User Permissions and Device Access

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

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

User Interfaces and User Types

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

CEPNM User Interface	Interface Description	CEPNM User Types
CEPNM web GUI	Web interface that facilitates day-to-day and administration operations using the web GUI. These users can have varying degrees of privileges and are classified into role-based access control (RBAC) classes and subclasses. This interface provides a subset of operations that are provided by the Cisco EPN Manager CLI admin and CLI config users.	**Cisco EPN 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 *user groups* (Admin, Super Users, Config Managers, and so forth). For information on the user groups, see Types of User Groups, on page 4. **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 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. **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.
North Bound Interface (NBI) REST API	NBI is REST Application Programming Interface that allows a client system to talk to CEPNM to carry out day-to-day and administration operations. Special privileged service account users are assigned to a client system to allow talking to CEPNM using this interface. These NBI users can also have varying degrees of privileges and are also classified into role-based access control (RBAC) classes and subclasses.	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 5

CEPNM 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.	**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.) To display a list of operations this user can perform, enter **?** at the prompt. Some tasks must be performed in config mode. To transition to config mode, use the procedure in Transition Between the Cisco EPN Manager admin CLI and Cisco EPN Manager config CLI, on page 3. The admin CLI user can create other CLI users for various reasons, using the following command: `(config) username username password role {admin|user} password` These users may have admin-like privilege/roles or lower-level privileges as defined during creation time. To create a Cisco EPN 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.
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.	
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 Cisco EPN Manager admin shell and CLI.	**Linux CLI admin user**—Created at installation time and used for Linux-level administration purposes.

How to Transition Between the CLI User Interfaces in Cisco EPN 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 EPN Manager admin CLI and Cisco EPN Manager config CLI

To move from the Cisco EPN Manager admin CLI to the Cisco EPN 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 18.

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.

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 5

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).

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–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.

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.

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	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 user 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	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

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
License Check	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
Diagnostic Tasks	Diagnostic Information	Controls access to diagnostic page.
	Unsanitized Device Config Export	Allows user to expose unsanitized Configuration Archive

Task Group Name	Task Name	Description
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.
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 delployed jobs
	Device Config Backup Job Edit Access	Allows user to change the external backup settings such as repository and file encrytion password
	Job Notification Mail	Allows user to configure notification mails for various job types
	Run Job	Allows user to run paused and scheduled jobs
	System Jobs Tab Access	Allows user to view the system jobs
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 defind 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 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
	Configuration Templates Read Access	Allows to access configuration templates in read only mode
	Configure ACS View Servers	Allows acess to manage ACS View Servers
	Configure Config Groups	Allows access to Config Group
	Configure ISE Servers	Allows users to manage ISE servers on Cisco EPN Manager
	Configure Templates	

Task Group Name	Task Name	Description
		Allow the user to do the CRUD operation of Feature Templates and configuration Template
	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
	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.
	Network Devices	Allows user to access to the Network devices
	Network Topology Edit	Allows user to create devices, links and network in the topology map, edit the manually created link to assign the interface
	Provisioning Access	Allows access to Provisioning

Task Group Name	Task Name	Description	
	QoS Profile Configuration Access	Allows user to create, modify, delete QoS profil;es and schedule QoS profiles deployment job or associate/disassociate interface and Import/Export QoS discovered profiles	
	Network Monitoring	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	
Incidents Alarms Events Access		Allows user to access incidents alarms events.	
Latest Config Audit Report		Allows user to view the latest config audit reports	
Network Topology		Allows users to launch the Network Topology map and view the devices and links in the map	
Performance Dashboard Access		Allow user to access the Performance dashboard	

Task Group Name	Task Name	Description
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	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
	Report Run History	Allows user to view report history
	Run Reports List	Allows user to run reports
	Saved Reports List	Allows user to save reports
	System Monitoring Reports	Allows user to view 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	
	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

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**, then click the **Job Approval** link.

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

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

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

Step 3 Find the jobs you want to configure for approval, and move them from the left field to the right field. For example, if you want an Admin 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 Number of Parallel Sessions Allowed

Cisco EPN Manager provides an option to configure the number of parallel sessions that you can run simultaneously. You can configure up to 15 parallel sessions.

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.

Create Virtual Domains to Control User Access to Devices

What Are Virtual Domains?

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

Virtual domains work in conjunction with user groups. Virtual domains control the devices a user can access, while user groups determine the actions a user can perform on those devices. Users with access to a virtual

domain (depending on their privileges) can configure devices, view alarms, and generate reports for the NEs in their virtual domain.

