Configuring the Cisco APIC-EM Settings

Logging into the Cisco APIC-EM

Step 1 In your browser address bar, enter the IP address of the Cisco APIC-EM in the following format:

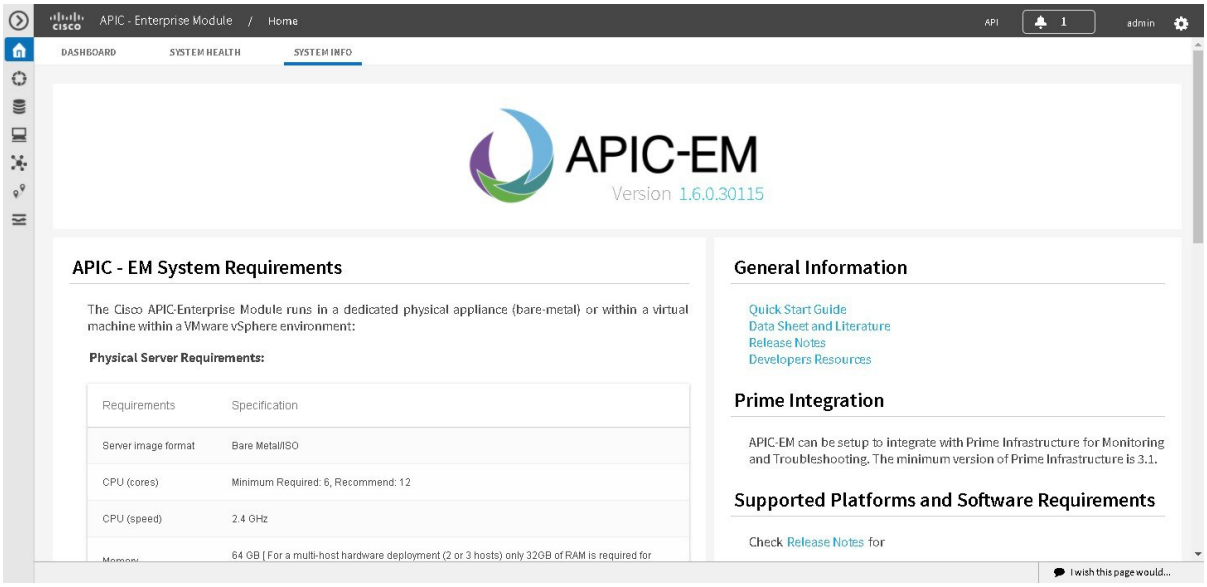
https://*IP address*

Step 2 On the launch page, enter your username and password that you configured during the deployment procedure.

The **Home** page of the APIC-EM controller appears. The **Home** page consists of the following three tabs:

- **DASHBOARD**
- **SYSTEM HEALTH**
- **SYSTEM INFO**

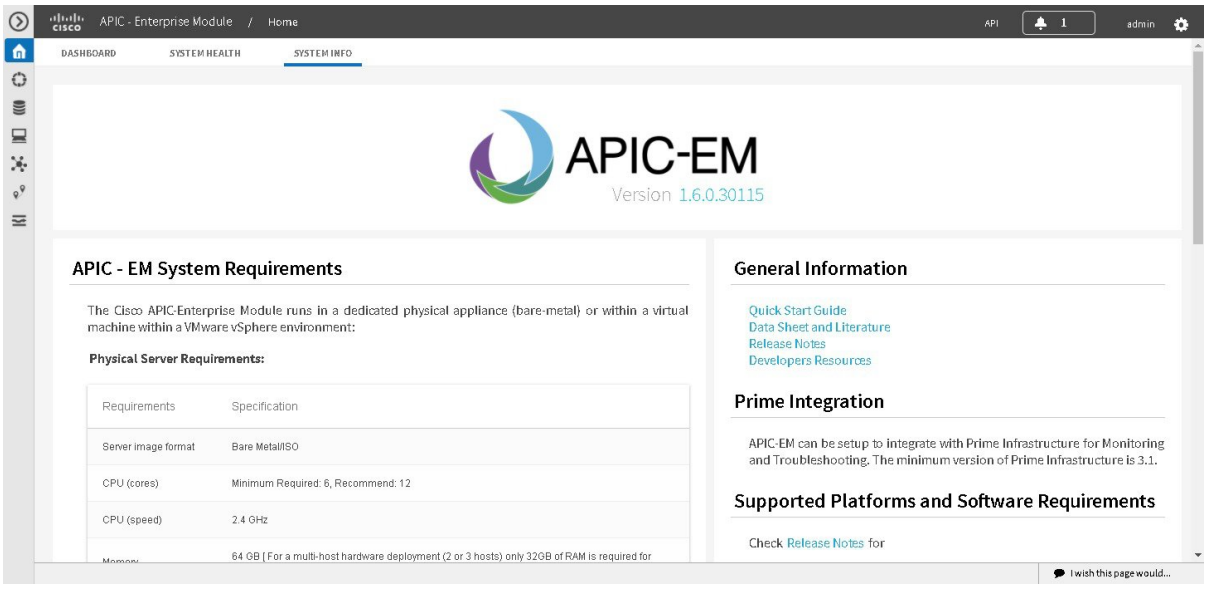
Figure 1: SYSTEM INFO Tab



Reviewing the SYSTEM INFO Tab

You can use the **SYSTEM INFO** tab to access information at a glance about the controller, its system requirements, supported platforms, and other information. The **SYSTEM INFO** tab is directly accessible from the **Home** page.

Figure 2: SYSTEM INFO Tab



Before you begin

You must have successfully deployed the Cisco APIC-EM and it must be operational.

All users can access the contents of the **SYSTEM INFO** tab. The **SYSTEM HEALTH** tab access is limited to users with ROLE_ADMIN privileges and RBAC scope configured to All. The **DASHBOARD** tab is limited to users with ROLE_ADMIN privileges and RBAC scope configured to All or ROLE_POLICY_ADMIN privileges and RBAC scope configured to All.

For information about user permissions and RBAC scopes required to perform tasks using the Cisco APIC-EM, see the chapter, "Managing Users".

Log into the Cisco APIC-EM **Home** page, as described in the previous procedure.

Step 1 On the **Home** page, click the **SYSTEM INFO** tab to view general information about the controller.

Proceed to perform any or all of the following actions listed in the steps below.

Step 2 Review the information displayed on the GUI page about system requirements.

Step 3 Review the information displayed on the GUI page about supported platforms and software requirements

Step 4 Review the information displayed on the GUI page about Prime Infrastructure support.

Step 5 Click the link to open the **Quick Start Guide**.

The **Quick Start Guide** provides an introduction to the controller and its basic functionality.

What to do next

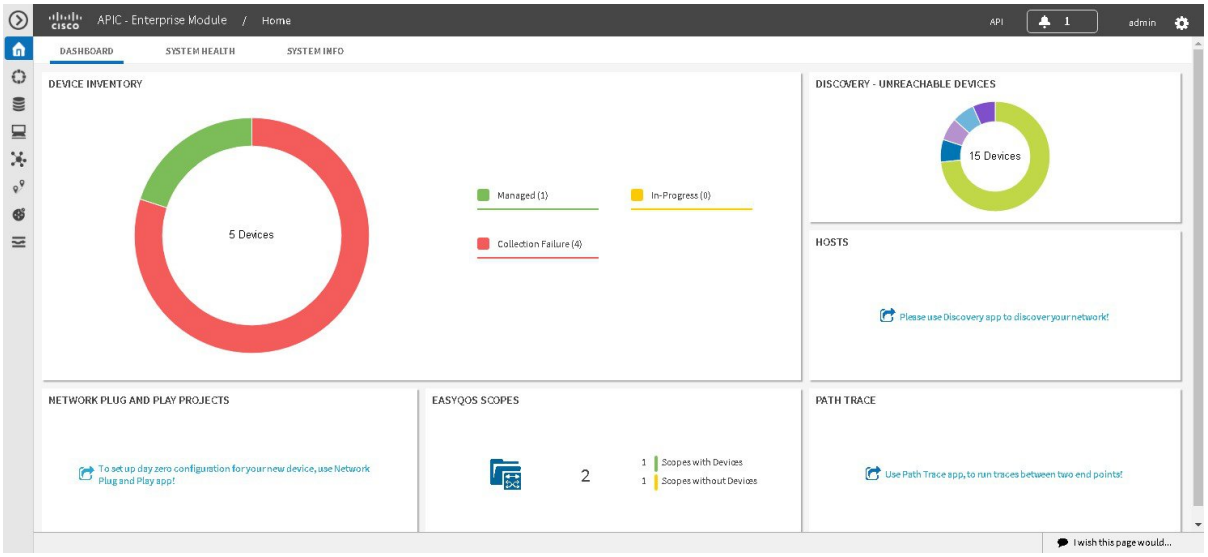
Click the datasheet links or Cisco DevNet links for additional information about the controller and access to Cisco DevNet, respectively.

Click the other tabs to review the controller's dashboard and system health.

Reviewing the DASHBOARD Tab

You can use the **DASHBOARD** tab to quickly view graphical displays of key applications on the controller and their operational status. This information can be used to monitor the controller, the network devices that the controller manages, as well as to assist in troubleshooting any problems. The **DASHBOARD** tab is directly accessible from the **Home** page.

Figure 3: DASHBOARD Tab



Before you begin

You must have successfully deployed the Cisco APIC-EM and it must be operational.

All users can access the contents of the **SYSTEM INFO** tab. The **SYSTEM HEALTH** tab access is limited to users with ROLE_ADMIN privileges and RBAC scope configured to All. The **DASHBOARD** tab is limited to users with ROLE_ADMIN privileges and RBAC scope configured to All or ROLE_POLICY_ADMIN privileges and RBAC scope configured to All.

For information about user permissions and RBAC scopes required to perform tasks using the Cisco APIC-EM, see the chapter, "Managing Users".

Log into the Cisco APIC-EM **Home** page, as described in the previous procedure.

Step 1 On the **Home** page, click the **DASHBOARD** tab to view information about the controller's current activities.

You can view data about the controller's current activities through the dashboard. This data is organized through a set of seven widgets, although only six widgets are displayed at a time.

Note A widget will not appear in the **DASHBOARD** tab if its underlying application has not been installed and enabled.

Unless you have started a discovery and/or a specific controller application, the widgets in the dashboard will be grayed out and inactive. After starting a discovery, data will start to populate and appear in these widgets. Data displayed is updated every few minutes.

Step 2 After performing a successful discovery, review the data displayed in each of the seven widgets.

Device Inventory	Graphical representation of the number of network devices (and percentages of network devices) being actively managed, in progress of being managed, and where there was a failure to connect to and collect device data. Collection failure icons in this widget are clickable and access additional data about the devices where there was a collection failure.
Discovery-Unreachable Devices	Graphical representation of the number of devices reachable and unreachable for a discovery. Clicking the circular icon in this field accesses the **Discovery** window for the specific discovery job.
Branch Sites	Graphical representation of the status of branch sites in your network for the IWAN application. This display includes the following data about branch site status: • Pending • In Progress • Failed • Provisioned **Note** This widget only appears if the IWAN application is installed and enabled.
Hosts	Graphical representation of the hosts in your network. Display includes the number of wired and wireless hosts (and percentages of network hosts as wired or wireless). **Note** This widget only appears if the IWAN application is neither installed or enabled.
Path Trace	Graphical representation of the successful and unsuccessful path traces. Clicking the circular icon in this field accesses the **Path Trace** window.
EasyQoS Scopes	Graphical representation of the policy scopes (EasyQoS) applied to the devices. Displays both number of policies with scopes and without scopes.

PnP Projects	Graphical representation of the status of Plug N Play projects for your network. This display includes the following data about PnP project status: • Provisioned • Pre-Provisioned • In-Progress • Failed Clicking the link in this widget launches the PnP application in the controller.

Each widget in the above table displays data related to an application. If that widget's application is not enabled on the controller, then no data will be visible for that application.

Step 3 Proceed to click within any widget icon to view additional detailed data about its subject matter.

Additionally, by clicking the appropriate link within the widget you can immediately access the underlying application.

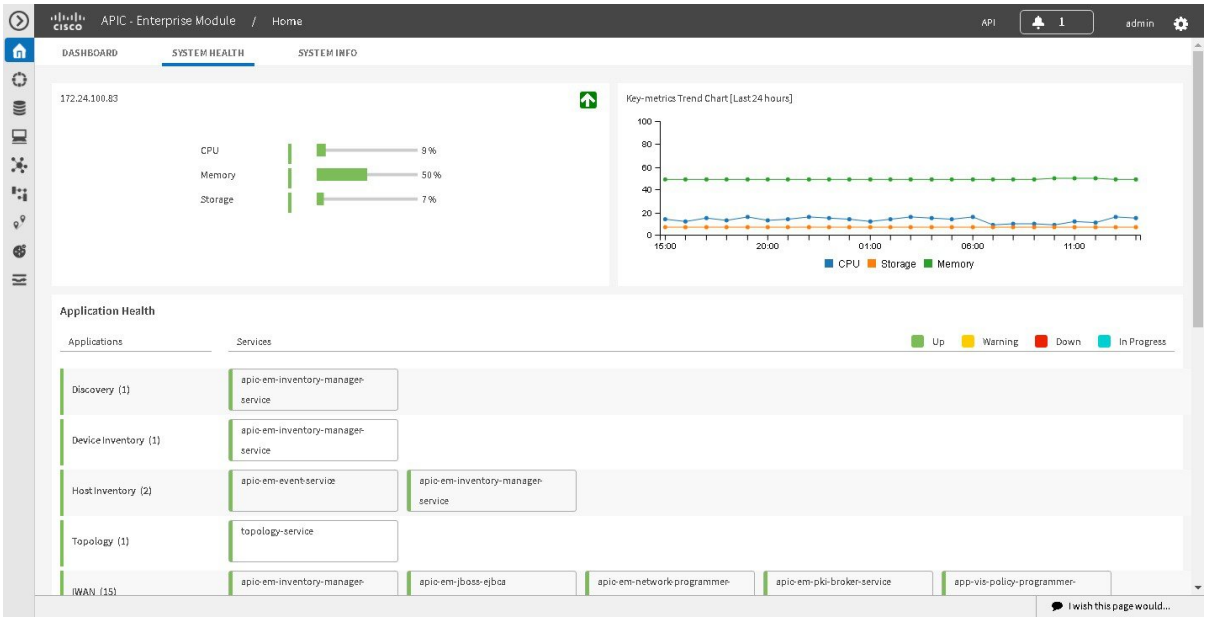
What to do next

Click the other tabs to review the controller's system health and system information.

Reviewing the SYSTEM HEALTH Tab

You can use the **SYSTEM HEALTH** tab to quickly view graphical displays of both the basic health of the system and the applications running on the controller. This information can be used to monitor the controller and its applications, as well as to assist in troubleshooting any problems. The **SYSTEM HEALTH** tab is directly accessible from the **Home** page.

Figure 4: SYSTEM HEALTH Tab



Before you begin

You must have successfully deployed the Cisco APIC-EM and it must be operational.

All users can access the contents of the **SYSTEM INFO** tab. The **SYSTEM HEALTH** tab access is limited to users with ROLE_ADMIN privileges and RBAC scope configured to All. The **DASHBOARD** tab is limited to users with ROLE_ADMIN privileges and RBAC scope configured to All or ROLE_POLICY_ADMIN privileges and RBAC scope configured to All.

For information about user permissions and RBAC scopes required to perform tasks using the Cisco APIC-EM, see the chapter, "Managing Users".

Log into the Cisco APIC-EM **Home** page, as described in the previous procedure.

Step 1 On the **Home** page, click the **SYSTEM HEALTH** tab to view information about the health of the basic system and the applications running on the controller.

The following information is displayed in the **SYSTEM HEALTH** tab.

System (Host) Health Data	Data displayed include: • Host IP address • CPU—Host CPU usage is displayed in MHZ. Both the currently used and available host CPU is displayed. • Memory—Host memory usage is displayed in GB. Both the currently used and available host memory is displayed. • Storage—Host storage usage is displayed in GB. Both the currently used and available host storage is displayed. **Note** If you have configured a multi-host cluster, then each host's data (CPU, memory, and storage) will be displayed in the UI. Color indicates status for the above host data: • Green—Indicates proper usage and support. • Blue—Indicates usage is approaching improper levels and triggers this warning (color change). • Orange—Indicates a failure based upon the usage exceeding the maximum supported value. Additionally, a graphical representation of the above data over the last 24 hours is displayed in this tab. Moving your cursor or mousing over the graph displays a data summation for specific date and time. **Note** By placing your cursor over (mouse over) a color warning in the window, further information about the warning or failure message appears.

