user</i>} <i>password</i></pre> <p>These users may have admin-like privilege/roles or lower-level privileges as defined during creation time. To create a Cisco Evolved Programmable Network Manager CLI user with admin privileges, run the username command with the admin keyword; otherwise, use the user keyword. For password limitations, see Create Admin User.</p>
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 admin shell and CLI.	<p>Linux CLI admin user—Created at installation time and used for Linux-level administration purposes.</p>

How to Transition Between the CLI User Interfaces in Cisco Evolved Programmable Network Manager

Refer to the following section to understand how to transition between the Cisco EPN Manager admin CLI and Cisco EPN Manager config CLI

Transition Between the Cisco Evolved Programmable Network Manager admin CLI and Cisco Evolved Programmable Network Manager config CLI

To move from the Cisco Evolved Programmable Network Manager admin CLI to the Cisco Evolved Programmable Network Manager 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)#
```

Enable and Disable root Access for the Cisco EPN Manager Web GUI

After installation, you should disable the Cisco EPN Manager 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 4](#).

Disable and Enable the Web GUI root User

-
- Step 1** Log into the Cisco EPN Manager 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. Once this is done, you can disable the web GUI **root** account.
- Step 2** Disable the Cisco EPN Manager 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

For Web Interface users, in Cisco EPN Manager user authorization is implemented through user groups. A user group contains a list of tasks that control which parts of Cisco EPN Manager 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 32](#).

Cisco EPN Manager 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, on page 5](#)

- [View and Change the Tasks a User Can Perform, on page 6](#)
- [View and Change the Groups a User Belongs To, on page 7](#)
- [View User Groups and Their Members, on page 7](#)
- [Create a Customized User Group, on page 23](#)
- [View and Change the Tasks a Group Can Perform, on page 24](#)
- [Use Cisco EPN Manager User Groups with RADIUS and TACACS+, on page 24](#)

Types of User Groups

Cisco EPN Manager provides the following predefined user groups:

- [User Groups—Web UI, on page 5](#)
- [User Groups—NBI, on page 6](#)

For information about CLI users, see [User Interfaces and User Types, on page 1](#).

User Groups—Web UI

Cisco EPN Manager provides the default web GUI user groups that are listed in the following table. You can assign users to multiple groups, except for the users that belong to the Monitor Lite user group (because Monitor Lite is for users with limited permissions).

See [View and Change the Tasks a Group Can Perform, on page 24](#) 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 . The best practice is to create other users with Admin or Super Users privileges, and disable the root web UI user as described in Disable and Enable the Web GUI root User, on page 4 .
Super Users	All operations (not by default). The group permissions are editable. Can enable permissions similar to those of a root user.
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. 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 Group	Group Task Focus
User-Defined 1-50	N/A; these are blank groups and can be edited and customized as required.
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.
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.

User Groups—NBI

Cisco EPN Manager provides the default NBI user groups that are 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 24](#) for information on the tasks that pertain to each user group and the default settings.

User Group	Provides access to:
NBI Read	RESTCONF NBI read operations (HTTP GET). Can also belong to other NBI and web UI user groups.
NBI Write	RESTCONF NBI write operations (HTTP PUT, POST, DELETE). Can also belong to other NBI and web UI user groups.

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 the user group and tasks you are authorized to perform.



Note If you want to check the *devices* a user can access, see [Assign Virtual Domains to Users, on page 37](#).

- Step 1** Choose **Administration > Users > Users and Roles**.
- Step 2** Choose the **Roles** tab, and locate the user group from the left pane under Roles.
- Step 3** Select the user group and choose **Task Permissions** tab, which lists the tasks that group members can and cannot perform.
- Selected check box means the group members can perform that task. If a checked box is greyed-out, it means you cannot disable the task. For example, Cisco EPN Manager 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 that 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 applies 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 24](#).
- Add the user to a different user group. The predefined user groups are described in [User Groups—Web UI, on page 5](#) and [User Groups—NBI, on page 6](#). 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 7](#).
- 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 24](#). To create a new customized group, see [Create a Customized User Group, on page 23](#).

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 26](#)). User groups are described in [Types of User Groups, on page 5](#).

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 and Roles**, then choose **Users**.

Step 2 In the **User Name** column, locate and select the user name check box. Click the **Edit** option. **Edit User** window appears.

- A checked check box means the user belongs to that group. If a checked box is grayed-out, it means you cannot remove the user from that group. For example, Cisco EPN Manager will not allow you to remove the user named **root** from the root user group.

Step 3 To change the groups the user belongs to, select and unselect the appropriate groups in the **Role Details** drop-down list, then click **Save**.

View User Groups and Their Members

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

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

The Roles 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 5](#).

Step 2 To view all members of a group, select a group name and choose **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 24](#)
 - [View and Change the Groups a User Belongs To, on page 7](#)
-

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
Administrative Operations	Appliance	Allows users to access appliances
	Application Server Management Access	Allows users to access and manage the application server
	Application and Services Access	Allows users to access application and their services
	Cisco DNA Center coexistence	Allows the users to access Cisco DNA center
	Data Migration	Allows the users to Data Migration
	Design Endpoint Site Association Access	Allows the users to access design endpoint sites
	Device Console Config	Allows user to run configuration commands on Device Console
	Device Console Show	Allows user to run show commands on Device Console
	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 users to access license center/smart license
	Logging	Gives access to the menu item which allows user to configure the logging levels
	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
User Defined Fields		

Task Group Name	Task Name	Description
		Allows user to create user defined fields
	User Preferences	Controls access to the Administration > User Preference menu.
