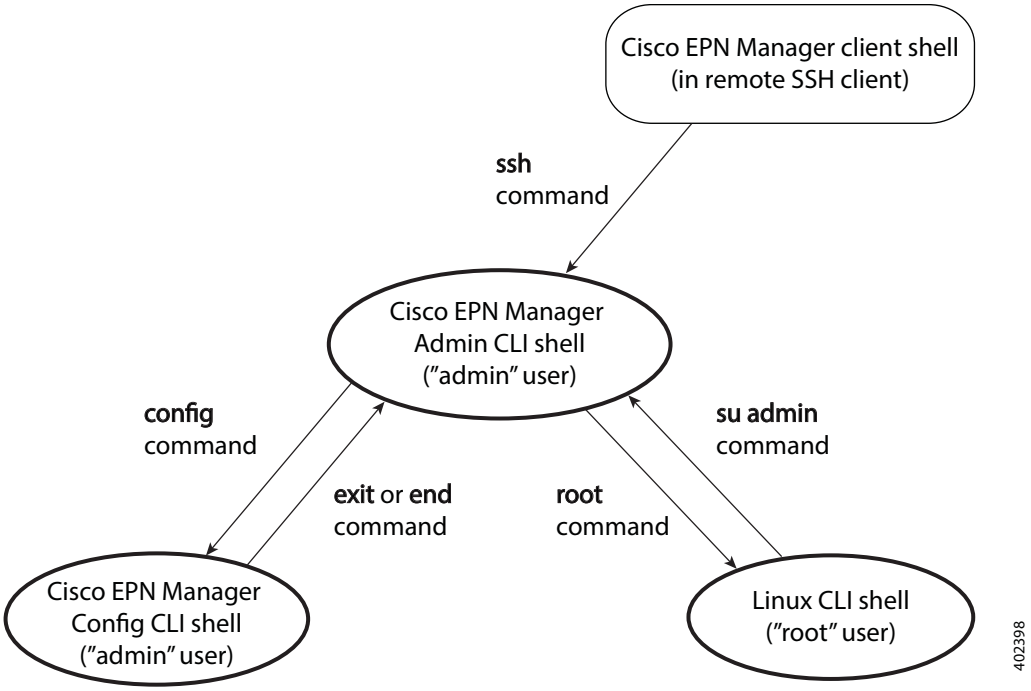
User Permissions and Device Access

Cisco EPN Manager User Interfaces and Transitioning Between Them

The Cisco EPN Manager application provides multiple user interfaces:

- Cisco EPN Manager web GUI—A web interface that facilitates day-to-day user and administration operations. This interface provides a subset of all operations that are provided by the Admin and Config CLI. You can use this interface if you have a web user account. Different kinds of web users are explained in Control the Actions Users Can Perform.
- Cisco EPN Manager 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 provides commands for advanced Cisco EPN Manager system administration tasks. These commands are explained throughout this guide. To use this, you must have admin user access (see Types of Users in Cisco EPN Manager). You can access this shell from a remote computer using SSH.
- Cisco EPN Manager Config CLI—Cisco proprietary shell which is restricted and more secure than the Linux shell. This Config shell and CLI provides commands for Cisco EPN Manager system configuration tasks. These commands are explained throughout this guide. To use this, you must have admin or other similar user access. You can access this shell from the Admin CLI shell.
- Linux CLI—Linux shell which provides all Linux command. The Linux shell should only be used by Cisco technical support representatives. Regular users with system administrators should not use the Linux shell. To use this, you must have Linux root user access. You cannot reach this shell from a remote computer using SSH; you can only reach it through the Cisco EPN Manager Admin shell and CLI. This shell is disabled by default for increased security.

The following figure illustrates how you can transition between these interfaces.



Transition Between Cisco EPN Manager admin CLI and Cisco EPN Manager config CLI

To move from the admin CLI to the 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)#
```

Transition Between Cisco EPN Manager admin CLI and Linux CLI

You may need to enable the Linux root; see Enable and Disable root Access for the CLI and Web GUI.

To move from the admin CLI to the Linux CLI, enter **root** at the admin prompt.