Application Health Data	Displays applications available from the **Navigation** pane, and the services that support each application. For example, the **Topology** application accessible in the GUI is supported by topology-service. Color bars indicate the status for the applications and the supporting service(s): • Green —Indicates that an application instance is starting. An application instance is the aggregation of the service instances. You can configure a minimum or maximum number of service instances, as well as grow and harvest these service instances (spin up or spin down the services). • Yellow—Indicates application instance and its supporting service instance(s) are experiencing issues and triggers this warning (color change). • Red—Indicates a failure of the application instance and its supporting service instance(s). You can harvest a service instance and then regrow it using the GUI. If the service instance does not regrow using the GUI, then you can manually regrow it. When you harvest a service instance, the controller will determine which instance is regrown (load balancing among them). • Blue—Indicates an in-progress state for the application or service instance (growing or harvesting).

Step 2 Place your cursor over a specific service to view additional information about it.

The following additional information is displayed about the service:

- Service name
- Service status (indicated by color code)
- Number of instances of the service currently running
- IP address or addresses of host where service instances are running
- Service version

Step 3 (Optional) Click the green-colored addition icon (+) within the service to grow (start up) an instance of that service for an application.

Caution Growing or harvesting services can be done for troubleshooting a service that is performing erratically. Be sure that you understand the possible effects of growing and harvesting services, because doing so could have unexpected results. For detailed information about growing and harvesting services for troubleshooting purposes, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Troubleshooting Guide*.

Step 4 (Optional) Click the red-colored subtraction icon (-) within the service to harvest (shut down) an instance of the service for an application.

Caution Growing or harvesting services can be done for troubleshooting a service that is performing erratically. Be sure that you understand the possible effects of growing and harvesting the services, because doing so could have unexpected results. For detailed information about growing and harvesting services for troubleshooting purposes, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Troubleshooting Guide*.

What to do next

Click the other tabs to review the controller's dashboard and system information.

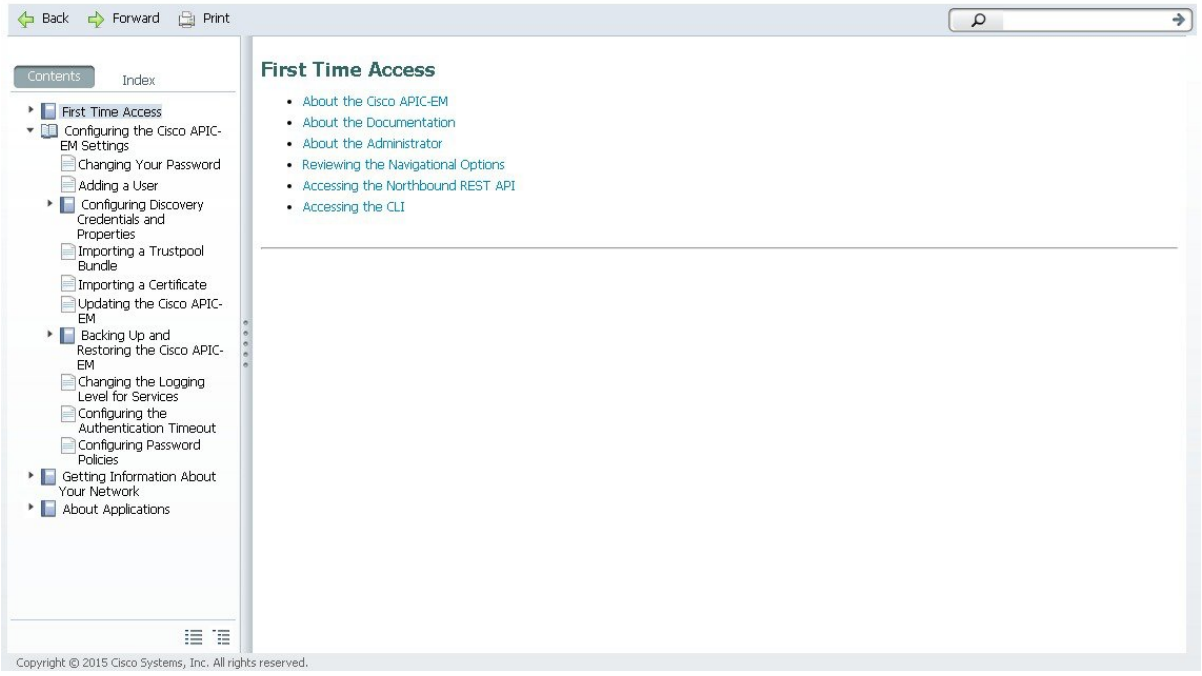
Quick Tour of the APIC-EM Graphical User Interface (GUI)

For a quick introduction to the Cisco APIC-EM GUI, log into the Cisco APIC-EM controller as an administrator and follow the procedure below.

Step 1 Click the **Quick Start Guide** link that appears on the Cisco APIC-EM **Home** page.

The *Quick Start Guide* opens in a separate window.

Figure 5: Quick Start Guide



Step 2 Take a few moments to review the contents of the *Quick Start Guide*, which provides a short introduction to the main components of the Cisco APIC-EM graphical user interface and briefly describes how to configure some of the Cisco APIC-EM settings.

What to do next

If you are using the IWAN application with Cisco Prime Infrastructure for your network, then proceed to configure your Prime credentials. If you are not using the IWAN application with Cisco Prime Infrastructure, then proceed to configure the discovery credentials for your network.

User Settings

About Role Based Access Control

Cisco APIC-EM allows you to define a user profile by role and Role-Based Access Control (RBAC) scope. The role defines the actions that a user may perform, and the RBAC scope defines the resources that a user may access. Currently, devices are the only resources that can be assigned to an RBAC scope.

A user who is assigned a role (for example, ROLE_ADMIN) and scope ALL permissions may perform the full range of actions of the role to the entire scope. However, if this same user is limited to only a subset of devices, the range of actions change, depending on the application (Discovery, EasyQoS, Path Trace, etc.). For detailed application behavior based on limited RBAC scope, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Configuration Guide*.

User Profiles

A user profile defines a user's login, password, role (permissions) and RBAC scope (resource access).

User profiles can exist on the Cisco APIC-EM controller or on an external AAA server. Both of the following types of profiles can coexist for any user:

- Internal user profile: resides on the Cisco APIC-EM controller.
- External user profile: resides on an external AAA server.

The default user profile that is created when the Cisco APIC-EM is deployed has administrator role (ROLE_ADMIN) permissions and access to all resources (RBAC scope ALL). In turn, this user can create other user profiles with various roles and RBAC scopes, including user profiles with ROLE_ADMIN and RBAC scope ALL permissions (a user with global RBAC scope) or with ROLE_ADMIN and RBAC scope set to a specific group (user with partial RBAC scope).

You can view external user profiles which includes a username and their authorization on the controller. You view external user profiles and their roles in the **External Users** window. The authorization for the user consists of an RBAC scope and role in that RBAC scope.

For information about configuring internal users, see Creating Internal Users, on page 20. For information about configuring external controller authentication, see Configuring External Authentication, on page 22.

About User Roles

Users are assigned user roles that specify the functions that they are permitted to perform:

- Administrator (ROLE_ADMIN)
- Policy Administrator (ROLE_POLICY_ADMIN)

- Observer (ROLE_OBSERVER)
- Installer (ROLE_INSTALLER)

When you deploy the Cisco APIC-EM for the first time, the configuration wizard prompts for a username and password. This first-time user is given full administrative (read and write) permissions for the controller and access to all resources. This user is able to create user profiles for other users.

Note Only users with the administrative role (ROLE_ADMIN) can create users profiles. These users can have RBAC scope set to ALL (user with global RBAC scope) or set to a specific group (user with partial RBAC scope).

Note We highly recommend that you configure at least two users with administrator (ROLE_ADMIN) privileges and SCOPE: ALL. In the unlikely event that one user is locked out or forgets his or her password, you have another user with administrative privileges who can help you to recover from this situation.

Administrator Role

A user's access to Cisco APIC-EM functionality is determined both by its role and the RBAC scope that it is assigned. In general, the administrator role has full read/write access to all of the Cisco APIC-EM functions:

- User and group settings

Note For security reasons, passwords are not displayed to any user, not even those with administrator privileges.

Note Although an administrator cannot directly change another user's password in the GUI, an administrator can delete and then re-create the user with a new password using the GUI.

- Discovery credentials and Discovery

Note Only users with access to all resources (RBAC scope set to ALL) can define discovery credentials and perform discovery.)

- Inventory
- Topology
- Path Trace
- EasyQoS (create, modify, and deploy QoS policies to devices)

- System-wide controller-administration functions, such as Network Settings (Trustpool, Controller Certificate, Proxy Certificate) and Controller Settings (Update, Backup & Restore, Logging Level, Auth Timeout, Password Policy, Prime Credentials, Telemetry Collection and Controller Proxy)
- App Management
- System Administration
- Audit Logs
- APIs

Depending on the user's RBAC scope, the administrator's role is impacted as follows:

- With access to all resources (RBAC scope set to ALL), the user can perform all of the administrator functions listed above to all resources.
- With access to a subset of resources (RBAC scope set to **Custom** with resource groups assigned), the user can perform all of the administrator functions listed above, but only to the resources assigned in the RBAC scope, with the following exceptions:
  - Users cannot define discovery credentials or perform discovery.
  - Users can create new users and assign RBAC scopes to them, but they can only assign the RBAC scopes for which they have administrative roles. They can delete only the users that they have created.

Note We highly recommend that you configure at least two users with administrator (ROLE_ADMIN) privileges and SCOPE: ALL. In the unlikely event that one user is locked out or forgets his or her password, you have another user with administrative privileges who can help you to recover from this situation.

Policy Administrator Role

A user's access to Cisco APIC-EM functionality is determined both by its role and the RBAC scope that it is assigned. In general, the policy administrator role has full read/write access to the following functions:

- Change Password
- Discovery Credentials and Discovery

Note Only users with access to all resources (RBAC scope set to ALL) can define discovery credentials and perform discovery.)

- Inventory
- Topology
- Path Trace
- EasyQoS (create, modify, and deploy QoS policies to devices)
- Prime Credentials

- Policy administration APIs

Depending on the user's RBAC scope, the policy administrator's role is impacted as follows:

- With access to all resources (RBAC scope set to ALL), the user can perform all of the policy administrator functions listed above for all resources.
- With access to a subset of resources (RBAC scope set to **Custom** with resource groups assigned), the user can perform all of the functions listed above (except define discovery credentials and perform discovery), but only for the resources assigned in the RBAC scope.

This role cannot access system-wide controller-administration functions, such as Users and Groups (except to change its own password), Network Settings (Trustpool, Controller Certificate, Proxy Certificate) and Controller Settings (Update, Backup & Restore, Logging Level, Auth Timeout, Password Policy, Telemetry Collection and Controller Proxy.)

Observer Role

A user's access to Cisco APIC-EM functionality is determined both by its role and the RBAC scope that it is assigned. With the exception of being able to change their own password, users with the observer role have read-only access (ability to view but not make any changes) to the following functions:

- Discovery Results
- Inventory
- Topology
- Path Trace
- EasyQoS
- System-wide controller-administration functions, such as Network Settings (Trustpool, Controller Certificate, Proxy Certificate) and Controller Settings (Update, Backup & Restore, Logging Level, Auth Timeout, Password Policy, Prime Credentials, Telemetry Collection and Controller Proxy)
- App Management
- System Administration
- Audit Logs
- APIs

Depending on the user's RBAC scope, the observer's role is impacted as follows:

- With access to all resources (RBAC scope set to ALL), the user can view all of the functions listed above for all resources.
- With access to a subset of resources (RBAC scope set to **Custom** with resource groups assigned), the user can view all of the functions listed above (except discovery credentials and discoveries), but only for the resources assigned in the RBAC scope.

Installer Role

Users who are assigned the installer role (ROLE_INSTALLER) can use the Cisco Plug and Play Mobile application to access the Cisco APIC-EM remotely to perform the following functions:

- View device status.
- Trigger device deployments.

Installers cannot access the Cisco APIC-EM GUI. As such, they are not bound by an RBAC scope.

Note For security reasons, passwords are not displayed to any user, not even those with administrator privileges.

Resource Groups

In Cisco APIC-EM, you create groups to contain related resources. Then, you assign the groups to users to provide them access to the resources in the group. You may only create groups that contain the resources (or a subset of resources) to which you have access. Currently, devices are the only resources that can be assigned to a group.

Keep the following guidelines in mind when creating resource groups:

- Only users with ROLE_ADMIN can define resource groups. A user with ROLE_ADMIN and access to all resources (RBAC scope set to ALL) can create resource groups that contain any or all of the available resources. A user with ROLE_ADMIN and access to only certain resources can create resource groups that only contain the same devices that the user has access to. Users cannot create resource groups that contain resources that they do not have access to.
- A resource group cannot contain another resource group.

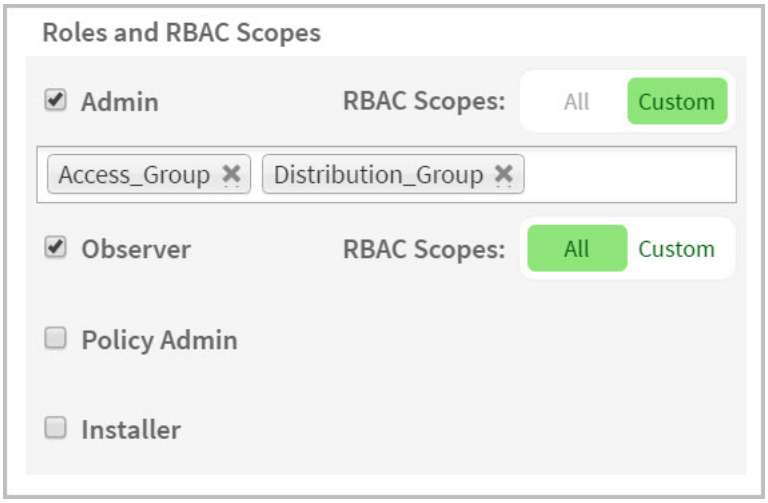
RBAC Scopes

The RBAC scope defines the resources that a user may access. Currently, devices are the only type of resource that can be assigned to an RBAC scope.

When you create a user profile, you can configure one or more user roles for the user. Each user role that you define is assigned a corresponding RBAC scope. The RBAC scope can be all of the resources (RBAC scope set to ALL) or it can be a limited set of resources (RBAC scope set to Custom). When you define a custom RBAC scope, you then need to assign resource groups to it.

For example, in the following figure, the Admin role has been assigned a custom RBAC scope, and the RBAC scope consists of two groups: Access_Group and Distribution_Group. This means that the user can perform all administrative functions to the devices in the Access_Group and Distribution_Group. The Observer role has been assigned the RBAC scope of ALL. This means that the user can view all of the devices in the Cisco APIC-EM.

Figure 6: Example of RBAC Scope Assignment



Keep the following guidelines in mind when defining RBAC scopes for users:

- A user can have only one role in a given RBAC scope.
- If a user is assigned a role for one RBAC scope and a different role for another RBAC scope, and the RBAC scopes have some resource groups in common, the user is given the higher privileged access to the common devices. For example, a user is assigned ROLE_ADMIN for group G1 and ROLE_OBSERVER for group G2. Groups G1 and G2 have device D1 in common. (The device is in both groups.) This situation results in the user being given ROLE_ADMIN privileges for device D1.
- Users who are working with the Cisco IWAN and Cisco Network PnP applications to monitor and manage devices and hosts must have their **RBAC Scopes** values set to **All**. The Cisco IWAN and Cisco Network PnP applications do not support **Custom** RBAC scopes.

About Role Based Access Control

Cisco APIC-EM allows you to define a user profile by role and Role-Based Access Control (RBAC) scope. The role defines the actions that a user may perform, and the RBAC scope defines the resources that a user may access. Currently, devices are the only resources that can be assigned to an RBAC scope.

A user who is assigned a role (for example, ROLE_ADMIN) and scope ALL permissions may perform the full range of actions of the role to the entire scope. However, if this same user is limited to only a subset of devices, the range of actions change, depending on the application (Discovery, EasyQoS, Path Trace, etc.). For detailed application behavior based on limited RBAC scope, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Configuration Guide*.

About Authentication and Authorization

Users and their roles are subject to an authentication and authorization process.

Note Currently, Cisco APIC-EM supports authentication and authorization. Accounting is not yet supported.

With the Cisco APIC-EM, each resource for the controller is mapped to an action and each action is mapped to a required permission for a user. All REST APIs are therefore protected by the controller authentication process.

You can configure the following types of authentication for user access to the Cisco APIC-EM:

- Internal—Local controller authentication based upon the usernames and passwords created using the controllers's own GUI. For information about configuring internal users, see Creating Internal Users, on page 20.
- External—External controller authentication based upon the usernames and passwords that exist on other AAA servers. For information about configuring external controller authentication, see Configuring External Authentication, on page 22.

When performing user authentication, the controller attempts to authenticate the user in the following order:

1. Authenticate with AAA server directory credentials using the RADIUS protocol (number of times attempted per user configuration using the GUI or APIs)
2. Authenticate with the user credentials that are configured locally on the controller (number of times attempted per user configuration using the controller GUI)

If the user credentials are authenticated in any of the above steps, then controller access is immediately granted.