	View Audit Logs Access	Allows user to view Network and System audits
	Audit Trails	Allows users to access audit trails
	LDAP Server	Allows users to access LDAP servers
	RADIUS Servers	Allows users to access RADIUS servers
	SSO Server AAA Mode	Allows users to access SSO servers in AAA mode only
	SSO Servers	Allows users to access SSO Servers
	TACACS+ Servers	Allows users to access TACACS+ servers
	Users and Groups	Allows users to access users and groups
	Virtual Domain Management	Allows users to manage virtual domains
	Virtual Elements Tab Access	Allows users to access the virtual elements tab

Task Group Name	Task Name	Description
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
	Email Notification	Allows user to configure email notification forwarding
	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
	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	
Background Ajax Call	License Check	Allows user to check validity of license, Controller license and MSE license
Configure Menu Task	Configure Menu Access	Allows user to access all features under Configuration Menu
	Unsanitized Device Config Export	Allows user to expose unsanitized Configuration Archive
Feedback and Support Tasks	Automated Feedback	Allows access 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.

Task Group Name	Task Name	Description
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 import groups
	Modify Groups	Allows user to edit group attributes such as name, parent, and rules
Help Menu Task	Help Menu Access	Allows user to access Help Menu
Home Menu Task	Home Menu Access	Allows user to access Homepage

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 view scheduled jobs.
	Config Deploy Edit Job	Allows user to edit config deployed jobs
	Device Config Backup Job Edit Access	Allows user to change the external backup settings such as repository and file encryption 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
Monitor Menu Task	Monitor Menu Access	Allows user to access all features under Monitor Menu

Task Group Name	Task Name	Description
Network Configuration	Add Device Access	Allows user to add devices to Cisco EPN Manager
	Admin Templates Write Access	Check thois check-box for enabling admin templates write access for user defin role
	Auto Provisioning	Allows access to auto provisioning
	Alarm Monitor Policies	Allows access to Alarm monitor policies
	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
	Config Archive Read Task	Allows config archive read access
	Config Archive Read-Write Task	Allows config archive read-write access
	Configlet Access	Allows Configlet access
	Configuration Templates Read Access	Allows to access configuration templates in read only mode
	Configure ACS View Servers	Allows users to configure ACS view servers
	Configure Access Points	Allows users to configure access points
	Configure Autonomous Access Point Templates	Allows users to access autonomous access point templates
Configure Choke Points		

Task Group Name	Task Name	Description
		Allows users to configure choke points
	Configure Config Groups	Allows access to Config Group
	Configure Controllers	Allows users to configure controllers
	Configure Ethernet Switch Ports	Allows the user to access ethernet switch ports
	Configure Ethernet Switches	Allows the user to access ethernet switches
	Configure ISE Servers	Allows users to manage ISE servers on Cisco EPN Manager
	Configure Lightweight Access Point Templates	Allows users to access lightweight access point templates
	Configure Mobility Devices	Allows users to access mobility devices
	Configure Spectrum Experts	Allows the users to configure spectrum experts
	Configure Switch Location Configuration Templates	Allows users to access switch location configuration templates
	Configure Templates	Allows the user to do the CRUD operation of Feature Templates and configuration Template
	Configure Third Party Controllers and Access Point	Allows the user to configure third party controllers and access points
	Configure WIPS Profiles	Allows the user to access WIPS profiles
	Configure WiFi TDOA Receivers	Allows the 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 Cisco EPN Manager
	Deploy Configuring Access	Allows user to deploy Configuration and IWAN templates

Task Group Name	Task Name	Description
	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 user to access the Global SSID groups
	MBC UI Framework Access	Allows the user to access MBC UI framework
	Migration Templates	Allows the user to access migration templates
	Device WorkCenter	Allows the user to access device WorkCenter
	Network Topology Edit	Allows user to create devices, links and network in the topology map, edit the manually created link to assign the interface
	Provisioning Access	Allows access to Provisioning
	QoS Profile Configuration Access	Allows user to create, modify, delete QoS profiles and schedule QoS profiles deployment job or associate/disassociate interface and Import/Export QoS discovered profiles
	Scheduled Configuration Tasks	Allows the user to edit scheduled configuration tasks
	TrustSec Readiness Assessment	Allows the user to access the TrustSec readiness assessment details
	View Compute Devices	Allows the users to view compute devices
	WIPS Service	

Task Group Name	Task Name	Description
		Allows the user to access WIPS services

Task Group Name	Task Name	Description
Network Monitoring	Ack and Unack Security Index Issues	Allows user to access the Ack and Unack Security Index Issues
	Admin Dashboard Access	Allows user to access the Admin Dashboard
	Chassis View Read	Allows chassis view read access
	Chassis View Read-Write	Allows chassis view read-write access
	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 the user to disable clients
	Identify Unknown Users	Allows the user to identify any unknown user
	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	Gives the user lync monitoring access
	Monitor Access Points	Allows the user to monitor the access points on the network
	Monitor Clients	Allows the user to monitor clients on the network
	Monitor Controllers	Allows the user to monitor controllers
	Monitor Ethernet Switches	Allows the user to monitor ethernet switches in the network