```
(admin)# root
#
```

To move from the Linux CLI back to the admin CLI, enter **su admin** at the Linux root prompt:

```
# su admin
(admin)#
```

LIMITED ORDERABILITY RELEASE

Types of Users in Cisco EPN Manager

Cisco EPN Manager User	Description
Cisco EPN Manager web GUI everyday users	Created by the Cisco EPN Manager web GUI root user for day to day operations using the web GUI. These users can having varying degrees of privileges and are often classified into role-based access control (RBAC) classes and subclasses. For more information, see View Cisco EPN Manager User Groups and Members.
Cisco EPN 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 Cisco EPN Manager web GUI user that has root privileges—that is, a web GUI user that belongs to the **root** user group. See Enable and Disable root Access for the CLI and Web GUI. **Note** This user is not the same as the Linux CLI root user.
Cisco EPN Manager CLI admin user	Created at installation and used for administration operations such as stopping and restarting the application and creating remote backup repositories. (A subset of these administration operations are available from the web GUI). To display a list of operations this user can perform, enter **?** at the prompt. Some tasks must be performed in config mode. To transition to config mode, use the procedure in Transition Between Cisco EPN Manager admin CLI and Cisco EPN Manager config CLI.
Cisco EPN Manager CLI users	Created by Cisco EPN Manager CLI admin user for a variety of reasons, using the following command: `(config) username username password role {admin | user} password` These users may have admin-like privileges or lower level privileges as defined during creation time. (There are variations of this **username** command.)
Linux CLI root user	Created at installation and used only by Cisco Support teams to debug product-related operational issues. This user should be disabled after installation and/or after Linux CLI operations are completed (see Enable and Disable root Access for the CLI and Web GUI).

LIMITED ORDERABILITY RELEASE

Enable and Disable root Access for the CLI and Web GUI

As described in Cisco EPN Manager User Interfaces and Transitioning Between Them, after installation, you should disable the following two accounts for security purposes:

- Linux CLI root user. Instead, use the Cisco EPN Manager admin CLI user to perform administration tasks using the Cisco EPN Manager CLI.
- Cisco EPN Manager web GUI **root** user. You should disable this account after creating at least one other web GUI user that has root privileges.

Disable and Enable the Linux CLI root User

Step 1 Log in to Cisco EPN Manager as the Cisco EPN Manager CLI admin user. See Establish an SSH Session With the Cisco EPN Manager Server.

Step 2 Disable the Cisco EPN Manager CLI root user account.

```
(admin)# root_disable
```

If you need to re-enable the account at a later time, use the following command:

```
(admin)# root_enable
```

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 **root** user group. See Add Users and Manage User Accounts. 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.)

```
(admin)# ncs webroot disable
```

If you need to re-enable the account at a later time, use the following command:

```
(admin)# ncs webroot disable
```

LIMITED ORDERABILITY RELEASE

Control the Actions Users Can Perform

View Cisco EPN Manager User Groups and Members

The actions Cisco EPN Manager users can perform are determined by the user group they belong to. Cisco EPN Manager provides a default set of user groups that contain the common tasks for network management user types—for example, Admin, Config Manager, System Monitoring, and so forth. To view these groups, choose **Administration > Users, Roles & AAA> User Groups**.

Each group has a predefined set of tasks, some of which are enabled and others which are disabled. Because most user groups are editable, you can adjust these settings according to your deployment's needs. See User Groups Reference for information on the tasks that pertain to each user group, along with the default settings.

Users can belong to multiple groups. However, there are a few groups that are special, meaning that if a user is assigned to that group, they cannot belong to any other group. One example is Monitoring Lite, which provides a very limited set of privileges.

Cisco EPN Manager also provides four user-defined groups which have no predefined settings. If you have a user type that does not match any of the predefined groups, create a user-defined group. You can pick and choose the exact privileges you want the group to have.

To view the members, click the group name, then click the **Members** tab.

The following tables describe the user groups provided by Cisco EPN Manager, which can be managed from the web GUI.

- User Groups—Web UI
- User Groups—NBI

User Groups—Web UI

Cisco EPN Manager provides the default web GUI user groups listed in Table 23-1. Users can belong to multiple web GUI user groups with the following exceptions:

- If a user is assigned to the User Assistant or Monitor Lite user groups, they cannot belong to any other user groups.
- A user cannot belong to a web GUI user group and an NBI user group.

See User Groups Reference for information on the tasks that pertain to each user group, along with the default settings.

Table 23-1 Cisco EPN Manager Web User Groups

Group Name	Group Task Focus
Root	All operations. Not editable. This Web GUI root user is available after installation and is described in Types of Users in Cisco EPN Manager. You should create other users that belong to this group.
Super Users	All operations (like root), but the tasks assigned to this group can be edited.
Admin	Administer the system and server. Can also perform monitoring and configuration operations. This user group is editable.
Config Managers	Configure and monitor the network (no administration tasks). This user group is editable.
System Monitoring	Monitor the network (no configuration tasks). This user group is editable.
User-Defined 1 - 4	Customizable. These groups can be edited and customized as needed.
User Assistant	User account creation. **Note** This group is not editable (you cannot customize the privileges), and members of the User Assistant group cannot belong to any other user group.
Monitor Lite	View network topology and use tags. **Note** This group is not editable (you cannot customize the privileges), and members of the User Assistant group cannot belong to any other user group.

User Groups—NBI

Cisco EPN Manager provides the default NBI user groups listed in Table 23-2. Users can belong to multiple NBI user groups with the following exceptions:

- A user cannot belong to an NBI user group and a web GUI user group.
- Users that are assigned to the North Bound API user group cannot belong to any other user groups.

Table 23-2 Cisco EPN Manager NBI User Groups

Group Name	Group Task Focus	Can members belong to other groups?
NBI Credential	Manage credentials using the NBI. This user group is not editable.	A user can belong to all (or a combination of) the NBI user groups. Members of the North Bound API group cannot belong to any non-NBI groups.
NBI Read	Perform NBI read operations (HTTP GET). This user group is not editable.	
NBI Write	Perform NBI write operations (HTTP PUT, POST, DELETE). This user group is not editable.	
North Bound API	Only access NBI (no UI access). This group is not editable. **Note** Members of the North Bound API group cannot belong to any other user group.	

Check and Adjust the Groups A User Belongs To

To find out which groups a user belongs to, choose **Administration > Users, Roles & AAA > Users**. Cisco EPN Manager lists all configured users with their status.

The Member of column lists all groups the user belongs to. To adjust the groups a user belongs to:

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

Step 2 Click the hyperlinked user name.

Step 3 Under the General tab, check and uncheck the user groups as needed, then click **Save**.

To check and adjust device access, see Assign and Unassign Virtual Domains from a User Account.

Check and Adjust the Tasks a User Group Can Perform

To check the tasks a group can perform, choose **Administration > Users, Roles & AAA> User Groups**. and click the group name. Greyed-out check boxes indicate settings that cannot be changed.

Note When you edit an existing group, the changes are applied to all of the group members.

To customize the task settings for a user group:

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

Step 2 Click the name of the group you want to customize.

Step 3 Adjust the permissions by checking and unchecking tasks. Remember that not all groups are editable (see View Cisco EPN Manager User Groups and Members).