Configuring RBAC Scope for Users within your Network

You can use the following workflow to assist in configuring RBAC scope for users and devices within your network.

1. Discover the devices within your network.

   Run a discovery on the devices within your network using the **Discovery** functionality of the controller. For information about this procedure, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Configuration Guide*.

2. Create a set of groups consisting of network devices for user access.

   For information about this procedure, see Configuring Groups for User Access, on page 17.

3. Assign network devices to their relevant groups.

   For information about this procedure, see Configuring Groups for User Access, on page 17.

4. Create internal users for the controller and assign their roles and RBAC scope.

   For information about this procedure, see Creating Internal Users, on page 20.

5. Configure external authentication and authorization for users from an AAA server.

   For information about this procedure, see Configuring External Authentication, on page 22.

6. View external users that have access to the Cisco APIC-EM using the controller's GUI.

   For information about this procedure, see Viewing External Users, on page 27.

Configuring Groups for User Access

The Cisco APIC-EM supports the configuration of groups.

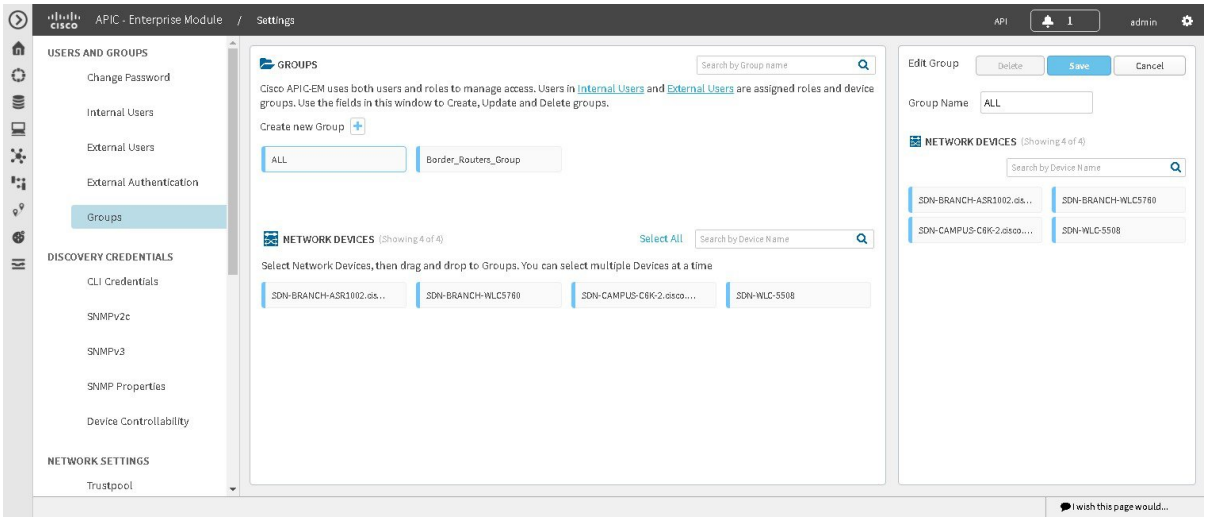
A group is a named entity that represents a specific set of resources for access-control purposes. You assign users to groups using RBAC scope. Assigning a user to a group with RBAC scope enables that user to access the resources in that group; if the user is not assigned to a particular group, the user cannot access the resources in that group. In the current release, groups can contain network devices only; hosts or other resources cannot belong to groups.

Note Hosts and wireless access points (only Cisco Unified access points) cannot be added to a specific group using the GUI. They are added to a group automatically when linked to a wireless LAN controller (WLC) or switch that is added to a group using the GUI.

You can configure groups using the **Groups** window in the Cisco APIC-EM GUI.

Note Hosts and wireless access points (Unified access points only) cannot be added to a group. Instead, they are automatically added to a group when the switch or wireless LAN controller to which the host or wireless access point is connected is added to the group.

Figure 7: Configuring Groups Window



Important Both internal and external users can be configured for group access using RBAC scope. You configure RBAC scope for internal users with the controller's GUI using the **Internal Users** page. You configure RBAC scope for external users on the AAA server itself.

Before you begin

You must have successfully deployed the Cisco APIC-EM and it must be operational.

You must have administrator (ROLE_ADMIN) permissions and either access to all resources (RBAC scope set to ALL) or an RBAC scope that contains all of the resources that you want to group. For example, to create

a group containing a specific set of resources, you must have access to those resources (custom RBAC scope set to all of the resources that you want to group).

For information about user permissions and RBAC scopes required to perform tasks using the Cisco APIC-EM, see the chapter, "Managing Users".

You must have successfully performed a discovery, with the resulting discovered devices appearing in the controller's **Inventory** window.

Step 1 In the **Home** window, click either **admin** or the **Settings** icon (gear) at the top right corner of the screen.

Step 2 Click the **Settings** link from the drop-down menu.

Step 3 In the **Settings** navigation pane, click **Groups** to view the **Groups** window.

The **Groups** window is divided into three fields.

Groups	Provides an addition icon where you can begin to create a group. After creating a group, it appears in this **Groups** field. A **Search by Group name** field permits you to enter a Group name and only display that group in this field.
Network Devices	Displays the discovered devices from your network. A **Search by Device name** field permits you to enter a device name to only display that device in this field. You add devices to a group by dragging and dropping a device from the **Network Devices** field directly onto a group in the **Groups** field. **Note** There are two possible controller GUI views for **Network Devices** based upon the user's role and scope (ADMIN with Scope ALL access or ADMIN with non-global scope access). An ADMIN with Scope ALL access is able to view the total number of devices, including any unassigned devices. An ADMIN with non-global scope access is only able to view the assigned devices.

Groups Overview	Displays total number of groups, discovered devices assigned to groups, and devices not assigned to groups. Clicking on a specific group in the **Groups** field provide options to delete, edit and save, or cancel (exit) the group. A **Search by Device name** field permits you to enter a device name to only display that device in this field. Clicking on a device provides the following information: • Name—Name of the discovered device. • IP address——IP address of the discovered device. • Family—Generic family name, for example "Routers" or "Wireless Controller". • Type—Specific type of device, for example," Cisco 3945 Integrated Services Router G2" • Device Tags—Tags applied to the device in the **Inventory** or **Topology** windows.

Step 4 Click the addition icon in the **Groups** field.

Step 5 Enter a name for the new group in the **Group Name** field that appears.

Step 6 Click the green checkmark to create and save the new group.

Step 7 Drag and drop any network device icons from the **Network Devices** field to the new group icon in the **Groups** field.

Dragging and dropping the network device icon to the new group icon will add that device to the new group.

You can also click on several network device icons in the **Network Devices** field to first form a selection of devices, and then drag and drop the entire selection of devices to the group icon to form the new group.

Note When creating an RBAC scope, the hosts and wireless access points that are associated with the selected network devices are also added to that RBAC scope.

Step 8 Continue creating groups and adding devices for your network.

What to do next

After configuring groups containing the appropriate devices for your network, access the **Internal Users** window. In this window, you assign group access permissions with the **RBAC Scope** field.

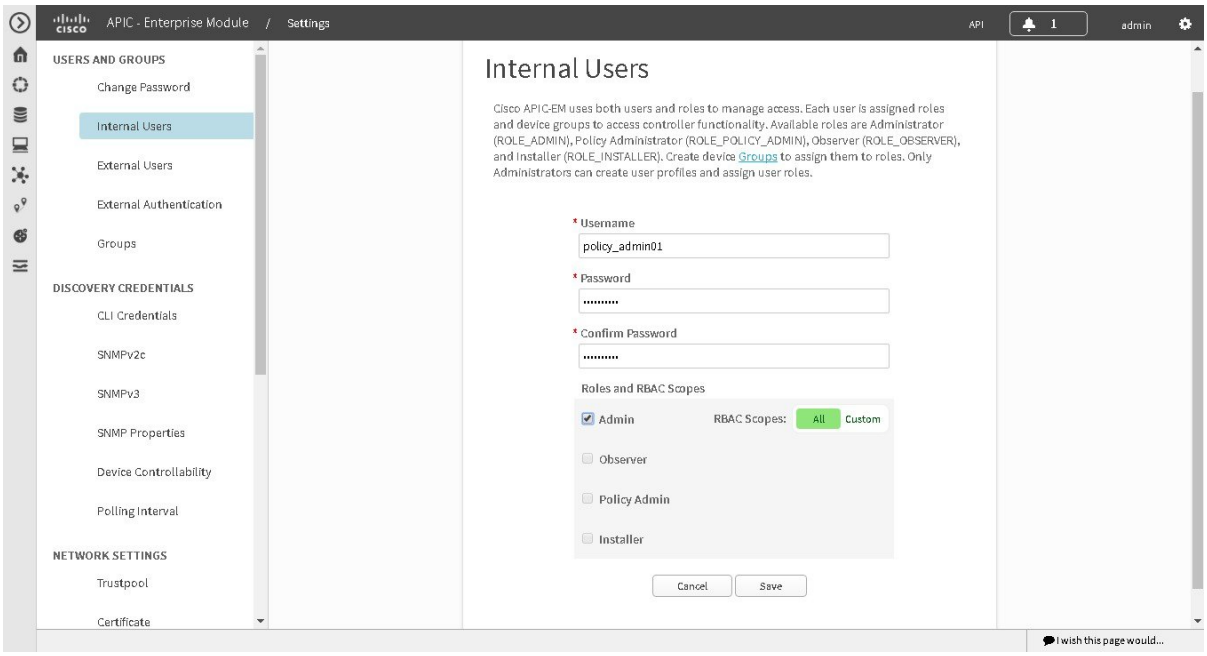
Creating Internal Users

You can create an internal user for the Cisco APIC-EM.

Note User information (credentials) is stored in a local database on the controller.

Note We highly recommend that you configure at least two users with administrator (ROLE_ADMIN) privileges and SCOPE: ALL. In the unlikely event that one user is locked out or forgets his or her password, you have another user with administrative privileges who can help you to recover from this situation.

Figure 8: Internal Users Window



Before you begin

You must have administrator (ROLE_ADMIN) permissions, as well as RBAC scope configured to all groups (global RBAC scope) or a specific subset of groups (non-global RBAC scope).

You must have configured the appropriate groups for the network devices using the **Groups** window in the controller's GUI.

Step 1 In the **Home** window, click either **admin** or the **Settings** icon (gear) at the top right corner of the screen.

Step 2 Click the **Settings** link from the drop-down menu.

Step 3 In the **Settings** navigation pane, click **Internal Users** to view the **Internal Users** window.

Step 4 Click **Create User**.

Step 5 In the **Create User** fields that now appear, you need to enter the username, password (twice), and role and group of the new user.

Step 6 Enter the username.

Step 7 Enter the password twice.

Step 8 Click the appropriate role for the user.

Step 9 Click the appropriate **RBAC Scope** for the user (either **All** or click and then select a **Custom** RBAC Scope).

The **ALL** option in the **RBAC Scopes** field contains all devices discovered by the controller.

Prior to configuring an internal user, set up RBAC scopes using **Groups** in the controller's GUI.

Step 10 Click **Save** to save the user configuration.

The **Users** window is displayed with the following information about the users:

- **Username**—Username assigned to the user.
- **Actions**—Icons that allow you to edit user information or delete a user.

What to do next

Proceed to configure any other internal users for your network devices. If necessary, configure external authentication for any external users for your network devices using the **External Authentication** window in the controllers' GUI.

Configuring External Authentication

The Cisco APIC-EM supports external authentication and authorization for users from an AAA server. The external authentication and authorization is based upon usernames, passwords, and attributes that already exist on a pre-configured AAA server. With external authentication and authorization, you can log into the controller with credentials that already exist on the AAA server. The RADIUS protocol is used to connect the controller to the AAA server.

The controller attempts to authenticate and authorize the user in the following order:

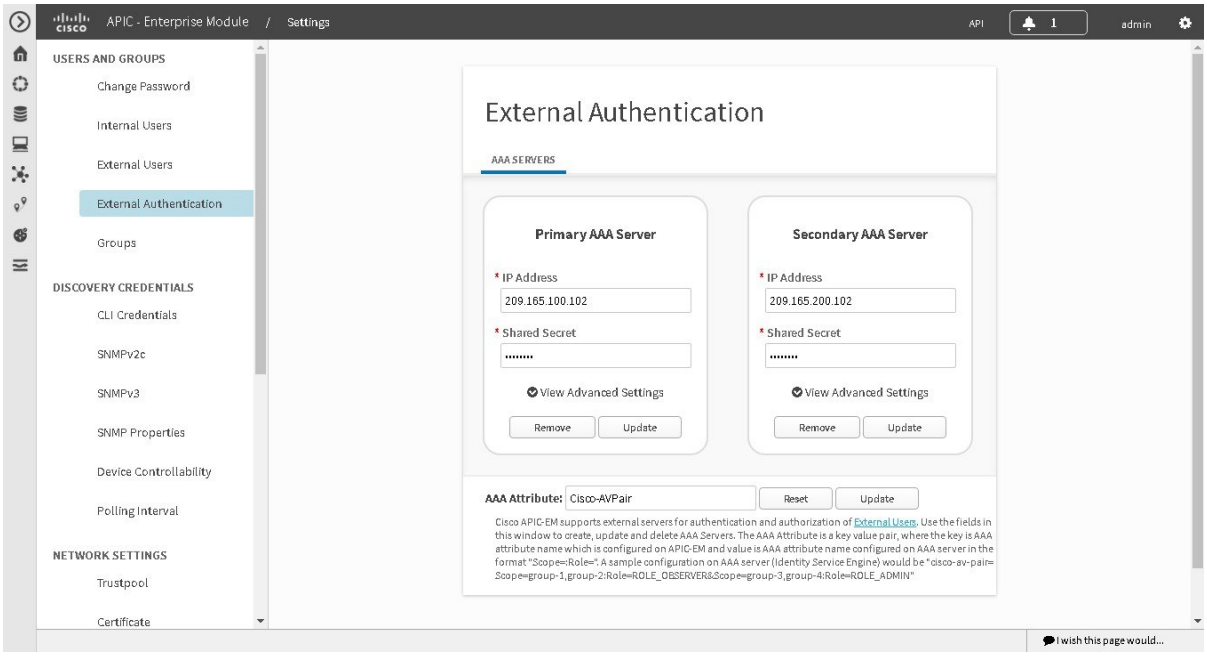
1. Authenticate/authorize with the user's credentials on a primary AAA server.
2. Authenticate/authorize with the user's credentials on a redundant or secondary AAA server.
3. Authenticate/authorize with the user's credentials managed by the Cisco APIC-EM.

A user is granted access to the controller only if both authentication and authorization is successful. When authentication/authorization is attempted using an AAA server, the response from that AAA server may be either a timeout or rejection:

- A timeout occurs when there is no response received from the AAA server within a specific period of time. If the AAA server times out for the authentication/authorization request on the first configured AAA server, then there is a failover to the secondary AAA server. If the secondary AAA server also times out for the authentication/authorization request, then a fall back to local authentication/authorization occurs.
- A rejection is an explicit denial of credentials. If the AAA server rejects an authentication/authorization attempt made from the controller, then there is a fall back to local authentication/authorization.

You configure parameters for the controller to connect to and communicate with an external AAA server, using the **External Authentication** window in the Cisco APIC-EM GUI.

Figure 10: External Authentication Window



Before you begin

You must have successfully deployed the Cisco APIC-EM and it must be operational.

You must have administrator (ROLE_ADMIN) permissions and either access to all resources (RBAC scope set to ALL) or an RBAC scope that contains all of the resources that you want to group. For example, to create a group containing a specific set of resources, you must have access to those resources (custom RBAC scope set to all of the resources that you want to group).

For information about user permissions and RBAC scopes required to perform tasks using the Cisco APIC-EM, see the chapter, "Managing Users".

You must have the AAA server already preconfigured, set up, and running. You must also configure the AAA server to interact with the Cisco APIC-EM. When configuring the AAA server to interact with the Cisco APIC- EM, perform the following additional steps:

- Register the Cisco APIC-EM with the AAA server.

Note This could also involve configuring a shared-secret on both the AAA server and Cisco APIC-EM controller.

- Configure an attribute name with a value on the AAA server (the attribute name must match on both the AAA server and controller, see step 10 in the following procedure).
- For a Cisco APIC-EM multi-host configuration, configure all individual host IP addresses and the Virtual IP address for the multi-host cluster on the AAA server.