	Monitor Interferers	Allows the user to monitor interferers
	Monitor Media Streams	Allows the user to monitor media streams
Monitor Mobility Devices		

Task Group Name	Task Name	Description
		Allows the user to monitor mobility devices on the network
	Monitor Security	Gives the user access to monitor security
	Monitor Spectrum Experts	Allows the user to monitor spectrum experts
	Monitor Tags	Allows the user to monitor Tags
	Monitor Third Party Controllers and Access Point	Allows the user to monitor third party controllers and access points in the network
	Monitor WiFi TDOA Receivers	Allows the user to Monitor WiFi TDOA receivers
	Monitoring Interfaces	Gives the user access to Monitoring Interfaces
	Monitoring Policies	Gives the user access to Monitoring Policies
	Network Topology	Allows users to launch the Network Topology map and view the devices and links in the map
	Packet Capture Access	Gives the user Packet Capture access
	Performance Dashboard Access	Allows the user to access the Performance dashboard
	PfR Monitoring Access	Gives the user access to PfR Monitoring
	RRM Dashboard	Allows the user to access the RRM dashboard
	Remove Clients	Gives the user permission to remove clients on the network
	Service Health Access	Allows the user to monitor service health
	Site Visibility Access	Gives the user access to Site Visibility
	Track Clients	Gives the user the ability to track clients
	View Security Index Issues	Allows the user to view any security index issues

Task Group Name	Task Name	Description
	Voice Diagnostics	Allows the user to access voice diagnostics
	Wireless Dashboard Access	Allows the user to access wireless dashboard
OTDR	OTDR Configure Profiles	Allows access to OTDR configure profiles
	OTDR run scans	Allows user access to OTDR scans
	OTDR Set Baselines	Allows access to OTDR baselines.
	OTDR View Scan results	Allows user to view OTDR scan results
Product Usage	Product Feedback	Allows user to access Help Us Improve page

Task Group Name	Task Name	Description
Reports	CE Performance Reports	Allows user to create the CE performance report
	CE Performance Reports Read Only	Allows user to create the read only CE performance report
	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
	Network Summary Reports	Allows user to create and run network summary reports
	Network Summary Reports Read Only	Allows user to view all Summary reports
	Optical Performance Reports	Allows user to create Optical performance reports
	Optical Performance Reports Read Only	Allows user to view Optical performance reports
	Performance Reports	Allows user to create performance reports
	Performance Reports Read Only	Allows user to view performance reports
	Report Launch Pad	Allows user to access the Report page
	Saved Reports List	Allows user to save reports
	System Monitoring Reports	Allows user to view System Monitoring Reports
	System Monitoring Reports Read Only	Allows user to view the read only system monitoring reports
Virtual Domains List	Allows user to create the Virtual Domain related report	

Task Group Name	Task Name	Description
Software Image Management	Add Software Image Management Servers	Allows user to add software imagemanagement servers
	Image Details View	Allows user to view the image details
	Manage Protocol	Allows user to manage the Protocols
	Swim Access Privilege	Swim Access Privilege
	Swim Activation	Swim Activation
	Swim Collection	Swim Collection
	Swim Delete	Swim Delete
	Swim Distribution	Swim Distribution
	Swim Preference Save	Allows user to save preference options on System Settings à Image Management page
	Software Info Update	Allows the user to edit and save image properties such as minimum RAM, minimum FLASH and minimum boot ROM version
	Swim Recommendation	Allows user to recommend images from Cisco.com and from the local repository
	Swim 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
	LDAP Server	Allows user to access the LDAP Server menu
	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 online help

Create a Customized User Group

Cisco EPN Manager provides a set of predefined user groups that help you control user authorization. These groups are described in [Types of User Groups, on page 5](#) 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 and Roles**, then choose **Roles**.
 - Step 2** Locate and select a User Defined group that has no members in the left-side Roles pane.
 - Step 3** Customize the group permissions by checking and unchecking tasks in the **Role Permissions** window. If a task is greyed-out, it means you cannot adjust its setting. You can rename any of the user groups by clicking the **Edit** icon in front of the User Defined group name.
 - Step 4** Click **Save** to save your group settings.

- Step 5** 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 26](#) for information on adjusting user accounts.

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 7](#).



Note If you want to change *device* access, see [Assign Virtual Domains to Users, on page 37](#).

- Step 1** Choose **Administration > Users > Users and Roles**, then choose **Roles**.

The Roles page lists all existing user groups.

- Step 2** Select a user group. The **Role Permissions** window lists the tasks permissions.

- A checked task means that group members have permission to perform that task. If a checked box is grayed-out, you cannot disable the task.
- A blank check box means that group members cannot perform that task. If a blank check box is grayed out, 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 affects *all group members*—check and uncheck tasks, then click **Save**.

Note Be careful. Selecting and deselecting tasks in the Group Detail window applies your changes to *all group members*. An alternative is to create a new group using one of the User Defined group templates; see [Create a Customized User Group, on page 23](#).

Use Cisco EPN Manager User Groups with RADIUS and TACACS+

Your RADIUS or TACACS+ servers must be configured to recognize the user groups that exist in Cisco EPN Manager. You can do this using the procedure in [Export the Cisco EPN Manager User Group and Role Attributes for RADIUS and TACACS+, on page 24](#).