Step 4 Click **Submit**. The changes are immediately applied to all group members.

User Groups, RADIUS, and TACACS

When you choose **Administration > Users, Roles & AAA> User Groups**, each group is listed with a Task List hyperlink. Use the hyperlink to synchronize permissions with RADIUS and TACACS authentication servers. For RADIUS and TACACS, when adding the user tasks in the ACS server, be sure to add the **Home Menu Access** task. It is mandatory.

Add Users and Manage User Accounts

- Create Web GUI Users with Administrator Privileges
- Add and Delete User Accounts
- Disable (Lock) a User Account
- Change a User's Password

Create Web GUI Users with Administrator Privileges

After installation, Cisco EPN Manager has a web GUI root account. This web GUI root user account is used for first-time login to the server. Do not use this account for normal operations. Instead, used it to create:

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

By default, the web root user will have access to all devices because the ROOT-DOMAIN virtual domain is automatically assigned to the account. (While user accounts control the actions a user can perform, virtual domains control the devices a user can access. For more information about virtual domains, see Control User Access to Devices Using Virtual Domains.

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

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

Step 3 Complete the required fields.

Step 4 Under Groups Assigned to This User, click **Admin**.

Step 5 Click **Save**.

LIMITED ORDERABILITY RELEASE

Add and Delete User Accounts

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

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

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

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

Step 3 Configure the user account.

a. Enter a username and password.

b. Control the actions the user can perform by selecting one or more user groups. For descriptions of user groups, see View Cisco EPN Manager User Groups and Members.

c. Control the devices a user can access, click the Virtual Domains tab and assign domains to the user. (see Control User Access to Devices Using Virtual Domains).

Step 4 Click **Save**.

To delete a user account, select a user, then choose **Delete User** from the Select a command drop-down list.

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 User Accounts.

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

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

Step 3 Choose **Select a command > Lock User(s)**, then click **Go**.

To unlock the account, repeat this procedure but choose **Select a command > Unlock User(s)**.

LIMITED ORDERABILITY RELEASE

Change a User's Password

In some cases you may want to force a user to change their password. You can enforce this through password rules (see Configure Global Password Policies for Local Authentication), or simply change their password yourself.

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

Step 2 Select the user whose password you want to change.

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

View User and User Group Audits and Active User Sessions

Check a System-Wide Users Audit

The System Audit page lists user actions that are related to product features—for example, when a user logged in, the pages they visited, and the actions they performed. You can use the search facility to list actions by user, IP address, virtual domain, and user group, among other criteria. To view this information, choose **Administration > Settings > System Audit**.

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

Check a User Group Audit

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

Step 2 Click the Audit Trail icon corresponding to the user group name for which you want to see the audit data. The Configuration Changes field provides a Details link if there are any configuration changes. Click the Details link for more information on the configuration changes done by an individual user.

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

Check a User Audit

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

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

Step 2 Click the Audit Trail icon corresponding to the user group name for which you want to see the audit data. The Configuration Changes field provides a Details link if there are any configuration changes. Click the Details link for more information on the configuration changes done by an individual user.

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

Configure Global User Permissions (Jobs, Timeouts, Password Policies)

Configure Job Approvers

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 Administrator privileges and does not run the job until one of the users approves it. By default, all jobs do not require approval.

To configure job approval:

Step 1 Choose **Administration > Settings > System Settings > Job Approval Settings**.

Step 2 Check the Enable Job Approval check box.

Step 3 Find the jobs you want to configure for approval, and move them from the left field to the right field. For example, if you want an Administrator user to approve adding new devices, move the Import job type.

Step 4 To specify a customized job type, enter a string using regular expressions in the Job Type field, then click **Add**. For example, to enable job approval for all job types that start with Config, enter **Config.***.

Step 5 Click **Save**.

Configure Session Timeouts for Idle Users