As an example of using the Cisco Identity Services Engine (ISE) GUI to configure values on an AAA server, you select **Authorization Profiles** in the Cisco ISE GUI navigation pane and proceed to configure an authorization profile. When configuring an authorization profile, you enter the following values:

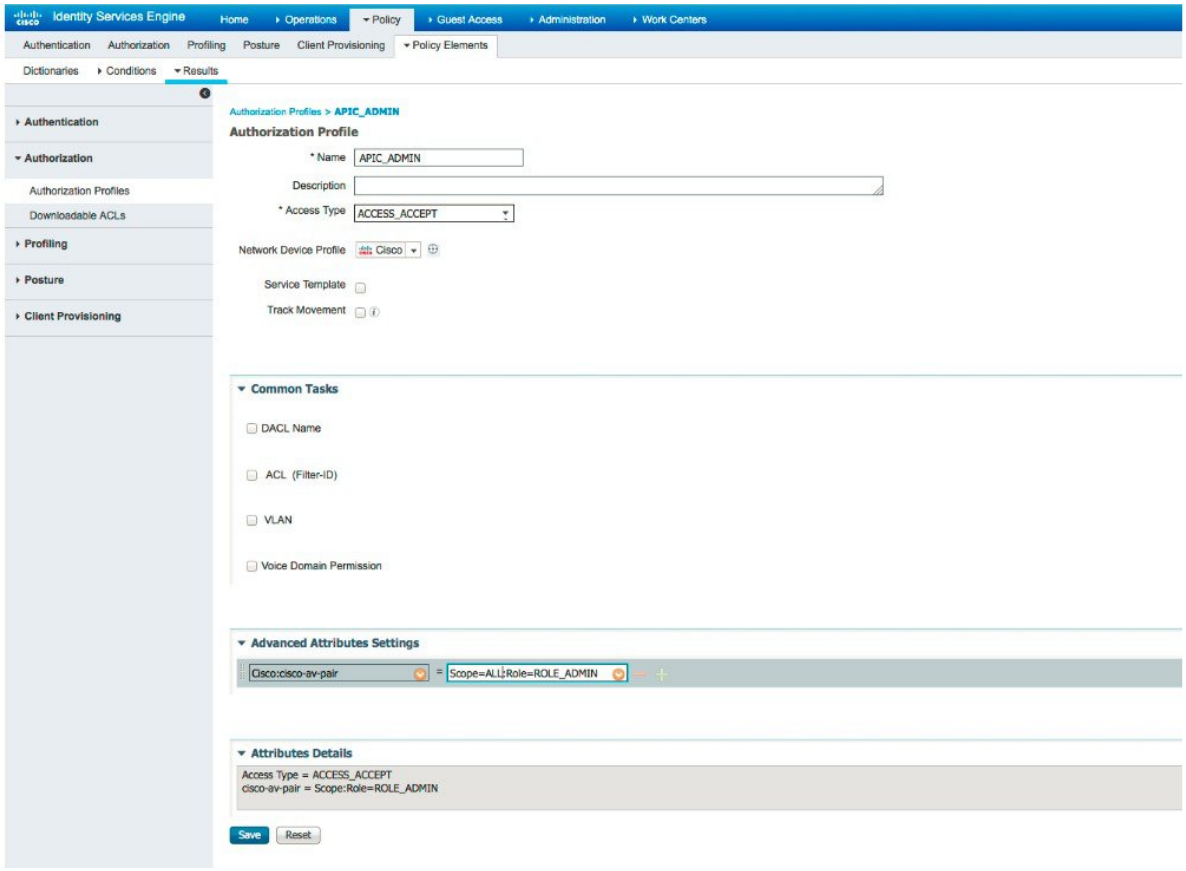
- **Name**: Enter a name for the authorization profile. We recommend that you enter a name similar to the role to be used for the profile. For example, for an admin (ROLE_ADMIN) use a name with "admin" within it, such as "APIC_ADMIN".
- **Description**: Enter a description for the profile
- **Access Type**: ACCESS_ACCEPT
- **Network Device Profile**: Cisco
- **Advance Attribute Settings**:
  - **Attribute Name**: cisco-av-pair (default value)
  - **Scope**: Scope=ALL:Role=ROLE_ADMIN

Note The above **Scope** value is used when setting up external users with administrator permissions (ROLE_ADMIN) and RBAC scope set to ALL. If you have users with different roles and different RBAC scopes, then use the following format for the **Scope** value:

Scope=grp1,grp2,grp5:Role=ROLE_ADMIN&Scope=grp3,grp4:Role=ROLE_OBSERVER

With this **Scope** value format the colon (:) separates the scope(s) from the role. Commas separate the different groups within the scope. The ampersand (&) separates the different roles.

Figure 9: AAA Server Configuration Example (Cisco ISE GUI)



Step 1 In the **Home** window, click either **admin** or the **Settings** icon (gear) at the top right corner of the screen.

Step 2 Click the **Settings** link from the drop-down menu.

Step 3 In the **Settings** navigation pane, click **External Authentication** to view the **External Authentication** window.

Step 4 Click the **AAA Server** tab to configure the controller with AAA server credential authentication values.

Step 5 Configure access to the AAA server for the controller by entering the following *required* information:

- **IP address**—Enter the IP address of your AAA server
- **Shared Secret**—Enter the AAA server's shared secret.

Click either **View Advanced Settings** to enter additional information for the configuration or **Apply** to save and apply your configuration.

Step 6 (Optional) Configure access to the AAA server for the controller by entering the following information:

- **Protocol**—RADIUS

  The Protocol field is grayed out, since RADIUS is the default protocol.

- **Authentication Port**—The default value for this field is 1812. Enter a different value if you do not use this common value for your AAA server.

- **Account Port**—The default value for this field is 1813. Enter a different value if you do not use this common value for your AAA server.

  Note Accounting is not supported in this controller release.

- **Retries**—Enter the number of times for the controller to attempt authentication, or accept the default value of 1.
- **Timeout (seconds)**—Enter the time interval for the controller to attempt authentication, or accept the default value of 2 seconds.

Click **Apply** to save and apply your configuration.

Step 7 Click the **Add AAA Server** tab to configure a *secondary* AAA server for the controller.

The *secondary* AAA server is the backup AAA server that is used for high availability.

Step 8 Configure access to the *secondary* AAA server for the controller by entering the following *required* information:

- **IP address**—Enter the IP address of your second AAA server
- **Shared Secret**—Enter the second AAA server's shared secret.

Important We recommend that the secondary AAA server has the same configuration as the primary AAA server, otherwise results are unpredictable.

Click either **View Advanced Settings** to enter additional information for the configuration or **Apply** to save and apply your configuration.

Step 9 (Optional) Configure access to the *secondary* AAA server for the controller by entering the following information:

- **Protocol**—RADIUS

  The Protocol field is grayed out, since RADIUS is the default protocol.

- **Authentication Port**—The default value for this field is 1812. Enter a different value if you do not use this common value for your AAA server.
- **Account Port**—The default value for this field is 1813. Enter a different value if you do not use this common value for your AAA server.
- **Retries**—Enter the number of times for the controller to attempt authentication, or accept the default value of 1.
- **Timeout (seconds)**—Enter the time interval for the controller to attempt authentication, or accept the default value of 2 seconds.

Click **Apply** to save and apply your configuration.

Step 10 Enter the **AAA Attribute**.

As part of the required, earlier AAA server configuration, you must have already configured an AAA attribute on the AAA server. The AAA attribute is a key value pair that consists of both a key and its value. The key is the AAA attribute name. On the Cisco APIC-EM, you register this AAA attribute name in the controller's GUI in this field. By doing so, you are instructing the controller to search for this key (AAA attribute name) in the AAA server response, after logging in with your AAA credentials.

Important The default AAA attribute name on the controller is Cisco-AVPair.

On the AAA server, you configure *both* the key (AAA attribute name) and its value. The key must be the same as that being configured on the Cisco APIC-EM. The value (which is only configured on the AAA server) supports the following format: Scope=*scope_value*:Role=*role_value*

For example: Scope=ALL:Role=ROLE_ADMIN

Note that if you have several users with different roles and scopes, then you use a different format:

For example: Scope=grp1,grp2:Role=ROLE_ADMIN&Scope=grp3,grp4:Role=ROLE_OBSERVER

This format used for multiple users, roles, and scopes is mandatory. The colon (:) separates the scope(s) from the roles in this format. Commas separate the groups within the scopes. The ampersand (&) separates the different role types.

You can only list the role once using this format. So, in the above example if you need to add an admin for a group 5 (grp5), you would need to rewrite using the following format:

Scope=grp1,grp2,grp5:Role=ROLE_ADMIN&Scope=grp3,grp4:Role=ROLE_OBSERVER

Once finished, click **Update** to save the **AAA Attribute** name.

What to do next

Log out of the Cisco APIC-EM.

Using your AAA server credentials, log back into the Cisco APIC-EM.

Access the **External Users** window on the controller's GUI to view the AAA server users, roles, and scope.

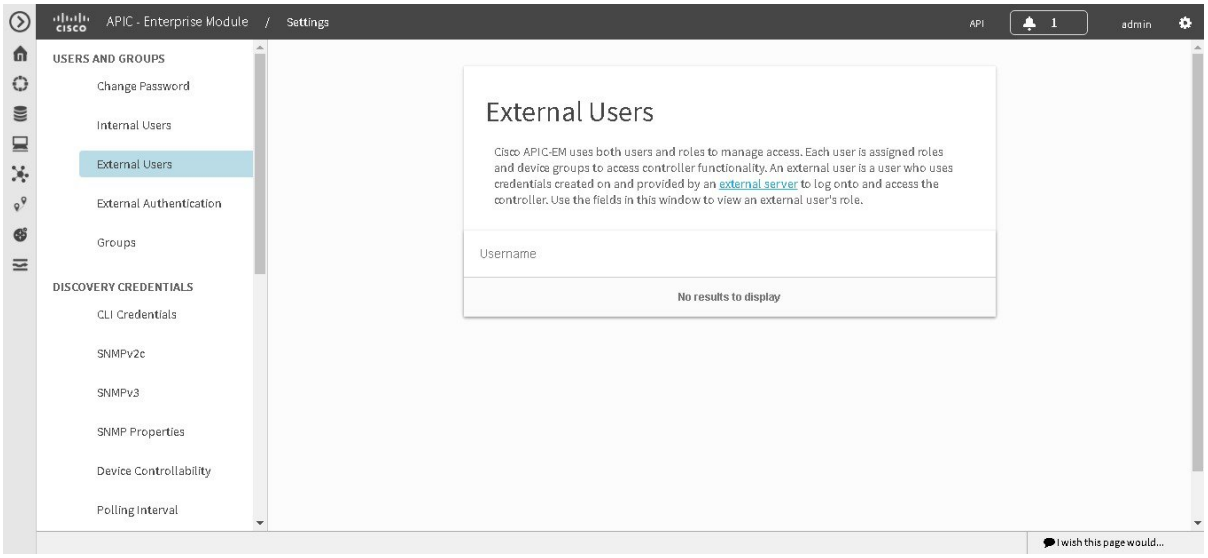
Note If the authentication/authorization is successful and access is granted, then the user's external authentication/authorization is saved in the controller's database. All users successfully granted access can be viewed in the **External Users** window.

Viewing External Users

You can view external users that have access to the Cisco APIC-EM using the controller's GUI. An external user is a user with credentials created on and provided by an external server to log onto and access the controller.

Use the fields in the **External Users** window to view an external user's role and the groups they belong to. For information about configuring external controller authentication, see Configuring External Authentication, on page 22.

Figure 11: External Users Window



Before you begin

You must have administrator (ROLE_ADMIN) permissions, as well as RBAC scope configured to all groups (global RBAC scope) or a specific subset of groups (non-global RBAC scope).

You have already configured external authentication for the controller with an AAA server.

Step 1 In the **Home** window, click either **admin** or the **Settings** icon (gear) at the top right corner of the screen.

Step 2 Click the **Settings** link from the drop-down menu.

Step 3 In the **Settings** navigation pane, click **External Users** to view the **External Users** window.

Step 4 Proceed to view any external users displayed in this window.

Note External users that were authenticated by the controller appear in this window. For example, if you configured an external user on an AAA server (with the name "user_grp01") and this user was authenticated by the controller, then user_grp01 will appear in this window as an active link. Click on the link to view additional user account status (Locked or Unlocked) and authorization (role: list of scopes).

Discovery Credentials

The Cisco APIC-EM supports two different types of discovery credentials: global and job specific (or discovery request-specific). Both types of discovery credentials can consist of CLI or SNMP credentials that are configured using the controller's GUI.

Global credentials can be configured in either the **Discovery** window or the **Discovery Credentials** windows (as described in this chapter). Job specific credentials are only configured in the **Discovery** window.

Note For information about the procedure to configure global and/or job specific credentials in the **Discovery** window, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Configuration Guide*.

Both CLI and SNMP credentials are required for a successful discovery. The SNMP credentials (either global or job specific) are used for *device* discovery. The CLI credentials (either global or job specific) are used for capturing or applying *device configurations* for the controller's inventory.

You should enter at least one set of SNMP credentials, either SNMPv2c or SNMPv3, for your device discovery. If you are going to configure SNMPv2 settings in your network, then SNMP Read Only (RO) community string values should be entered in the controller to assure a successful discovery and populated inventory. However, if an SNMP RO community string and SNMP Read Writer (RW) community string is not entered into the controller, as a *best effort*, discovery will run with the default SNMP RO community string "public." Additionally, if no SNMP RO community string is entered but a SNMP RW community string is entered, then the SNMP RW community string will be used as SNMP RO community string.

Note You can enter values for both SNMP versions (SNMPv2c and SNMPv3) for a single discovery. The controller supports multiple SNMP credential configurations. Altogether, you can enter a maximum of 5 global device credentials (SNMP or CLI) using the **Discovery Credentials** windows as described in this chapter, with an additional credentials set being created in the **Discovery** window. Therefore, for a single discovery scan request, you can configure a total of 6 credential sets of each type (CLI or SNMP).

Global Credentials

Global credentials are defined as preexisting credentials that are common to the devices in a network. Global credentials (CLI and SNMP) are configured on the devices using the GUI (**Discovery** window or **Discovery Credentials** window) and permit successful login to the devices. Global credentials are used by the Cisco APIC-EM to authenticate and access the devices in a network that share this device credential when performing network discoveries.

You can configure the global CLI credentials in the **CLI Credentials** window. You access this window by clicking either **admin** or the **Settings** icon (gear) on the menu bar at the upper right of the screen. You then click the **Settings** link from the drop-down menu and then click **CLI Credentials** on the Setting Navigation pane. You can also configure global CLI credentials in the **Credentials** field in the **Discovery** window. For information about the procedure to configure global CLI credentials in the **Discovery** window, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Configuration Guide*.

You configure the global SNMP credentials in the **SNMPv2c** or **SNMPv3** window . You access these windows by clicking either **admin** or the **Settings** icon (gear) on the menu bar at the upper right of the screen. You then click the **Settings** link from the drop-down menu and then click one of the SNMP window links on the Setting Navigation pane. You can also configure global SNMP credentials in the **Credentials** field in the **Discovery** window. For information about the procedure to configure global SNMP credentials in the **Discovery** window, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Configuration Guide*.

Note Multiple credentials can be configured in the **CLI Credentials** window.

Job Specific Credentials

Job specific credentials (request-specific credentials) are defined as preexisting *device* credentials for a specific network device or set of devices that do not share the global credentials.

You configure job specific credentials in the **Discovery** window prior to performing a discovery that is exclusive for that set of network devices. You access this window by clicking **Discovery** on the Navigation pane.

Discovery Credentials Example

Assume a network of 200 devices that form a CDP neighborship (neighboring devices discovered using Cisco Discovery Protocol (CDP)). In this network, 190 devices share a global credential (Credential-0) and the 10 remaining devices each have their own unique or job specific credentials (Credential 1- 5)

To properly authenticate and access the devices in this network by the Cisco APIC-EM, you perform the following tasks:

1. Configure the CLI global credentials as Credential-0 for the controller.

   You can configure the global credentials in the **CLI Credentials** window. You access this window, by clicking either **admin** or the **Settings** icon (gear) on the menu bar at the upper right of the screen. You then click the **Settings** link from the drop-down menu and then click **CLI Credentials** on the Setting Navigation pane.

2. Configure the SNMP (v2c or v3) global credentials.

   You can configure these global credentials in the two SNMP windows. You access these GUI windows by clicking the **Settings** button at the top right and then clicking **SNMPv2c** or **SNMPv3** on the Setting Navigation pane.

3. Run a **CDP** discovery using one of the 190 device IP addresses (190 devices that share the global credentials) and selecting the global credentials in the GUI. You run a **CDP** discovery in the **Discovery** window. You access this window, by clicking **Discovery** on the Navigation pane.

4. Run 10 separate **Range** discoveries for each of the remaining 10 devices using the appropriate job specific credentials and SNMP values (for example, Credential-1, Credential-2-5, etc.).

   You configure the job specific credentials in the **Discovery** window. You access this window, by clicking **Discovery** on the Navigation pane.

5. Review the **Device Inventory** table in the **Device Inventory** window to check the discovery results

Discovery Credentials Rules

Discovery credentials (global and job specific) operate under the rules as described in the bullet list and table below.