Export the Cisco EPN Manager User Group and Role Attributes for RADIUS and TACACS+

If you are using RADIUS or TACACS+, you must copy all Cisco EPN Manager user group and role information into your Cisco Identity Services Engine (ISE) server. You can do this using the Task List dialog box provided in the Cisco EPN Manager web GUI. If you do not export the data into your Cisco ISE server, Cisco EPN Manager 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).



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

Step 1

In Cisco EPN Manager:

- a) Choose **Administration > Users > Users and Roles > Roles**.
- b) From the Roles list, select the user group, and copy the role for each user group by clicking the **Task List** icon (in front of Role Permissions).
 - 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 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 ISE, see:

- [Use Cisco ISE With RADIUS or TACACS+ for External Authentication](#) , on page 42
- 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

- [Create Web GUI Users with Administrator Privileges](#), on page 25
- [Add and Delete Users](#), on page 26
- [Disable \(Lock\) a User Account](#), on page 27
- [Change a User's Password](#), on page 27

Create Web GUI Users with Administrator Privileges

After installation, Cisco EPN Manager 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 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 and Roles**, then choose **Users**.
- Step 2** On the **Users** window, click to display a new user entry in the table.
- Step 3** Enter the username in the **User Name** 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** (Optional) Enter the **First Name**, **Last Name**, and **Description** for the user.
- Step 6** Enter the email address in the **Email Address** text box.
- Step 7** In the **Role** drop-down list, choose **Admin**.
- Step 8** From the **Virtual Domains**, 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 32](#).
- Note** If you select a parent virtual domain the child (subordinate) virtual domains under it will also get selected.
- Step 9** Click **Save**.
- Note** When you create a new user, do not autofill or save the user credentials in the browser.
-

What to do next

For security purposes, disable the web GUI root account as described in [Disable and Enable the Web GUI root User, on page 4](#).

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 must edit the user account to add the domain access. See [Create Virtual Domains to Control User Access to Devices, on page 32](#).

If you want to temporarily disable an account (rather than delete it), see [Disable \(Lock\) a User Account, on page 27](#).


-
- Step 1** Choose **Administration > Users > Users and Roles**, then choose **Users**.
- Step 2** Click to display a new user entry.
- Step 3** Configure the user account.
- a) Enter a username and password.

Note To autogenerate the password, enter the username and the email address. For more information, see [Auto-generate a User's Password, on page 28](#).
 - b) Enter the first name, last name, and a description for the user.

- c) Control the actions that 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 7](#).
- d) Control the devices that a user can access from the **Virtual Domains** space and assigning domains to the user. (See [Create Virtual Domains to Control User Access to Devices, on page 32](#).)

Step 4 Click **Save**.

Note When you create a new user, do not autofill or save the user credentials in the browser.

Step 5 To delete user accounts, select a user, and click .

Step 6 Click **Delete** to confirm that you 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 Cisco EPN Manager GUI. You might want to do this if a user is temporarily changing job functions. If the user tries to log in, Cisco EPN Manager 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 26](#).

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 27](#) and [Configure Global Password Policies for Local Authentication, on page 30](#).

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

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

Step 3 Click  to lock the user (or  **Unlock User(s)** to unlock the user).

Change a User's Password

You can configure password rules to force users to change their passwords (see [Configure Global Password Policies for Local Authentication, on page 30](#)). Users can change their own passwords as described in [Change Your Password](#). To change a user's password manually, use this procedure:

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

Step 2 Select the username and click  icon, which opens the Edit User window.

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

Auto-generate a User's Password

Cisco EPN Manager offers you the option to auto-generate the password for new and existing users based on the email server availability. If this option is enabled, the system sends an email to the user with password details.



Note The **Auto-generate Passwords** option is available only if the email server is configured.

To auto-generate the password and email it to the user, follow this procedure:

Before you begin

Configure the email sever. For more information, see [Set Up the SMTP E-Mail Server](#).



-
- Step 1** Choose **Administration > Users > AAA**, select **Settings**, and expand the **Local Password Policy** drop-down.
 - Step 2** Select the **Auto-generate Passwords** check box.
 - Step 3** Click **Save All Changes** to save your changes.
 - Step 4** Go to **Administration > Users > Users and Roles**, then click **Users**.
 - a) For a new user, enter the user name and email address.
 - b) For an existing user, reset the password.
 - Step 5** Click **Save** to save your changes and send an email notification to the user.
-

Find Out Which Users Are Currently Logged In

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



Note By default, Cisco EPN Manager displays 50 records without pagination for the subsequent records. To view more than 50 records, click the settings icon at the top-right corner of the screen and enter the required value in **My Preferences > General > Items per Page List** field.

-
- Step 1** Choose **Administration > Users > Users and Roles**, then choose **Active Sessions** tab. Cisco EPN Manager lists all users that are currently logged in to the Cisco EPN Manager server, including their client machine IP address.
 - Step 2** To view a historical list of all actions performed by this user, click the  icon that corresponds to the user name, and choose **Audit Trail**. If the user performed any actions on managed devices (for example, the user added new devices to Cisco EPN Manager), the device IP addresses are listed in the Device IP Address column.
 - Step 3** If you want to end an active user session, click , and choose **Terminate Session**.