For security purposes, client sessions are disabled after 15 minutes of inactivity. Cisco EPN Manager allows you to configure individual and global timeouts. Individual users can adjust their own timeout, but it cannot exceed the global setting.

To check or change these settings, choose **Administration > User Preferences**.

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

If you change a setting, it is immediately applied when you click **Save**.

Configure Global Password Policies for Local Authentication

If you are using local authentication (Cisco EPN Manager's authentication mechanism), you control the global password policies. If you are authenticating Cisco EPN Manager users using external authentication, the policies must be configured from the external application.

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

Control User Access to Devices Using Virtual Domains

What Are Virtual Domains?

Virtual domains are logical groupings of devices and are used to control who has access to specific sites and devices. 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.

The e-mail address and time zone that you specify in the Virtual Domains page (**Administration > Virtual Domains**) are used when scheduling and e-mailing domain specific reports. The scheduled time of the report can be set to the time zone specific to the virtual domain and the scheduled report can be e-mailed to the e-mail address specified for the virtual domain. For more information.

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

LIMITED ORDERABILITY RELEASE

How Virtual Domains Affect Cisco EPN Manager Features

Virtual domains are organized hierarchically. Parent domains contain all elements that are in the child domains. The “ROOT-DOMAIN” domain includes all virtual domains.

Reports

Report results are filtered according to the viewer’s assigned virtual domains. If new components are added to a viewer’s assigned domain, the new components are only displayed in reports executed after the component was added.

Reports are only visible in the current virtual domain. The parent virtual domain cannot view the reports from its subvirtual domain.

Search

Search results are filtered according to the viewer’s assigned virtual domains. If new components are added to a viewer’s assigned domain, the new components are only displayed in searches executed after the component was added.

The saved searches are only visible in the current virtual domain. The parent virtual domain cannot view these search results.

Alarms

Alarms are filtered according to the viewer’s assigned virtual domains. Alarms that occurred before the component was added to the domain are not displayed in the alarm history.

Note Alarm E-Mail Notifications—Only the ROOT-DOMAIN virtual domain can enable Location Notifications, Location Servers, and Cisco EPN Manager email notification.

Templates

When you create or discover a template in a virtual domain, it is only available to that virtual domain.

Note If you create a subvirtual domain and then apply a 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

Config groups in a virtual domain can also be viewed by the parent virtual domain. A parent virtual domain can modify config groups for a sub (child) virtual domain.

E-Mail Notification

E-Mail notification can be configured per virtual domain. An e-mail is sent only when alarms occur in that virtual domain.

RADIUS and TACACS+

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

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

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

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

Step 3 Click **Export**.

Step 4 Highlight the text in the RADIUS or TACACS+ Custom Attributes list (depending on which one you are currently configuring), go to your browser menu, and choose **Edit > Copy**.

Step 5 Log in to ACS.

Step 6 Navigate to User or Group Setup.

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

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

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

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

Create and Edit Virtual Domains

When you create a virtual domain, you can leverage the device groupings that already exist—for example, devices that are grouped by device type or location. Those device groupings do not apply any access control.

For example, say Cisco EPN Manager has a device group named *Cisco ASR 9000 Series Aggregation Services Routers* with five Cisco ASR 9000 routers in it. To apply role-based access control to the group, add it to a virtual domain.

Note For TACACS+/RADIUS+ users: If more than one virtual domain exists, make sure a domain is specified in the custom attributes fields in the TACACS+/RADIUS server. Otherwise Cisco EPN Manager will not allow the user to log in. (If no domains exist, the user is assigned the ROOT-DOMAIN.)

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

Step 2 Click the Add New Domain icon.

Step 3 Enter a name that represents the domain (for example, San Jose or ASR 9000), and click **Submit**.

Step 4 Select the devices you want to add to the domain.

a. In the Select Network Devices pop-up, select the devices you want to add to the virtual domain. You can:
   - Filter the devices according to existing device groups using the Filter By drop-down list.
   - Search for specific devices by entering a string in the Search field.

   For very long lists, you can further minimize the results using the Quick Filter box (by entering a string).