Job Specific Credential Rules

- Job specific credentials can be provided when creating a new network discovery, but only a single set of job specific credentials is allowed per network discovery.
- Job specific credentials take precedence over any configured global credentials.

- If the job specific credentials are provided as part of a network discovery and cause an authentication failure, then discovery is attempted a second time with the configured global credentials (if explicitly selected in the **Discovery** window of the controller's GUI). If discovery fails with the global credentials then the device discovery status will result in an authentication failure.
- When using Cisco APIC-EM APIs for a network discovery and the job specific credentials (both CLI and SNMP) are *not* provided as part of the network discovery, then the global credentials (both CLI and SNMP provided by the user) are used to authenticate devices.

Global Credential Rules

Table 1: Global Credential Rules

Global Credentials	Job Specific Credentials	Result
Not configured	Not configured	If the network discovery is run from the controller's GUI, then the default SNMP read community string (public) is used for the discovery scan. A discovery failure will not occur in this case. If the network discovery is run using Cisco APIC-EM APIs, then a discovery failure will occur since both CLI and SNMP credentials must be configured for a successful device discovery using the Cisco APIC-EM APIs.
Not configured	Configured	The specified job specific credentials will be used for discovery.
Configured	Not configured	All the configured global credentials will be used.
Configured but not selected	Configured	Only the job specific credentials will be used.
Configured and selected	Not configured	Only selected global credential will be used.
Configured and selected	Configured	Both specified credentials (global and job specific) will be used for discovery.
Configured, but wrong global credential IDs are mentioned in the discovery POST REST API.	Correct job specific credentials configured	Discovery fails. **Note** This scenario is only possible by API not from the controller GUI.

Global Credentials	Job Specific Credentials	Result
Configured, but wrong global credential IDs are mentioned in the discovery POST REST API.	Not configured	Discovery fails. **Note** This scenario is only possible by API not from the controller GUI.

Discovery Credentials Caveats

The following are caveats for the Cisco APIC-EM discovery credentials:

- If a device credential changes in a network device or devices after Cisco APIC-EM discovery is completed for that device or devices, any subsequent polling cycles for that device or devices will fail. To correct this situation, an administrator has following options:
  - Start a new discovery scan with changed job specific credentials that matches the new device credential.
  - Edit the existing discovery by updating or modifying the global credentials, and then rerun the discovery scan.
- If the ongoing discovery fails due to a device authentication failure (for example, the provided discovery credential is not valid for the devices discovered by current discovery), then the administrator has following options:
  - Stop or delete the current discovery. Create one or more new network discovery jobs (either a **CDP** or **Range** discovery type) with a job specific credential that matches the device credential.
  - Create a new global credential and execute a new discovery selecting the correct global credential.
  - Edit an existing global credential and re-run the discovery.
- Deleting a global credential does not affect already discovered devices. These already discovered devices will not report an authentication failure.
- The Cisco APIC-EM provides a REST API which allows the retrieval of the list of managed network devices in the Cisco APIC-EM inventory. The purpose of this API is to allow an external application to synchronize its own managed device inventory with the devices that have been discovered by the Cisco APIC-EM. For example, for Cisco IWAN scenarios, Prime Infrastructure makes use of this API in order to populate its inventory with the IWAN devices contained in the Cisco APIC-EM inventory in order to provide monitoring of the IWAN solution.

Note Only the username is provided in clear text. SNMP community strings and passwords are not provided in cleartext for security reasons.

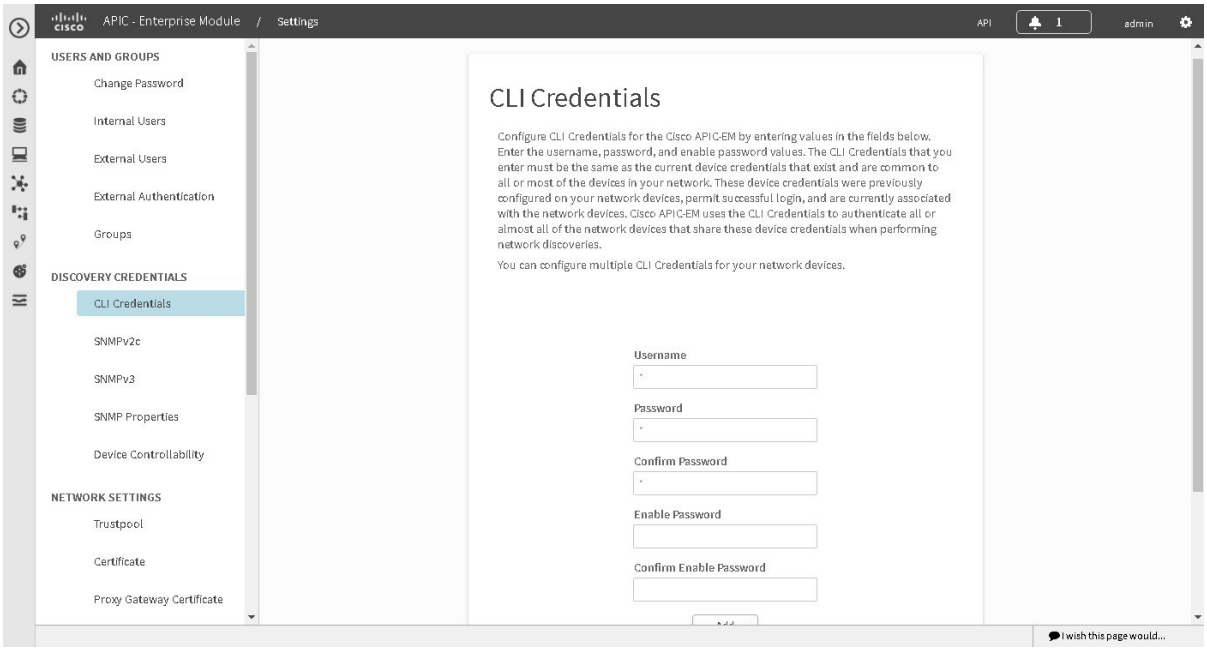
Configuring CLI Credentials—Global

CLI credentials are defined as preexisting *device* credentials that are common to most of the devices in a network. CLI credentials are used by the Cisco APIC-EM to authenticate and access the devices in a network that share this CLI credential when performing devices discoveries.

You configure the CLI global credentials in the **CLI Credentials** window or the **Discovery** window. This procedure describes how to configure CLI global credentials in the **CLI Credentials** window.

Note You can configure up to five CLI credentials.

Figure 12: CLI Credentials Window



Before you begin

You must have successfully deployed the Cisco APIC-EM and it must be operational.

You must have administrator (ROLE_ADMIN) permissions and either access to all resources (RBAC scope set to ALL) or an RBAC scope that contains all of the resources that you want to group. For example, to create a group containing a specific set of resources, you must have access to those resources (custom RBAC scope set to all of the resources that you want to group).

For information about user permissions and RBAC scopes required to perform tasks using the Cisco APIC-EM, see the chapter, "Managing Users".

Step 1 In the **Home** window, click either **admin** or the **Settings** icon (gear) at the top right corner of the screen.

Step 2 Click the **Settings** link from the drop-down menu.

Step 3 In the **Settings** navigation pane, click **CLI Credentials** to view the **CLI Credentials** window.

In the **CLI Credentials** window, enter the appropriate CLI global credentials for the devices within your network or networks.

Step 4 Enter the CLI Credentials username in the **Username** field.

Step 5 Enter the CLI Credentials password in the **Password** field.

Step 6 Reenter the CLI Credentials password in the **Confirm Password** field to confirm the value that you just entered.

Step 7 If your network devices have been configured with an enable password, then enter the CLI Credentials for the enable password in the **Enable Password** field.

Note Both the CLI credentials password and enable password are saved in the controller in encrypted form. You cannot view these original passwords after you enter them.

Step 8 If you entered an enable password in the **Enable Password** field, reenter it in the **Confirm Enable Password** field to confirm the value that you just entered.

Step 9 In the **CLI Credentials** window, click **Add** to save the credentials to the Cisco APIC-EM database.

What to do next

Proceed to configure SNMP values for your network device discovery.

For a successful device discovery (with all the device information to be collected), CLI credentials (global and/or job specific) should be configured using the controller. The global credentials for CLI and SNMP (v2c or v3) can be configured in the **Discovery Credentials** windows (as described in this chapter) or the **Discovery** window, and are used in addition to any job specific credentials (for CLI and SNMP) that are also configured in the **Discovery** window.

Configuring SNMP

You configure SNMP for device discovery using the following **Discovery Credentials** windows in the Cisco APIC-EM GUI:

- **SNMPv2c**
- **SNMPv3**
- **SNMP Properties**

Note You can also configure SNMP for device discovery in the **Discovery** window of the controller's GUI. For information about the procedures to configure SNMP for device discovery in the **Discovery** window, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Configuration Guide*.

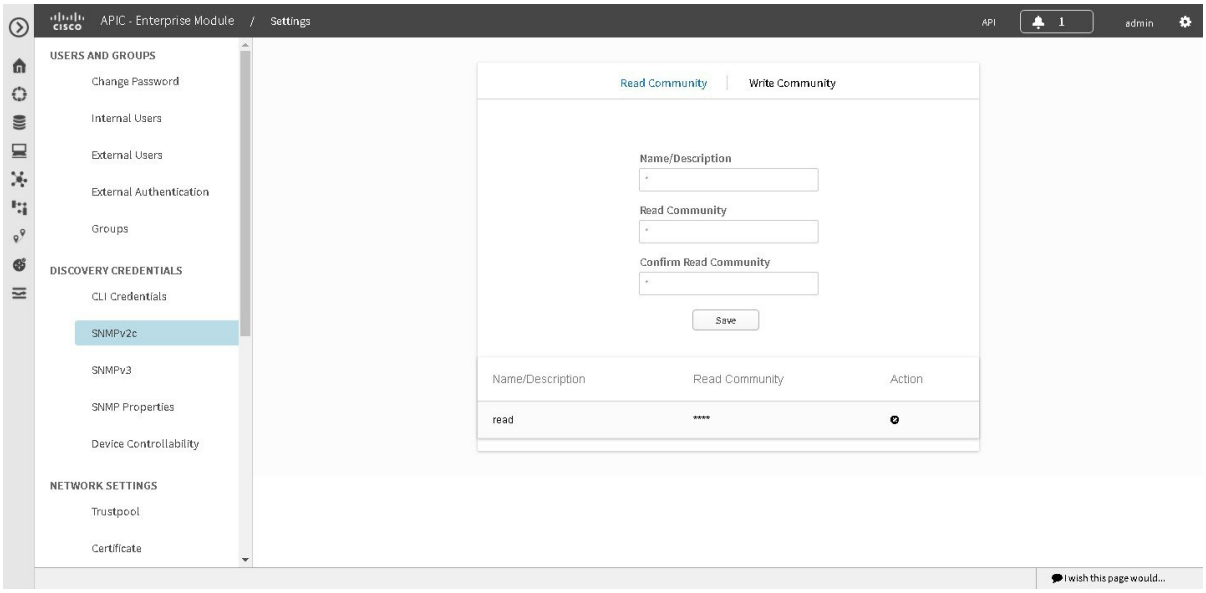
Important You can use SNMP and the existing security features in SNMP v3 to secure communications between the controller and the devices in your network. SNMP v3 provides both privacy (encryption) and authentication capabilities for these communications. If possible for your network, we recommend that you use SNMPv3 with both privacy and authentication enabled.

Configuring SNMPv2c

You configure SNMPv2c for device discovery in the **SNMPv2c** window in the Cisco APIC-EM GUI. The SNMP values that you configure for SNMPv2c for the controller must match the SNMPv2c values that have been configured for your network devices.

Note You can configure up to five read community strings and five write community strings.

Figure 13: Configuring SNMPv2c



SNMP is an application-layer protocol that provides a message format for communication between SNMP managers and agents. SNMP provides a standardized framework and a common language used for the monitoring and management of devices in a network. The different versions of SNMP are SNMPv1, SNMPv2, SNMPv2c, and SNMPv3.

SNMPv2c is the community string-based administrative framework for SNMPv2. Community string is a type of password, which is transmitted in clear text. SNMPv2c does not provide authentication or encryption (noAuthNoPriv level of security).

Note In addition to configuring SNMPv2c for device discovery in the controller, a "best effort" Cisco APIC-EM discovery is in place, meaning that devices having SNMP with Read-Only (RO) community string set to "public" will be discovered all the time irrespective of the configured SNMP Read/Write community string.

Before you begin

You must have successfully deployed the Cisco APIC-EM and it must be operational.

You must have your network's SNMP information available for this configuration procedure.

You must have administrator (ROLE_ADMIN) permissions and either access to all resources (RBAC scope set to ALL) or an RBAC scope that contains all of the resources that you want to group. For example, to create a group containing a specific set of resources, you must have access to those resources (custom RBAC scope set to all of the resources that you want to group).

For information about user permissions and RBAC scopes required to perform tasks using the Cisco APIC-EM, see the chapter, "Managing Users".

Step 1 In the **Home** window, click either **admin** or the **Settings** icon (gear) at the top right corner of the screen.

Step 2 Click the **Settings** link from the drop-down menu.

Step 3 In the **Settings** navigation pane, click **SNMPv2c** to view the **SNMPv2c** window.

Step 4 In the **SNMPv2c** window, click **Read Community**.

Enter your **Read Community** values:

- **Name/Description**—Description of the Read-Only (RO) community string value and/or the device or devices that are configured with it.
- **Read Community**—Read-Only community string value configured on devices that you need the controller to connect to and access. This community string value must match the community string value pre-configured on the devices that the controller will connect to and access.
- **Confirm Read Community**—Reenter the Read-Only community string to confirm the value that you just entered.

Note If you are configuring SNMPv2c for your discovery, then configuring **Read Community** values is mandatory.

Step 5 Click **Save** to save your **Read Community** values.

The **Read Community** values will appear in the table below.

Step 6 (Optional) In the **SNMPv2c** window, click **Write Community**.

Enter your **Write Community** values:

- **Name/Description**—Description of the Write community string value and/or the device or devices that are configured with it.
- **Write Community**—Write community string value configured on devices that you need the controller to connect to and access. This community string value must match the community string value pre-configured on the devices that the controller will connect to and access.
- **Confirm Write Community**—Reenter the Write community string to confirm the value that you just entered.

Step 7 (Optional) Click **Save** to save your **Write Community** values.

The **Write Community** values will appear in the table below.

What to do next

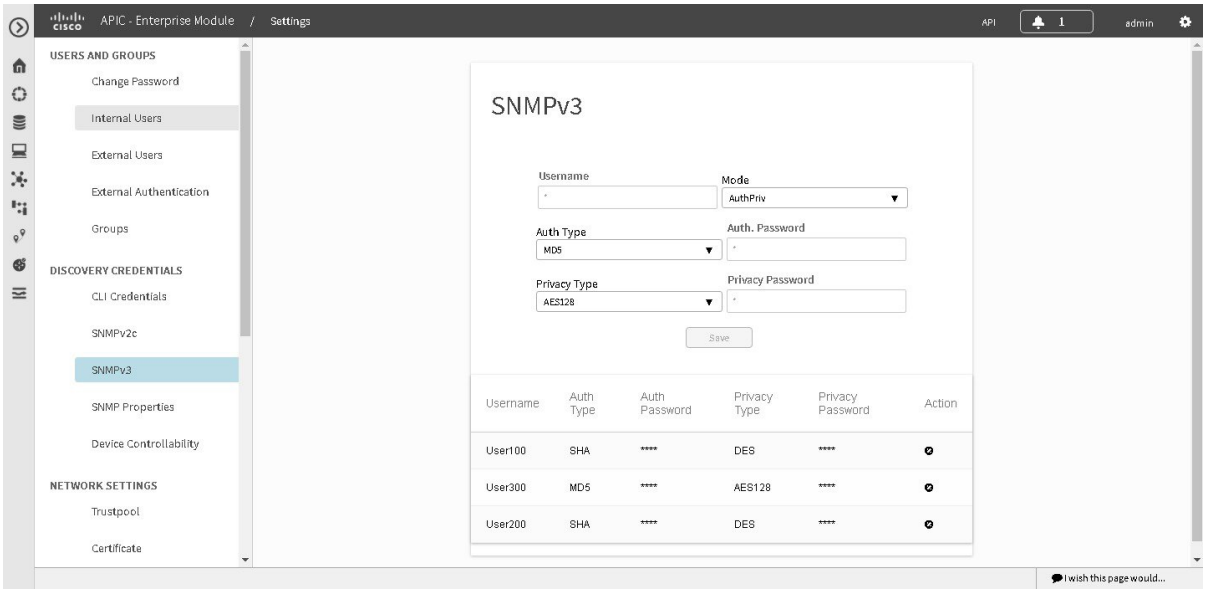
If required for your SNMP configuration, proceed to configure either **SNMPv3** or **SNMP Properties** using the GUI.

If you are finished with your SNMP configuration, then proceed to import an X.509 certificate and private key into the controller, if necessary for your network configuration.