Note **Terminate Session** terminates only an active user session. If you want to prevent the user from logging back in again, see [Disable \(Lock\) a User Account, on page 27](#).

View the Tasks Performed By Users (Audit Trail)

Cisco EPN Manager 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, 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 or issues commands on a network element through the **Device Console**), 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), Cisco EPN Manager displays an audit entry for each switch.


To find out which users are currently logged into the Cisco EPN Manager web GUI, see [Find Out Which Users Are Currently Logged In, on page 28](#).

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


- [Audit Changes Made By Users \(Change Audit\)](#)
-

Step 1 Choose **Administration > Users > Users and Roles**.

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

- Choose **Users**.
- Locate the user name, click the  icon, and choose **Audit Log**.

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

- Choose **Roles**.
 - Locate the user group name and click the **Members** tab. Click the  icon corresponding to that group and choose **Audit Trail**.
-

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, Cisco EPN Manager sends an e-mail to all users with Admin privileges, 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**, and click the **Job Approval** link at the top-right corner of the window.

- 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.

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** checkbox. Enabling this checkbox lets you choose from Job Type Order list. Choose the required option.
- Step 3** Check the **Enable Mail for Job Approval** checkbox. By default this checkbox is unchecked. Enter the email addresses of the job approvers.
- Step 4** Click **Save**.
-

Configure Global Password Policies for Local Authentication

If you are using local authentication (Cisco EPN Manager authentication mechanism), you control the global password policies from the web GUI. If you are authenticating Cisco EPN Manager users using external authentication, the policies are controlled by an external application (see [Set Up External Authentication Using the 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 > AAA**, choose **Settings**, and expand the **Local Password Policy** drop-down.



Note You must select the **Change password** on the first login check box to prompt the new users to change the default password on their initial login to Cisco EPN Manager. Deselecting this checkbox launches the Home Dashboard page on logging in.

Configure Number of Parallel Sessions Allowed



Note This setting applies only to the sessions logged in from the Cisco EPN Manager web-interface.

-
- Step 1** Choose **Administration > Settings > System Settings**, then choose **General > Server**.
- Step 2** Under **Parallel Sessions**, enter a value between 1 and 15 in the **Number of parallel sessions allowed** field.

Step 3 Click **Save**. You need to restart the system for this change to take effect.

Configure the Global Timeout for Idle Users

Cisco EPN Manager provides 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.

The Idle Timeout feature starts functioning when the browser is open, but there is no user interaction. It means that, if the idle timeout is 10 minutes and the browser is open and user does not have any key strokes or mouse clicks, then the user will be logged out after 10 minutes of inactivity. However, if the browser is killed without logging out from Cisco EPN Manager, by default, the session expires in 60 minutes regardless of the idle timeout value set in Cisco EPN Manager.

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 31](#).

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 must log out and log back in for this change to take effect.

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 [Configure the Global Timeout for Idle Users, on page 31](#).


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 must 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 must log out and log back in for this change to take effect.

Create Virtual Domains to Control User Access to Devices

- [What Are Virtual Domains?, on page 32](#)
- [How Virtual Domains Affect Cisco EPN Manager Features, on page 33](#)
- [Create New Virtual Domains, on page 34](#)
- [Import a List of Virtual Domains, on page 35](#)
- [Add Network Devices to Virtual Domains, on page 36](#)
- [Assign Virtual Domains to Users, on page 37](#)
- [Export the Cisco EPN Manager Virtual Domain Attributes for RADIUS and TACACS+, on page 38](#)
- [Edit a Virtual Domain, on page 37](#)
- [Delete a Virtual Domain, on page 37](#)

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 Cisco EPN Manager. Each virtual domain must have a name and can have an optional description, email address, and time zone. Cisco EPN Manager 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 (see [Work In a Different Virtual Domain](#)).

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 Cisco EPN Manager 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, on page 33](#)
- [Search and Virtual Domains, on page 33](#)
- [Alarms and Virtual Domains, on page 33](#)
- [Maps and Virtual Domains, on page 34](#)
- [Configuration Templates and Virtual Domains, on page 34](#)
- [Config Groups and Virtual Domains, on page 34](#)
- [Email Notifications and Virtual Domains, on page 34](#)

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 Cisco EPN Manager, 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 Cisco EPN Manager 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, Cisco EPN Manager 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 (<i>new-domain</i>) here:	See this procedure:
ROOT-DOMAIN > <i>new-domain</i>	Create Virtual Domains Directly Under ROOT-DOMAIN, on page 35
ROOT-DOMAIN > <i>existing-domain</i> > <i>new-domain</i>	Create Child Virtual Domains (Sub-domains), on page 35
ROOT-DOMAIN > <i>existing-domain</i> > <i>existing-domain</i> > <i>new-domain</i>	
(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 35](#).

If a virtual domain exists under ROOT-DOMAIN, and you want to create a new domain under it (a child domain), see [Create Child Virtual Domains \(Sub-domains\), on page 35](#).

-
- Step 1** Choose **Administration > Users > Virtual Domains**.
 - Step 2** In the Virtual Domains sidebar menu, click the *i* (info) icon and click **Create Sub Domain**.
 - Step 3** Enter the name and description for the domain.
 - Step 4** 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 36](#).