You can create virtual domains after you have added devices to 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 19
- Search and Virtual Domains, on page 19
- Alarms and Virtual Domains, on page 19
- Maps and Virtual Domains, on page 20
- Configuration Templates and Virtual Domains, on page 20
- Config Groups and Virtual Domains, on page 20
- Email Notifications and Virtual Domains, on page 20

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 (*new-domain*) here:	**See this procedure:**
ROOT-DOMAIN > ***new-domain***	Create Virtual Domains Directly Under ROOT-DOMAIN, on page 21
ROOT-DOMAIN > *existing-domain* > ***new-domain***	Create Child Virtual Domains (Subdomains), on page 21
ROOT-DOMAIN > *existing-domain* > *existing-domain* > ***new-domain***	
(etc.)	

Create Virtual Domains Directly Under ROOT-DOMAIN

The following procedure creates an empty virtual domain under ROOT-DOMAIN. You can also create multiple virtual domains at one time by using the procedure in Import a List of Virtual Domains, on page 22.

If a virtual domain already exists under ROOT-DOMAIN, and you want to create a new domain under it (a child domain), see Create Child Virtual Domains (Subdomains), on page 21.

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

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

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

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

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

What to do next

Add devices to the virtual domain as described in Add Network Devices to Virtual Domains, on page 23.

Create Child Virtual Domains (Subdomains)

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

Do not use this procedure if you want the new virtual domain to appear directly under ROOT- DOMAIN. In that case, see Create Virtual Domains Directly Under ROOT-DOMAIN, on page 21.

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

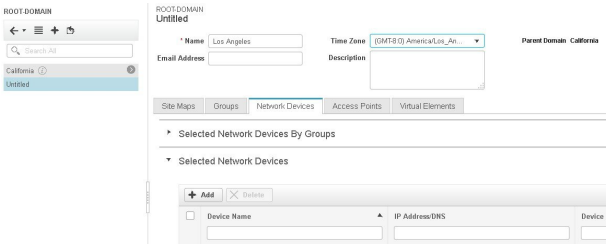
Step 2 In the Virtual Domains sidebar menu:

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

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

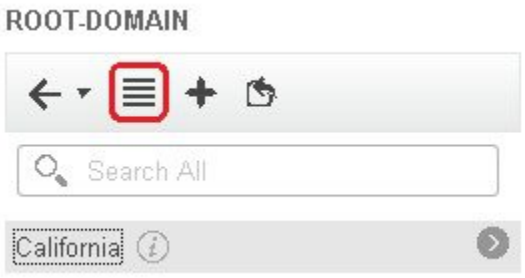
c) In the popup window, click **Create Sub Domain**. The navigation pane switches to the list view, with the parent domain **California** displayed above **Untitled**.

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

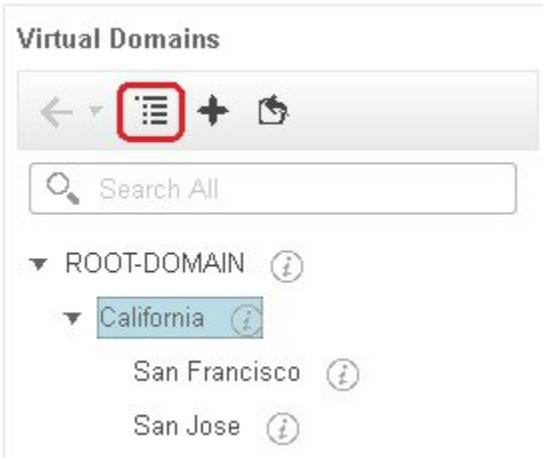


Step 4 (Optional) Enter the new domain's time zone, email address and description.

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



The view reverts to the hierarchical view.



What to do next

Add devices to the virtual domain as described in Add Network Devices to Virtual Domains, on page 23.

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 23.

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 **Network Devices** tab, then click **Add**.

Step 4 Select the network devices you want to add to the domain. Note that the 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 both the child and parent domain.

a) Select the devices you want to add to the domain. You can use the **Filter By** drop-down list to locate the devices you want to add.

b) Click **Select**.

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

Step 6 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.

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 23.
- To delete devices, select the devices using their check boxes, then click **Delete**.

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

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

Delete a Virtual Domain

Use this procedure to delete a virtual domain from 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:

- The virtual domain does not contain any network elements and does not have any child domains.
- It is not the only domain a user can access. In other words, if a 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.