Configuring SNMPv3

You configure SNMPv3 for device discovery in the **SNMPv3** window in the Cisco APIC-EM GUI. The SNMP values that you configure for SNMPv3 for the controller must match the SNMPv3 values that have been configured for your network devices. You can configure up to five SNMPv3 settings.

Figure 14: Configuring SNMPv3



SNMP is an application-layer protocol that provides a message format for communication between SNMP managers and agents. SNMP provides a standardized framework and a common language used for the monitoring and management of devices in a network. The different versions of SNMP are SNMPv1, SNMPv2, SNMPv2c, and SNMPv3.

SNMPv3 provides secure access to devices by a combination of authenticating and encrypting frames over the network. The following are supported SNMPv3 security models:

- Message integrity—Ensures that a packet has not been tampered with in-transit.
- Authentication—Determines the message is from a valid source
- Encryption—Scrambles the packet contents to prevent it from being seen by unauthorized sources

SNMPv3 provides for both security models and security levels. A security model is an authentication strategy that is set up for a user and the role in which the user resides. A security level is the permitted level of security within a security model. A combination of a security model and a security level determines which security mechanism is employed when handling an SNMP packet.

The security level determines if an SNMP message needs to be protected from disclosure and if the message needs to be authenticated. The various security levels that exist within a security model are as follows:

- noAuthNoPriv—Security level that does not provide authentication or encryption
- AuthNoPriv—Security level that provides authentication but does not provide encryption

- AuthPriv—Security level that provides both authentication and encryption

The following table identifies what the combinations of security models and levels mean:

Table 2: SNMP Security Models and Levels

Model	Level	Authentication	Encryption	What Happens
v2c	noAuthNoPriv	Community String	No	Uses a community string match for authentication.
v3	noAuthNoPriv	User Name	No	Uses a username match for authentication.
v3	AuthNoPriv	Either: • HMAC-MD5 • HMAC-SHA	No	Provides authentication based on the Hash-Based Message Authentication Code (HMAC) Message Digest 5 (MD5) algorithm or the HMAC Secure Hash algorithm (SHA)
v3	AuthPriv	Either: • HMAC-MD5 • HMAC-SHA	Either: • CBC-DES • CBC-AES-128	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Provides Data Encryption Standard (DES) 56-bit encryption in addition to authentication based on the Cipher Block Chaining (CBC) DES (DES-56) standard or CBC-mode AES for encryption.

Before you begin

You must have successfully deployed the Cisco APIC-EM and it must be operational.

You must have your network's SNMP information available for this configuration procedure.

You must have administrator (ROLE_ADMIN) permissions and either access to all resources (RBAC scope set to ALL) or an RBAC scope that contains all of the resources that you want to group. For example, to create

a group containing a specific set of resources, you must have access to those resources (custom RBAC scope set to all of the resources that you want to group).

For information about user permissions and RBAC scopes required to perform tasks using the Cisco APIC-EM, see the chapter, "Managing Users".

Note With SNMPv3, passwords (or passphrases) must be at least 8 characters in length (minimum). Additionally, for several Cisco Wireless LAN controllers, passwords (or passphrases) must be at least 12 characters in length (minimum). Failure to ensure these required minimum character lengths for the passwords will result in devices not being discovered, monitored, and/or managed by the controller.

Step 1 In the **Home** window, click either **admin** or the **Settings** icon (gear) at the top right corner of the screen.

Step 2 Click the **Settings** link from the drop-down menu.

Step 3 In the **Settings** navigation pane, click **SNMPv3** to view the **SNMPv3** window.

If you use SNMPv3 in your network to monitor and manage devices, then configure the SNMPv3 values for discovery for your network.

Step 4 In the **SNMPv3** window, enter a **Username** value and choose a **Mode** from the drop down menu.

The following **Mode** options are available:

- **AuthPriv**
- **AuthNoPriv**
- **NoAuthNoPriv**

Note Subsequent **SNMPv3** configuration options might or might not be available depending upon your selection for this step.

Step 5 If you selected **AuthPriv** or **AuthNoPriv** as a **Mode** option, then choose an **Authentication** type from the drop down menu and enter an authentication password.

The following **Authentication** options are available:

- **SHA**—Authentication based on the Hash-Based Message Authentication Code (HMAC), Secure Hash algorithm (SHA) algorithm
- **MD5**—Authentication based on the Hash-Based Message Authentication Code (HMAC), Message Digest 5 (MD5) algorithm

Step 6 If you selected **AuthPriv** as a **Mode** option, then choose a **Privacy** type from the drop down menu and enter a SNMPv3 privacy password.

The SNMPv3 privacy password is used to generate the secret key used for encryption of messages exchanged with devices that support DES or AES128 encryption.

The following **Privacy** type options are available:

- **DES**—Data Encryption Standard (DES) 56-bit encryption in addition to authentication based on the Cipher Block Chaining (CBC) DES (DES-56) standard.

- **AES128**—Cipher Block Chaining (CBC) mode AES for encryption.

Step 7 Click **Save** to save your SNMPv3 configuration values.

The **SNMPv3** configured values will appear in the table below.

What to do next

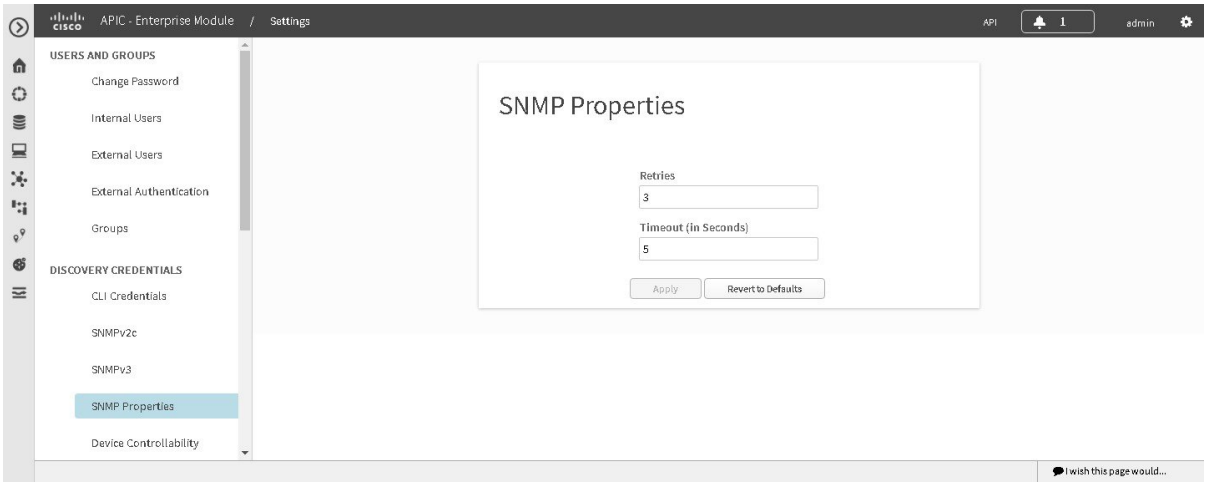
If required for your SNMP configuration, proceed to configure either **SNMPv2c** or **SNMP Properties** using the GUI.

If you are finished with your SNMP configuration, then proceed to import an X.509 certificate and private key into the controller, if necessary for your network configuration.

Configuring SNMP Properties

You configure SNMP properties for device discovery in the **SNMP Properties** window in the Cisco APIC-EM GUI.

Figure 15: Configuring SNMP Properties



Before you begin

You must have successfully deployed the Cisco APIC-EM and it must be operational.

You must have your network's SNMP information available for this configuration procedure.

You must have administrator (ROLE_ADMIN) permissions and either access to all resources (RBAC scope set to ALL) or an RBAC scope that contains all of the resources that you want to group. For example, to create a group containing a specific set of resources, you must have access to those resources (custom RBAC scope set to all of the resources that you want to group).

For information about user permissions and RBAC scopes required to perform tasks using the Cisco APIC-EM, see the chapter, "Managing Users".

Step 1 In the **Home** window, click either **admin** or the **Settings** icon (gear) at the top right corner of the screen.

Step 2 Click the **Settings** link from the drop-down menu.

Step 3 In the **Settings** navigation pane, click **SNMP Properties** to view the **SNMP Properties** window.

Configure the SNMP property settings for discovery in your network.

Step 4 In the **SNMP Properties** window, enter a value in the **Retries** field.

The value entered in this field is the number of attempts the controller attempts to use SNMP to communicate with your network devices.

Step 5 In the **SNMP Properties** window, enter a value in the **Timeout** field.

The value entered in this field is the length of time in seconds the controller attempts to use SNMP to communicate with your network devices.

Step 6 Click **Apply** to save your SNMP configuration values.

You can also click **Revert to Defaults** to revert to the SNMP property default values. The following are the SNMP property default values:

- **Retries**—3
- **Timeout**—5

What to do next

If required for your SNMP configuration, proceed to configure either **SNMPv2c** or **SNMPv3** using the GUI.

If you are finished with your SNMP configuration, then proceed to import an X.509 certificate and private key into the controller, if necessary for your network configuration.

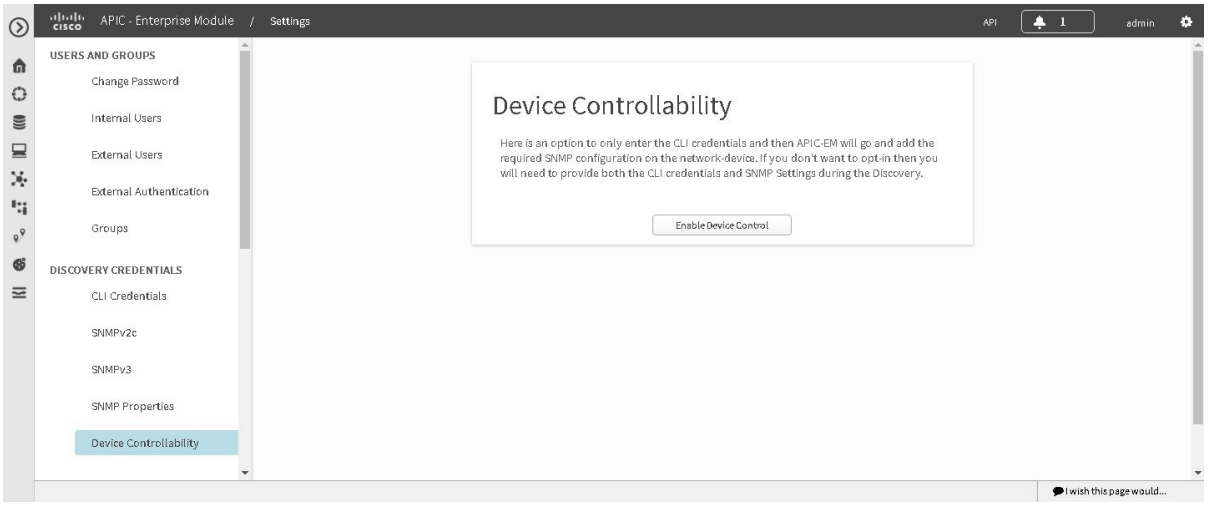
Enabling Device Controllability

You can enable device controllability using the Cisco APIC-EM GUI. When you enable device controllability, the controller automatically configures (applies) the SNMP credentials that you entered using the controller's GUI on any network devices without SNMP credentials or without matching SNMP credentials.

Note The device controllability functionality depends upon whether the CLI credentials provided by the user permits the controller to log into the device in enable mode (privilege level 15 for Cisco IOS devices).

You can enable device controllability for device discovery in the **Device Controllability** window in the Cisco APIC-EM GUI

Figure 16: Enabling Device Controllability



Before you begin

You must have successfully deployed the Cisco APIC-EM and it must be operational.

You must have administrator (ROLE_ADMIN) permissions and either access to all resources (RBAC scope set to ALL) or an RBAC scope that contains all of the resources that you want to group. For example, to create a group containing a specific set of resources, you must have access to those resources (custom RBAC scope set to all of the resources that you want to group).

For information about user permissions and RBAC scopes required to perform tasks using the Cisco APIC-EM, see the chapter, "Managing Users".

Step 1 In the **Home** window, click either **admin** or the **Settings** icon (gear) at the top right corner of the screen.

Step 2 Click the **Settings** link from the drop-down menu.

Step 3 In the **Settings** navigation pane, click **Device Controllability** to view the **Device Controllability** window.

Step 4 Click **Enable Device Control** to enable this feature.

What to do next

If you have not already done so, configure SNMP in either the **Discovery** window or the appropriate **CLI Credentials** window for SNMP in **Settings**.

Network Settings

Importing the Controller's Server Certificate

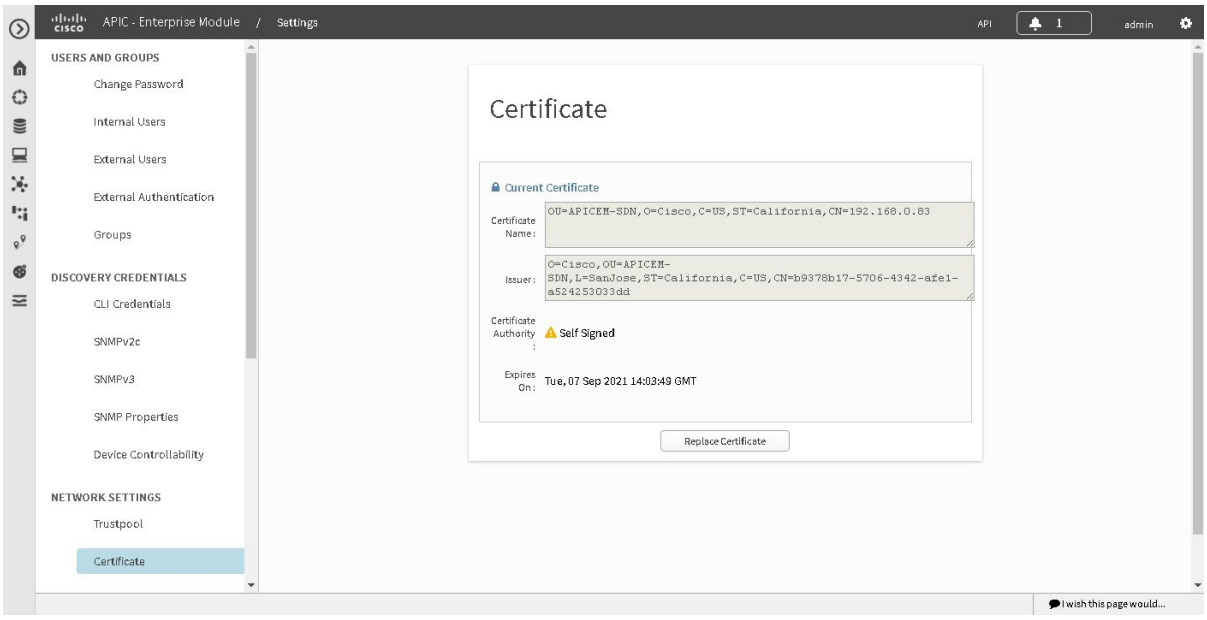
The Cisco APIC-EM supports the import and storing of an X.509 certificate and private key into the controller. After import, the certificate and private key can be used to create a secure and trusted environment between the Cisco APIC-EM, NB API applications, and network devices.

Note If you have a multi-host deployment and you plan to acquire a valid CA-issued certificate for your controller HTTPS server, then use the virtual IP address that you assigned to the multi-hosts as the Common Name for the certificate when you order. If you are using a host name instead, make sure the host name is DNS-resolvable to the virtual IP address of the multi-host deployment.

If you already have a single host Cisco APIC-EM with a previously purchased CA-issued certificate for its external IP address, then it is ideal to use that original physical IP address of the single host as the virtual IP address of the multi-host deployment. This way you can save your investment in the CA-issued certificate and external client applications can continue using the same IP address to access your Cisco APIC-EM services.

You import a certificate and private key using the **Certificate** window in the Cisco APIC-EM GUI.

Figure 17: Certificate Configuration Window



Important The Cisco APIC-EM itself does NOT interact with any external CA directly; therefore, it does not check any Certificate Revocation Lists and it has no way to learn of revocation of its server certificate by an external CA. Note, also, that the controller does not automatically update its server certificate. Replacement of an expired or revoked server certificate requires explicit action on the part of a ROLE_ADMIN user. Although the controller has no direct means of discovering the revocation of its server certificate by an external CA, it does notify the admin of expiration of its server certificate as well as self-signed key being operational.

Before you begin

You must have successfully deployed the Cisco APIC-EM and it must be operational.

You must have acquired an X.509 certificate and private key from a well-known certificate authority (CA) for the import.

You must have administrator (ROLE_ADMIN) permissions and either access to all resources (RBAC scope set to ALL) or an RBAC scope that contains all of the resources that you want to group. For example, to create a group containing a specific set of resources, you must have access to those resources (custom RBAC scope set to all of the resources that you want to group).