Create Child Virtual Domains (Sub-domains)

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 35](#).

-
- 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.)
 - b) Click the information (**i**) icon next to the domain name. This opens a data popup window.
 - c) In the popup window, click **Add a Sub Domain**. The navigation pane switches to the list view, with the parent domain displayed above the child domain named **Untitled**.
 - Step 3** Enter a name in the **Name** text box. The name in the navigation pane will change from **Untitled** to the **child domain name** after you save the new child domain.
 - Step 4** (Optional) Add a description.
 - Step 5** Click **Create** and confirm the creation of the new child domain.
-

What to do next

Add devices to the virtual domain as described in [Add Network Devices to Virtual Domains, on page 36](#).

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 36](#).

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 the **Add** icon from the left-pane.
 - Step 4** You can either add network devices by group or add a network device to a specific location group.
 - Step 5** To add devices from groups, select the **Groups** tab, click **Add**, and the **Add Group** pop-up appears, which lists the applicable location and user-defined groups. Select the group to add the device and click **Select** to add the groups to the Selected Network Devices by Group table.
 - Step 6** To add individual devices, select the **Network Devices** tab, 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 7** 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.
 - Note** Select Network Devices dialog lists all managed devices, not only those that are in the parent domain. If you add a device that is not included in the parent domain, Cisco EPN Manager adds it to the child and parent domain.
 - Note** You cannot add more than 500 network devices in a single shot using **Select All** function. To add more than 500 devices, use the **Filter By** option multiple times.
 - Step 8** Click **Submit** to view the summary of the virtual domain contents.
 - Step 9** 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 37](#).

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 Cisco EPN Manager Virtual Domains with RADIUS and TACACS+, on page 38](#).

-
- Step 1** Choose **Administration > Users > Users and Roles > Users**.
- Step 2** Select the user to grant device access. Click the  icon, which opens the Edit User window.
- Step 3** From the **Virtual Domains** space, add or remove domains by checking or unchecking the checkboxes, and 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 36](#).
 - To delete devices, select the devices using their check boxes, then click **Delete**.
- Step 5** Click **Save** to apply and save your changes.
-

Delete a Virtual Domain

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

Before you begin

You can only delete a virtual domain if:

- It is not the only domain a user can access. In other words, if a Cisco EPN Manager 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 Cisco EPN Manager Virtual Domains with RADIUS and TACACS+

Your RADIUS or TACACS+ servers must be configured to recognize the virtual domains that exist in Cisco EPN Manager. You can do this using the procedure in [Export the Cisco EPN Manager Virtual Domain Attributes for RADIUS and TACACS+](#), on page 38 .

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 Cisco EPN Manager:

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

Export the Cisco EPN Manager Virtual Domain Attributes for RADIUS and TACACS+

If you are using RADIUS or TACACS+, you must copy all Cisco EPN Manager virtual domain information into your Cisco ISE server. You can do this using the Virtual Domains Custom Attributes dialog box that is provided in the web GUI. If you do not export the data into your Cisco ISE server, Cisco EPN Manager 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 40.

Step 1

In Cisco EPN Manager:

- 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 the text* in the TACACS+ Custom Attributes field and choose **Copy**.

Step 2

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

- [Use Cisco ISE With RADIUS or TACACS+ for External Authentication](#) , on page 42

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

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

- a) For the applicable user or group, click **Edit Settings**.
- b) Paste the attributes list into the appropriate text box.
- c) Select the check boxes to enable these attributes, then click **Submit + Restart**.

Configure Local Authentication

Cisco EPN Manager uses local authentication by default, which means that user passwords are stored and verified from the Cisco EPN Manager database.

To check the authentication mode:

SUMMARY STEPS

1. Choose **Administration > Users > AAA > Settings**. The selection is displayed on the **AAA Mode Settings** page. If you are using local authentication, make sure to configure password policies. See [Configure Global Password Policies for Local Authentication](#), on page 30.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Choose Administration > Users > AAA > Settings . The selection is displayed on the AAA Mode Settings page. If you are using local authentication, make sure to configure password policies. See Configure Global Password Policies for Local Authentication , on page 30.	If you want to use SSO with local authentication, see Use SSO With Local Authentication , on page 40. For information on external authentication, see .

Use SSO With Local Authentication

To use SSO with local authentication, you must add the SSO server and then configure Cisco EPN Manager to use SSO in local mode.

If you have deployed Cisco EPN Manager in a high availability environment where you have a primary and backup server, refer to the instructions in [Configure an SSO Server in an HA Environment](#).

Cisco EPN Manager 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 Cisco EPN Manager server, choose **Local** mode (not RADIUS or TACACS+).

- [Add the SSO Server, on page 48](#)
- [Configure SSO Mode on the Cisco EPN Manager Server, on page 48](#)

Configure External Authentication

Users with web GUI root user or Super User privileges can configure the Cisco EPN Manager 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 Cisco EPN Manager 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.



Note You can use up to three AAA servers together, only if they support the same RADIUS, TACACS+ or LDAP protocol. Using servers having different protocols together is not supported. However, if you want to use multiple AAA servers running different protocols, then you must use Cisco ISE as a proxy between Cisco EPN Manager and the AAA servers. In this case, you need to set up your authentication logic based on the Cisco ISE configurations.