b. Check the devices you want to add and click **OK**. For existing domains, you can select and unselect devices.

Step 5 Create the virtual domain by clicking **Submit**.

To edit an existing domain, choose **Administration > Virtual Domains**, select the domain from the navigation pane, and make the necessary changes.

Assign and Unassign Virtual Domains from a User Account

Once a virtual domain is assigned to a user, 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.

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

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

Step 3 Click the Virtual Domains tab.

Step 4 Make your changes using the Add and Remove buttons, then click **Save**.

Adjust and Delete Virtual Domains

Choose a virtual domain from the Virtual Domain Hierarchy on the left sidebar menu to view or edit its assigned network devices. After assigning elements to a virtual domain and submitting the changes, Cisco EPN Manager might take some time to process these changes, depending on how many elements are added.

If you delete a device from the ROOT-DOMAIN, the device is removed from Cisco EPN Manager.

LIMITED ORDERABILITY RELEASE

If the device is explicitly associated with the ROOT-DOMAIN or any other virtual domain that is not the child of the current virtual domain and if you delete the device from the current virtual domain, the device is removed from this virtual domain but it is not removed from Cisco EPN Manager.

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

Step 2 Choose a virtual domain hierarchy from the Virtual Domain Hierarchy left sidebar menu.

Step 3 Adjust the members using the Add and Delete buttons, then click **Save**.

Step 4 Click **Save** to confirm the changes.

Configure AAA

Users with web GUI root user or SuperUser privileges can configure Cisco EPN Manager to communicate with external RADIUS, TACACS+, or SSO servers for authentication, authorization, and accounting (AAA). If you have multiple AAA servers, users are authenticated on the second server only if the first server is not reachable or has network problems.

You can also use local AAA, which uses the local database for user information and authentication.

Each group on the User Groups page (**Administration > Users, Roles & AAA> User Groups**) contains a hyperlink to a list of tasks that group can perform. You can use that lists when adding the user tasks in the ACS server. See Check and Adjust the Tasks a User Group Can Perform.

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

See these topics for more information:

- Add the RADIUS, TACACS+, or SSO Server
- Configure AAA Mode

Add the RADIUS, TACACS+, or SSO Server

If your deployment of Cisco EPN Manager is in a high availability environment where you have a primary server and a backup server, refer to the instructions in Configure an SSO Server in High Availability Environment

Cisco EPN Manager can use a maximum of three AAA servers.

Step 1 Choose **Administration > Users, Roles & AAA** and the server type: **RADIUS Servers, SSO Servers, or TACACS+ Servers**.

Step 2 Choose **Select a command > Add** *server-type* **Server**, then click **Go**.

Step 3 Enter the server information.

- For RADIUS and TACACS+: The shared secret you enter on this page must match the shared secret configured on the TACACS+ server. You can use alphabets, numbers, and special characters except ‘ (single quote) and “ (double quote).

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

Configure AAA Mode

Configure Local, TACACS+ or RADIUS

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

Step 2 Select Local, TACACS+, or RADIUS.

Step 3 If you are using TACACS+ and RADIUS and you want to revert to the local database when the external RADIUS or TACACS+ server is down:

a. Select **Enable Fallback to Local**.

b. Specify the fall back conditions:

If you want fallback to the local database:	Choose:
Only when external server is unreachable	**ONLY on no server response**
When external server is unreachable OR when the server cannot authenticate the user	**on authentication failure or no server response**

Step 4 Click **Save**.

Configure SSO

Keep the following in mind if you want to use SSO.

- Because Cisco EPN Manager2014 does not support CA certificates and self-signed certificates in Java, SSO requires accurate DNS configuration. You must define the DNS with fully qualified domain name (FQDN). For example, the **nslookup** command and expected data when configuring DNS with FQDN is:

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

- For SSO operation, Cisco EPN Manager requires that the SSL/TLS certificate hold the fully qualified domain name (FQDN) in the Common Name (CN) field. To verify that the certificate used by your 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.

LIMITED ORDERABILITY RELEASE

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

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

Step 2 Select SSO and click **Save**.

Step 3 Choose **Administration > Users, Roles & AAA > SSO Server Settings**.

Step 4 Choose which SSO Server AAA mode you want to use: Local, RADIUS, or TACACS+.

Note RADIUS requires separate credentials for different locations (East and West Coast). TACACS+ is an effective and secure management framework with a built-in failover mechanism.

Step 5 For RADIUS or TACACS+: If you want to fall back to the local server when the external server is unreachable, select the **Enable Fallback to Local**.

Step 6 Click **OK**.