For information about user permissions and RBAC scopes required to perform tasks using the Cisco APIC-EM, see the chapter, "Managing Users".

Step 1 In the **Home** window, click either **admin** or the **Settings** icon (gear) at the top right corner of the screen.

Step 2 Click the **Settings** link from the drop-down menu.

Step 3 In the **Settings** navigation pane, click **Certificate** to view the **Certificate** window.

Step 4 In the **Certificate** window, view the current certificate data.

When first viewing this window, the current certificate data that is displayed is the controller's self-signed certificate. The self-signed certificate's expiration is set for several years in the future.

Note The **Expiration Date and Time** is displayed as a Greenwich Mean Time (GMT) value. A system notification will appear in the controller's GUI 2 months before the expiration date and time of the certificate.

Additional displayed fields in the **Certificate** window include:

- Certificate Name—The name of the certificate.
- Issuer—The issuer name identifies the entity that has signed and issued the certificate.
- Certificate Authority—Either self-signed or name of the CA.
- Expires On—Expiration date of the certificate.

Step 5 To replace the current certificate, click the **Replace Certificate** button.

The following new fields appear:

- **Certificate**—Fields to enter certificate data
- **Private Key**—Fields to enter private key data

Step 6 In the **Certificate** fields, choose the file format type of the certificate:

- **PEM**—Privacy enhanced mail file format
- **PKCS**—Public-key cryptography standard file format

Choose one of the above file types for the certificate that you are importing into the Cisco APIC-EM.

Step 7 If you choose **PEM**, then perform the following tasks:

- For the **Certificate** field, import the **PEM** file by dragging and dropping this file into the **Drag n' Drop a File Here** field.

  Note For a PEM file, it must have a valid PEM format extension (.pem, .cert, .crt). The maximum file size for the certificate is 10KB

- For the **Private Key** field, import the private key by dragging and dropping this file into the **Drag n' Drop a File Here** field.
  - Choose the encryption option from the **Encrypted** drop-down menu for the private key.
  - If encryption is chosen, enter the passphrase for the private key in the **Passphrase** field.

    Note For the private keys, they must have a valid private key format extension (.pem or .key).

Step 8 If you choose **PKCS**, then perform the following tasks:

- For the **Certificate** field, import the **PKCS** file by dragging and dropping this file into the **Drag n' Drop a File Here** field.

  Note For a PKCS file, it must have a valid PKCS format extension (.pfx, .p12). The maximum file size for the certificate is 10KB

- For the **Certificate** field, enter the passphrase for the certificate using the **Passphrase** field.

  Note For PKCS, the imported certificate also requires a passphrase.

- For the **Private Key** field, choose the encryption option for the private key using the drop-down menu.
- For the **Private Key** field, if encryption is chosen, enter the passphrase for the private key in the **Passphrase** field.

Step 9 Click the **Upload/Activate** button.

Step 10 Return to the **Certificate** window to view the updated certificate data.
The information displayed in the **Certificate** window should have changed to reflect the new certificate name, issuer, and certificate authority.

Related Topics

Cisco APIC-EM Controller Certificate and Private Key Support
Cisco APIC-EM Controller Certificate Chain Support
Obtaining a CA-Signed Certificate for the Cisco APIC-EM Controller

Importing a Trustpool Bundle

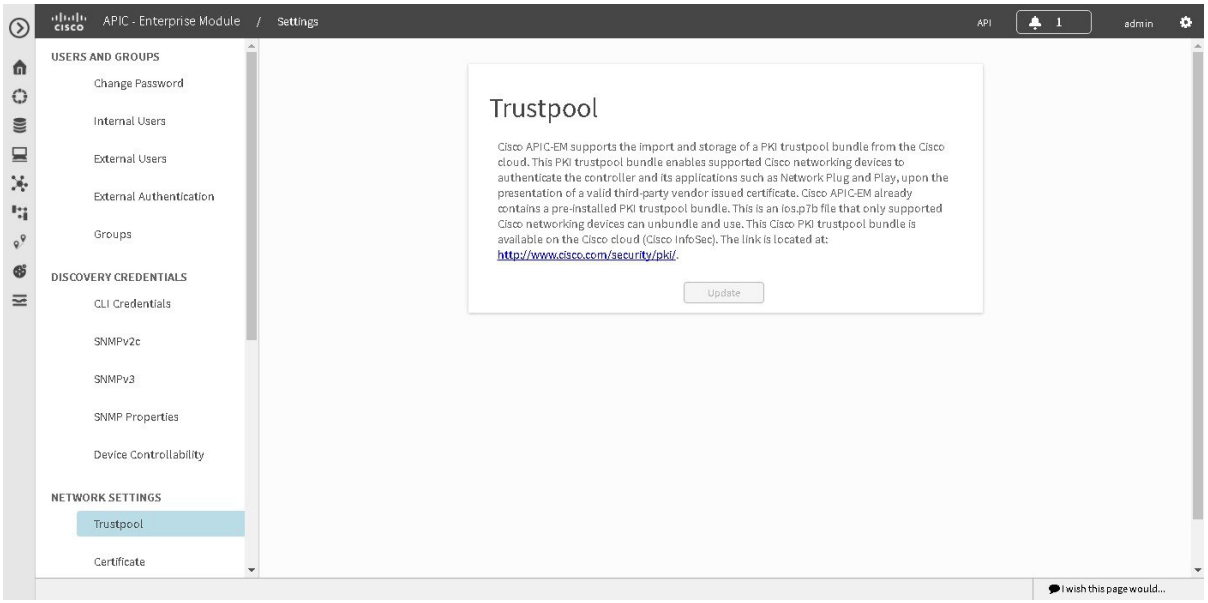
The Cisco APIC-EM contains a pre-installed Cisco trustpool bundle (Cisco Trusted External Root Bundle). The Cisco APIC-EM also supports the import and storage of an updated trustpool bundle from Cisco. The trustpool bundle is used by supported Cisco networking devices to establish a trust relationship with the controller and its applications, such as Network PnP.

Note The Cisco trustpool bundle is an ios.p7b file that only supported Cisco devices can unbundle and use. This ios.p7b file contains root certificates of valid certificate authorities including Cisco itself. This Cisco trustpool bundle is available on the Cisco cloud (Cisco InfoSec). The link is located at: http://www.cisco.com/security/pki/.

The trustpool bundle provides you with a safe and convenient way to use the same CA to manage all your network device certificates, as well as your controller certificate. The trustpool bundle is used by the controller to validate its own certificate as well as a proxy gateway certificate (if any), to determine whether it is valid CA signed certificate or not. Additionally, the trustpool bundle is available to be uploaded to the Network PnP enabled devices at the beginning of their PnP workflow so that they can trust the controller for subsequent HTTPS-based connections.

You import the Cisco trust bundle using the **Trustpool** window in the Cisco APIC-EM GUI.

Figure 18: Trustpool Window



Before you begin

You must have successfully deployed the Cisco APIC-EM and it must be operational.

You must have administrator (ROLE_ADMIN) permissions and either access to all resources (RBAC scope set to ALL) or an RBAC scope that contains all of the resources that you want to group. For example, to create a group containing a specific set of resources, you must have access to those resources (custom RBAC scope set to all of the resources that you want to group).

For information about user permissions and RBAC scopes required to perform tasks using the Cisco APIC-EM, see the chapter, "Managing Users".

Step 1 In the **Home** window, click either **admin** or the **Settings** icon (gear) at the top right corner of the screen.

Step 2 Click the **Settings** link from the drop-down menu.

Step 3 In the **Settings** navigation pane, click **Trustpool** to view the **Trustpool** window.

Step 4 In the **Trustpool** window, view the **Update** button.

The **Update** button in the controller's **Trustpool** window becomes active when an updated version of ios.p7b file is available and Internet access is available. The **Update** button remains inactive if there is no Internet access or if there is no updated version of the ios.p7b file.

Step 5 Click the **Update** button to initiate a new download and install of the trustpool bundle.

Note After the new trustpool bundle is downloaded and installed on the controller, the controller then makes this trustpool bundle available to the supported Cisco devices to download.

Related Topics

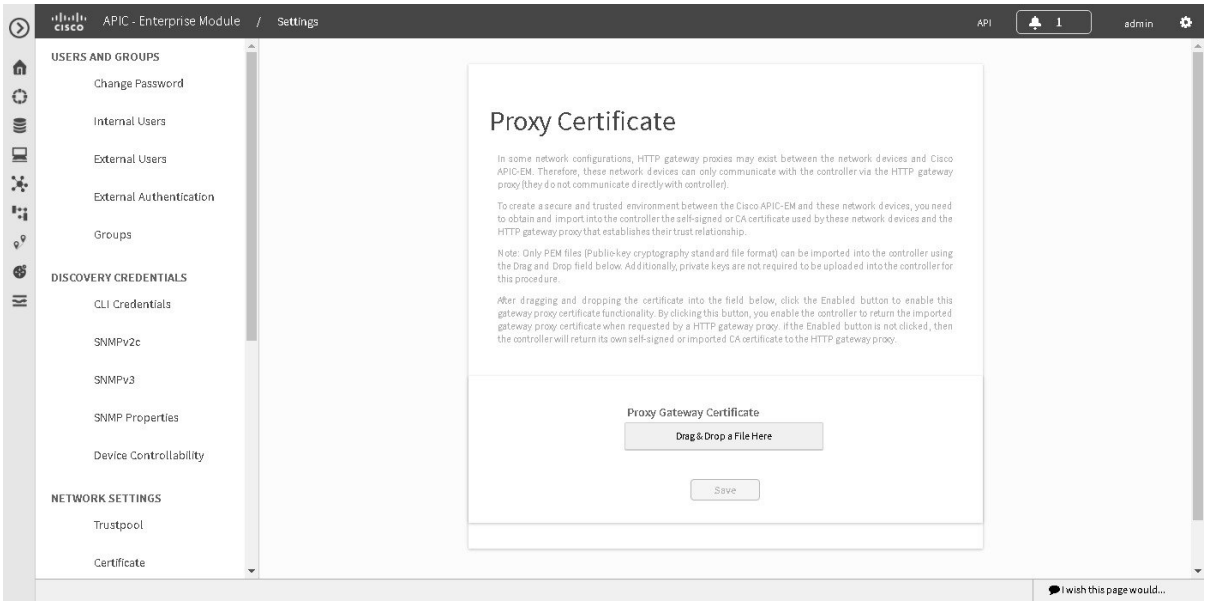
Cisco APIC-EM Trustpool Support

Importing a Proxy Gateway Certificate

In some network configurations, proxy gateways may exist between the Cisco APIC-EM and the remote network it manages (containing IWAN and PnP network devices). Common ports such as 80 and 443 pass through the gateway proxy in the DMZ, and for this reason SSL sessions from the network devices meant for the controller terminate at the proxy gateway. Therefore, the network devices located within these remote networks can only communicate with the controller via the proxy gateway. In order for the network devices to establish secure and trusted connections with the controller, or if present, a proxy gateway, then the network devices should have their PKI trust stores appropriately provisioned with the relevant CA root certificates or the server's own certificate under certain circumstances.

In network topologies where there is a proxy gateway present between controller and the remote network it manages, follow the procedure below to import a proxy gateway certificate into the controller.

Figure 19: Proxy Gateway Certificate Window



Before you begin

You have successfully deployed the Cisco APIC-EM and it is operational.

In your network, an HTTP proxy gateway exists between the controller and the remote network it manages (containing IWAN and PnP network devices) . These network devices will use the proxy gateway's IP address to reach the Cisco APIC-EM controller and its services.

You have the certificate file currently being used by the proxy gateway. The certificate file contents can consist any of the following:

- The proxy gateways’s certificate in PEM format, with the certificate being self-signed.
- The proxy gateway’s certificate in PEM format, with the certificate being issued by a valid, well-known CA.
- The proxy gateway's certificate and its chain in PEM format.

The certificate used by the devices and proxy gateway must be imported into the controller by following this procedure.

Step 1 In the **Home** window, click either **admin** or the **Settings** icon (gear) at the top right corner of the screen.

Step 2 Click the **Settings** link from the drop-down menu.

Step 3 In the **Settings** navigation pane, click **Proxy Gateway Certificate** to view the **Proxy Certificate** window.

Step 4 In the **Proxy Gateway Certificate** window, view the current proxy gateway certificate data (if this exists).

Note The **Expiration Date and Time** is displayed as a Greenwich Mean Time (GMT) value. A system notification will appear in the controller's GUI 2 months before the expiration date and time of the certificate.

Step 5 To add a proxy gateway certificate, drag and drop the self-signed or CA certificate to the **Drag n' Drop a File Here** field.

Note Only PEM files (Public-key cryptography standard file format) can be imported into the controller using this field. Additionally, private keys are neither required nor uploaded into the controller for this procedure.

Step 6 Click the **Save** button.

Step 7 Refresh the **Proxy Gateway Certificate** window to view the updated proxy gateway certificate data.
The information displayed in the **Proxy Gateway Certificate** window should have changed to reflect the new certificate name, issuer, and certificate authority.

Related Topics

Security and Cisco Network Plug and Play

PKI Certificate Management

The Cisco APIC-EM provides PKI-based connections in the following distinct PKI planes:

- Controller PKI Plane—With this plane, there exists HTTPS connections in which the controller is the server in the client-server model, and the controller's server certificate secures the connection.
- Device PKI Plane—With this plane, there exists DMVPN connections between devices in the control plane of the network, bilaterally authenticated and secured by the device ID certificates of both devices that participate in the connection. These certificates/keys are issued by a private CA that the Cisco APIC-EM controller provides (Device PKI CA).

The PKI certificate management procedures described in this section only involves the Device PKI plane and include:

- Changing the private CA from a root CA to a subordinate CA. This procedure requires that you replace the CA certificate of the private CA with one signed by the external CA.
- Changing the lifetime of the device ID certificates that secure device-to-device connections between IWAN-managed devices.

Changing the Role of the PKI Certificate from Root to Subordinate

The Cisco APIC-EM permits the user to change the role of the Device PKI CA from a root CA to a subordinate CA.

When changing the private controller's CA from a root CA to a subordinate CA note the following:

- If you intend to have the controller act as a subordinate CA, then it is assumed that you already have a root CA (for example Microsoft CA) and you are willing to accept the controller as a subordinate CA.
- As long as the the subordinate CA is not fully configured, then the controller will continue to operate as an internal root CA.
- You will need to generate a Certificate Signing Request (CSR) file for the controller (as described in this procedure) and manually have it signed by your external root CA.

Note The controller will continue to run as an internal root CA during this time.

- Once the CSR is signed by the external root CA, then this signed file must be imported back into the controller using the GUI (as described below in this procedure).

  After the import, the controller will initialize itself as the subordinate CA and provide all the existing functionality of a subordinate CA.

- The switch over from internal root CA to subordinate CA is not automatically supported; therefore, it is assumed that no devices have yet been configured with the internal root CA. In case any devices are configured, then it is the responsibility of the network administrator to manually revoke the existing device ID certificates before switching to the subordinate CA.

- Note that there is no rollover provisioning for the subordinate CA, so for this reason we recommend that you choose the longest possible certificate lifetime for subordinate certificate, and not less than 2 years.

- There is no controller warning for expiration of the subordinate CA certificate.

- The subordinate CA certificate lifetime as displayed in the GUI is just read from the certificate itself; it is not computed against the system time. So if you install a certificate with a lifespan of one year today and then look at it in the GUI next July, then the GUI will still show that the certificate has a one year lifetime.

- The subordinate CA certificate should be in PEM format only.

- Due to a Cisco IOS XE crypto PKI import limitation, devices cannot import a PKCS bundle (made up of a device certificate, device key and the subordinate CA certificate) exceeding 4KB size. This problem occurs when the Cisco APIC-EM device PKI CA is changed to SubCA mode with a subordinate CA certificate that has several and/or lengthy X509 attributes defined, thereby increasing the size of the device PKCS bundle beyond 4KB. To circumvent this issue, get the subordinate CA certificate issued with very minimal attributes. For example, do not include CDP distribution and OCSP settings.