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](#)
- [Use Cisco ISE With RADIUS or TACACS+ for External Authentication](#)
- [Use SSO with External Authentication](#)

Use RADIUS or TACACS+ for External Authentication





These topics explain how to configure Cisco EPN Manager to use RADIUS or TACACS+ servers.

- [Add a RADIUS or TACACS+ Server to Cisco EPN Manager, on page 41](#)

- [Configure RADIUS or TACACS+ Mode on the Cisco EPN Manager Server, on page 41](#)

Add a RADIUS or TACACS+ Server to Cisco EPN Manager

To add a RADIUS or TACACS+ server to Cisco EPN Manager:

-
- Step 1** Choose **Administration** > **Users** > **AAA**, then choose **Servers**. From this window, you can add, edit settings, and delete a new RADIUS/TACACS+ server.
- Step 2** Select the type of server that you want to add.
- For RADIUS, click the **RADIUS** tab. Click the  icon.
 - For TACACS+, click the **TACACS+** tab. Click the  icon.
- Step 3** Enter the required information—IP address, DNS Name, and so forth. For Cisco EPN Manager to communicate with the external authentication server, the shared secret entered 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. Enter the Retransmit Timeout and the Retries.
- Step 4** Select the authentication type.
- PAP—Password-based authentication protocol requires two entities to share a password in advance and use the password for authentication.
 - CHAP—Challenge-Handshake Authentication Protocol requires the client and server to 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** Click **Test** to check the connectivity of the AAA server. The connectivity test passes only if the port, authentication type, and shared key that you have entered match the TACACS or RADIUS server.
- Step 6** Click **Save**.
- Step 7** To edit a RADIUS/TACACS+ server:
- a) Click the checkbox next to the RADIUS/TACACS+ server and click . After making changes, click **Save**.
- Step 8** To delete a RADIUS/TACACS+ server:
- a) Click the checkbox next to the RADIUS/TACACS+ server and click . The Delete dialog box opens. Click **Delete** to confirm.
-

Configure RADIUS or TACACS+ Mode on the Cisco EPN Manager Server

-
- Step 1** Choose **Administration** > **Users** > **AAA**, then choose **Settings**.
- Step 2** Select **TACACS+** or **RADIUS**.
- Step 3** Select the **Fallback to Local** checkbox to enable the use of the local database when the external AAA server is down.
- Step 4** If you want to revert to local authentication when the external RADIUS or TACACS+ server goes down, perform the following steps:

- a) Select **Fallback to Local**.
- b) Specify the fallback conditions:
 - **Only on no server response**—only when the external server is unreachable or has network problems. If you select this option, you can login as an AAA user only.
 - **On authentication failure or no server response**—either when the external server is unreachable, or has network problems, or the external AAA server cannot authenticate the user. If you select this option, you can login as a local user and an AAA user.

Step 5 Click **Save All Changes**.

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 Cisco Evolved Programmable Network Manager with Cisco ISE to authenticate the Cisco Evolved Programmable Network Manager 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.



Note Cisco Evolved Programmable Network Manager natively supports LDAP.

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 Cisco Evolved Programmable Network Manager, on page 43
Add Cisco Evolved Programmable Network Manager as an AAA client in Cisco ISE	Add Cisco Evolved Programmable Network Manager as a Client in Cisco ISE, on page 44
Create a user group in Cisco ISE	Create a User Group in Cisco ISE, on page 44
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 44

(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 Cisco Evolved Programmable Network Manager 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 45
(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 Cisco Evolved Programmable Network Manager 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 46
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 in Cisco ISE, on page 43
Create an authentication policy to define the protocols that Cisco ISE must use to communicate with Cisco Evolved Programmable Network Manager, and the identity sources that it uses for authenticating users to Cisco Evolved Programmable Network Manager	Create an Authentication Policy in Cisco ISE, on page 47
Add Cisco ISE as a RADIUS or TACACS+ server in Cisco Evolved Programmable Network Manager	
Configure the RADIUS or TACACS+ mode on the Cisco Evolved Programmable Network Manager server	Configure RADIUS or TACACS+ Mode on the Cisco EPN Manager Server, on page 41

Supported Versions of Cisco ISE in Cisco Evolved Programmable Network Manager

Cisco Evolved Programmable Network Manager supports Cisco ISE 1.x and 2.x releases .

Configure an Authorization Policy 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 Cisco EPN Manager 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 Cisco EPN Manager-System Monitoring-Group and choose this group from the Identity Groups drop-down list. Similarly, define an authorization profile as Cisco EPN Manager-System Monitoring-authorization profile and choose this profile from the Permissions drop-down list. Now, you have defined a rule where all users belonging to the Cisco EPN Manager System Monitoring identity group receive an appropriate authorization policy with system monitoring custom attributes defined.
- Step 5** Click **Done**, and then click **Save**.
-

Add Cisco Evolved Programmable Network Manager 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 Cisco Evolved Programmable Network Manager 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 Cisco Evolved Programmable Network Manager.

- 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 Cisco Evolved Programmable Network Manager.



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 Cisco Evolved Programmable Network Manager custom attributes for RADIUS. You will need to add this information to Cisco ISE in this procedure.

- Cisco Evolved Programmable Network Manager user roles and tasks—see [Export the Cisco EPN Manager User Group and Role Attributes for RADIUS and TACACS+, on page 24](#)
- Cisco EPN Manager virtual domains—see [Export the Cisco EPN Manager Virtual Domain Attributes for RADIUS and TACACS+, on page 38](#)

-
- 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.

Step 8 Click **Submit**.

Create an Authorization Profile for TACACS+ in Cisco ISE

You can 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, tasks, and virtual domains created in Cisco Evolved Programmable Network Manager.

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:

Before you begin

Make sure you have the complete list of the following Cisco Evolved Programmable Network Manager custom attributes for TACACS+. You will need to add this information to Cisco ISE in this procedure.

- Cisco Evolved Programmable Network Manager user roles and tasks—see [Export the Cisco EPN Manager User Group and Role Attributes for RADIUS and TACACS+](#), on page 24
 - Cisco Evolved Programmable Network Manager virtual domains—see [Export the Cisco EPN Manager Virtual Domain Attributes for RADIUS and TACACS+](#), on page 38
-

- Step 1** Log in to Cisco ISE as the admin user.
- Step 2** Choose **Work Center** > **Device Administration** > **Policy Elements**.
- Step 3** From the left sidebar, choose **Results** > **TACACS Profiles**.
- Step 4** In the **TACACS Profiles** page, click **Add**.
- Step 5** From the **Access Type** drop-down list, choose **ACCESS_ACCEPT**.
- Step 6** In the **TACACS Profiles** page, enter the name and description of the authorization profile.
- Step 7** In the **Raw View Profile Attributes** area, paste in the complete list of TACACS+ custom attributes for:
- User roles, including the tasks
 - Virtual domains

Note Be sure to add the Home Menu Access task. It is mandatory.

Step 8 Click **Submit**.

Configure an Authorization Policy 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 Cisco EPN Manager 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 Cisco EPN Manager-System Monitoring-Group and choose this group from the Identity Groups drop-down list. Similarly, define an authorization profile as Cisco EPN Manager-System Monitoring-authorization profile and choose this profile from the Permissions drop-down list. Now, you have defined a rule where all users belonging to the Cisco EPN Manager System Monitoring identity group receive an appropriate authorization policy with system monitoring custom attributes defined.
- Step 5** Click **Done**, and then click **Save**.
-

Create an Authentication Policy in Cisco ISE

Authentication policies define the protocols that Cisco ISE uses to communicate with Cisco EPN Manager, and the identity sources that it uses for authenticating users to Cisco EPN Manager. 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 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 48](#)
- [Delete SSO Server, on page 48](#)
- [Configure SSO Mode on the Cisco EPN Manager Server, on page 48](#)

Cisco EPN Manager does not support localization on the SSO sign-in page.

Add the SSO Server

If you have deployed Cisco EPN Manager in a high availability environment where you have a primary and backup server, refer to the instructions in [Configure an SSO Server in an HA Environment](#).


Cisco EPN Manager can be configured with a maximum of three AAA servers.

- Step 1** Choose **Administration > Users > AAA**, then choose **Servers**. Select the **SSO** tab. From this window, you can add, edit settings, and delete a new SSO server.
- Step 2** Click the  icon.
- Step 3** Enter the SSO information. The maximum number of server retries for an SSO server authentication request is nine.
- Step 4** Click **Save**.

Note You can also add the Cisco EPN Manager server you are using as an SSO server. To add, select the **Add self as SSO** checkbox.

Delete SSO Server

You can delete the SSO server that is added to Cisco EPN Manager. To delete the SSO server:

- Step 1** Choose **Administration > Users > AAA**, then choose **Servers**. Select the **SSO** tab.
- Step 2** Select the servers that you want to delete.
- Step 3** Click the checkbox next to the SSO server and click . The Delete dialog box opens. Click **Delete** to confirm.

Configure SSO Mode on the Cisco EPN Manager Server

The SSO functionality distributes CA certificate when the SSO server is added to the SSO client.

Cisco EPN Manager supports CA and self-signed certificates as long as the Common Name (CN) field of the certificate contains the Fully Qualified Domain Name (FQDN) of the server on the SSO client and SSO server. The server must be capable of name resolution from the IP address to FQDN. In addition, the hostname must match the left-most component of the FQDN. SSO requires accurate DNS configuration. You must define the DNS with fully qualified domain name (FQDN). For example, the nslookup command and expected data when configuring DNS with FQDN is:

```
hostname CUSTOMER_HOSTNAME
nslookup CUSTOMER_HOSTNAME
Server:...
Address:...
Name: CUSTOMER_HOSTNAME.example.com
Address:....
```

For SSO operation, Cisco EPN Manager requires that the SSL/TLS certificate holds the FQDN in the CN field. To verify that the certificate used by your Cisco EPN Manager server has the FQDN in the CN field, use your browser to view the certificate. If the certificate does not contain the FQDN in the CN field, you must regenerate the certificate and redistribute it to all users that have the old certificates.



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 > AAA**, then choose **SSO Settings**.
 - Step 2** Choose which **SSO Server AAA Mode** you want to use. You can select only one at a time.
 - Step 3** Select/de-select **Enable Single Sign-Out** checkbox.
 - Step 4** Choose a time span from the **Ticket Granting Ticket Timeout** drop-down.
 - Step 5** Click **Save All Changes**.
-