  The following command output is provided as an example of content from a subordinate CA certificate that can impact the file size, as well as the fields within the certificate where content should be minimized:

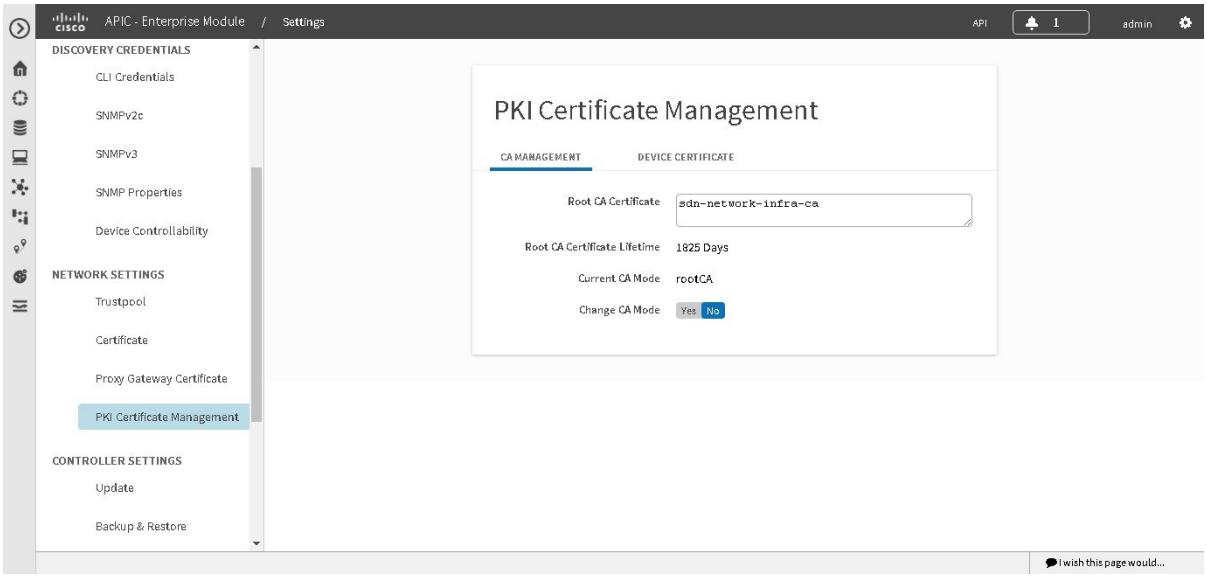
```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            2e:00:00:00:0e:28:d7:1f:24:a1:1e:ef:70:00:00:00:00:00:0e
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: DC=com, DC=apic-em, CN=apic-em-CA
        Validity
            Not Before: Oct 18 19:56:54 2016 GMT
            Not After : Oct 19 19:56:54 2016 GMT
        Subject: CN=sdn-network-infra-subca
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:cd:a7:65:a4:c4:64:e6:e0:6b:f2:39:c0:a2:3b:
                    <snip>
                    85:a3:44:d1:a2:b3:b1:f5:ff:28:e4:12:41:d3:5f:
                    bf:e9
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                D2:DD:FA:E4:A5:6A:3C:81:29:51:B2:17:ED:82:CE:AA:AD:91:C5:1D
            X509v3 Authority Key Identifier:
                keyid:62:6F:C7:83:42:82:5F:54:51:2B:76:B2:B7:F5:06:2C:76:59:7F:F8

            X509v3 Basic Constraints: critical
```

```
            CA:TRUE
        X509v3 Key Usage: critical
            Digital Signature, Certificate Sign, CRL Sign
        1.3.6.1.4.1.311.21.7:
            0-.%+.....7.....#...I......^...Q...._...S..d...
Signature Algorithm: sha256WithRSAEncryption
     18:ce:5b:90:6b:1d:5b:b4:df:fa:d3:8e:80:51:6f:46:0d:19:
```

- The subordinate CA does not interact with the higher CAs, so it will not be aware of any revocation of the certificates at a higher level. Due to this fact, any information about certificate revocation will also not be communicated from the subordinate CA to the network devices. Since the subordinate CA does not have this information, all the network devices will only use the subordinate CA as the CDP source.

You change the role of the private (internal) controller's CA from a root CA to a subordinate CA using the **PKI Certificate Managment** window in the Cisco APIC-EM GUI.

Figure 20: PKI Certificate Management Window



Before you begin

You must have successfully deployed the Cisco APIC-EM and it must be operational.

You must have administrator (ROLE_ADMIN) permissions and either access to all resources (RBAC scope set to ALL) or an RBAC scope that contains all of the resources that you want to group. For example, to create a group containing a specific set of resources, you must have access to those resources (custom RBAC scope set to all of the resources that you want to group).

For information about user permissions and RBAC scopes required to perform tasks using the Cisco APIC-EM, see the chapter, "Managing Users".

You must have a copy of the root CA certificate to which you will subordinate the private (internal) controller's PKI certificate.

Step 1 In the **Home** window, click either **admin** or the **Settings** icon (gear) at the top right corner of the screen.

Step 2 Click the **Settings** link from the drop-down menu.

Step 3 In the **Settings** navigation pane, click **PKI Certificate Management** to view the **PKI Certificate Management** window.

Step 4 Click the **CA Management** tab.

Step 5 Review the existing root or subordinate CA certificate configuration information from the GUI.

Root CA Certificate	Displays current root CA certificate (either external or internal root CA certificate).
Root CA Certificate Lifetime	Displays the current lifetime value of the current root CA certificate in days.
Current CA Mode	Displays the current CA mode: root CA or subordinate CA.
Change to Sub CA mode	Button used to change from a root CA to subordinate CA.

Step 6 In the **CA Management** tab, for **Change to Sub CA mode** click **Yes**.

Step 7 In the **CA Management** tab, click **Next**.

Step 8 Review the **Root CA to Sub CA** warnings that appears:

- Changing from root CA to subordinate CA is a process that cannot be reversed.
- You must ensure that no network devices have been enrolled or issued a certificate in root CA mode. Any network devices accidently enrolled in root CA mode must be revoked before changing from root CA to subordinate CA.
- Network devices must come online only after this subordinate CA configuration process is finished.

Step 9 Click **OK** to proceed.

The **PKI Certificate Management** window changes and displays an **Import External Root CA Certificate** field.

Step 10 Drag and drop your root CA certificate into the **Import External Root CA Certificate** field and click **Upload**.

The root CA certificate will then be uploaded into the controller and used to generate a Certificate Signing Request (CSR).

When the upload process is finished a **Certificate Uploaded Successfully message** appears.

Step 11 After the upload process is finished and the success message appears, click **Next** to proceed.

The controller will then generate and display the CSR.

Step 12 View the controller generated Certificate Signing Request (CSR) in the GUI and perform one of the following actions:

- Click the **Download** link to download a local copy of the CSR file.

  You can then attach this CSR file to an email to send to your root CA.
- Click the **Copy to the Clipboard** link to copy the CSR file's content.

  You can then paste this CSR content to an email or attachment to an email and send to your root CA.

Step 13 Send the CSR file to your root CA.

You must send the CSR file to your root CA. Your root CA will then return to you a subordinate CA file that you must import back into the controller.

Step 14 After receiving the subordinate CA file from your root CA, access the controller's GUI again and return to the **PKI Certificate Management** window.

Step 15 Click the **CA Management** tab.

Step 16 Click **Yes** for the **Change CA mode** button in the **CA Management** tab.

After clicking **Yes**, the GUI view with the CSR is displayed.

Step 17 Click **Next** in the GUI view with the CSR being displayed.

The **PKI Certificate Management** window changes and displays an **Import Sub CA Certificate** field.

Step 18 Drag and drop your subordinate CA certificate into the **Import Sub CA Certificate** field and click **Apply**.

The subordinate CA certificate will then be uploaded into the controller.

After the upload finishes, the GUI window changes to display the subordinate CA mode in the **CA Management** tab.

Step 19 Review the fields in the **CA Management** tab.

Sub CA Certificate	Displays current subordinate CA certificate.
External Root CA Certificate	Displays Root CA certificate.
Sub CA Certificate Lifetime	Displays the lifetime value of the subordinate CA certificate in days.
Current CA Mode	Displays SubCA mode.

Related Topics

Device PKI Plane Modes

Viewing the Device Certificate Lifetime

The Cisco APIC-EM enables the user to view the certificate lifetime of network devices managed and monitored by the private (internal) controller's CA. The controller's default value for the certificate lifetime is 365 days.

Note You cannot change the certificate lifetime default value.

Before you begin

You must have successfully deployed the Cisco APIC-EM and it must be operational.

You must have administrator (ROLE_ADMIN) permissions and either access to all resources (RBAC scope set to ALL) or an RBAC scope that contains all of the resources that you want to group. For example, to create a group containing a specific set of resources, you must have access to those resources (custom RBAC scope set to all of the resources that you want to group).

For information about user permissions and RBAC scopes required to perform tasks using the Cisco APIC-EM, see the chapter, "Managing Users".

Step 1 In the **Home** window, click either **admin** or the **Settings** icon (gear) at the top right corner of the screen.

Step 2 Click the **Settings** link from the drop-down menu.

Step 3 In the **Settings** navigation pane, click **PKI Certificate Management** to view the **PKI Certificate Management** window.

Step 4 Click the **Device Certificate** tab.

Step 5 From here, you can review the device certificate and current device certificate lifetime.

Related Topics

Device PKI Plane Modes

Logs and Logging

The Cisco APIC-EM generates the following log types that are accessible through the GUI:

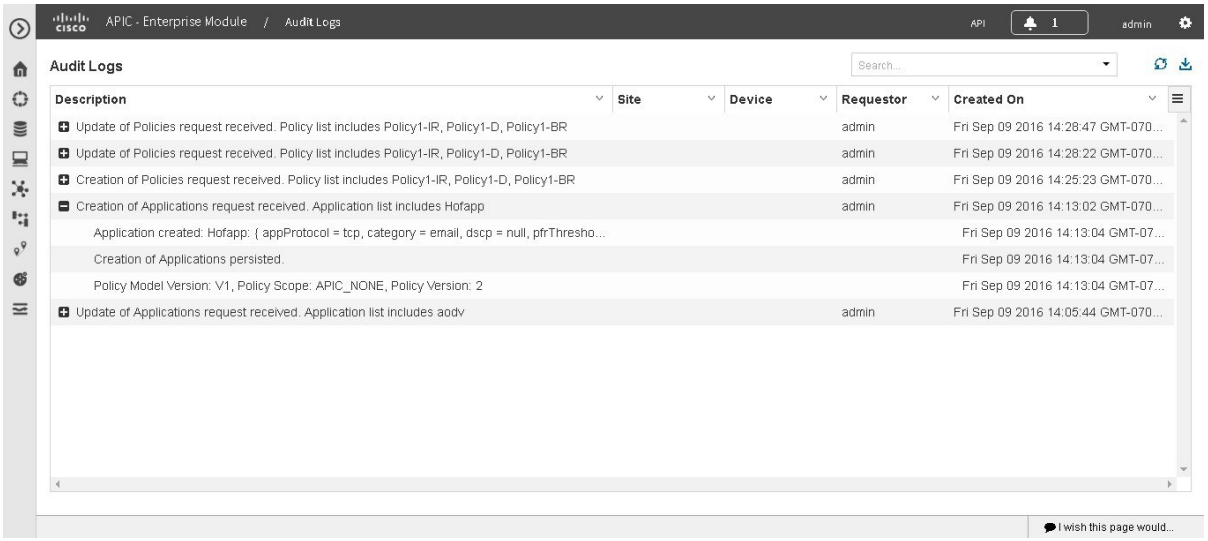
- Audit Logs—Logs used primarily to monitor policy creation and application.
- Service Logs—Logs used to monitor the controller services.

Viewing Audit Logs

Audit logs capture information about the various ; applications (EasyQoS, PnP and IWAN). Additionally, the audit logs also capture information about device PKI notifications. The information in these audit logs can be used to assist in troubleshooting any issues involving the applications or device PKI certificates.

You can view audit logs using the **Audit Logs** window in the Cisco APIC-EM GUI. The Cisco APIC-EM also supports the ability to export the audit logs to a local system.

Figure 21: Audit Logs Window



Before you begin

You must have successfully deployed the Cisco APIC-EM and it must be operational.

You must have either administrator (ROLE_ADMIN), policy administrator (ROLE_POLICY_ADMIN), or Observer (ROLE_OBSERVER) permissions and the appropriate resource scope to perform this procedure.

Step 1 In the **Home** window, click either **admin** or the **Settings** icon (gear) at the top right corner of the screen.

Step 2 Click the **Audit Logs** link from the drop-down menu.

The **Audit Logs** window appears. In the **Audit Logs** window, you can view logs about the current policies in your network. These policies were applied to network devices by either the IWAN or EasyQoS applications.

The following information is displayed for each policy in the window:

- **Description**—Application or policy audit log description
- **Site**—Name of site for the specific audit log
- **Device**—Device or devices for the audit log
- **Requestor**—User requesting audit log
- **Created On**—Date application or policy audit log was created.

Step 3 Click on the addition icon (+) next to an audit log to view the children audit logs in the **Audit Logs** window.

Each audit log can be a parent to several child audit logs. By clicking on this icon, you can view a series of additional children audit logs.

Note An audit log captures data about a task performed by the controller. Children audit logs are sub-tasks to that one task performed by the controller.

Step 4 Perform a search of the audit logs by clicking on the **Search** field in the **Audit Logs** window, entering a specific parameter, and then clicking the **Submit** button.

You can search for a specific audit log by the following parameters:

- Description
- Requestor
- Device
- Site
- Start Date
- End Date

Step 5 Click on the dual arrow icon to refresh the data displayed in the window.

The data displayed in the window is refreshed with the latest audit log data.

Step 6 Click on the down arrow icon to download a local copy of the audit log in .csv file format.

A .csv file containing audit log data is downloaded locally to your system. You can use the .csv file for additional review of the audit log or archive it as a record of activity on the controller.

What to do next

Proceed to review any additional log files using the controller's GUI, or download individual audit logs as .csv files for further review or archiving purposes.

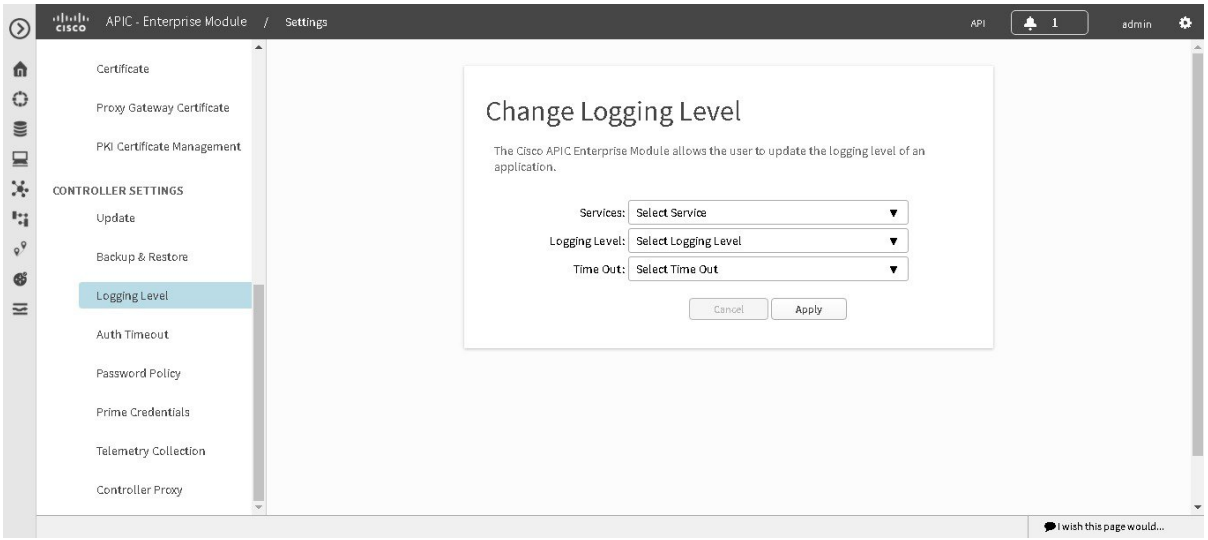
Changing the Logging Level for Services

You can change the logging level for the Cisco APIC-EM services by using the **Changing the Logging Level** window in the Cisco APIC-EM GUI.

A logging level determines the amount of data that is captured to the controller's log files. Each logging level is cumulative, that is, each level contains all the data generated by the specified level and any higher levels. For example, setting the logging level to **Info** also captures **Warn** and **Error** logs.

You may want to adjust the logging level to assist in troubleshooting any issues by capturing more data. For example, by adjusting the logging level you can capture more data to review in a root cause analysis or rca support file.

Figure 22: Service Logging Level Window



The default logging level for services in the controller is informational (**Info**). You can change the logging level with the GUI to set it to debug or trace to capture more information.

Caution Any logs collected at the **Debug** level or higher should be handled with restricted access.

Note The log files are created and stored in a centralized location on your controller. From this location, the controller can query and display them in the GUI. The total compressed size of the log files is 2GB. If log files created are in excess of 2GB, then the pre-existing log files are overwritten with the newer log files.

Note The log files are created and stored in a centralized location on your controller. From this location, the controller can query and display them in the GUI The total compressed size of the log files is 2GB. If log files created are in excess of 2GB, then the pre-existing log files are overwritten with the newer log files.

Before you begin

You must have successfully deployed the Cisco APIC-EM and it must be operational.

You must have either administrator (ROLE_ADMIN) or policy administrator (ROLE_POLICY_ADMIN) permissions and the appropriate RBAC scope to perform this procedure.

For information about user permissions and RBAC scopes required to perform tasks using the Cisco APIC-EM, see the chapter, "Managing Users".

Step 1 In the **Home** window, click either **admin** or the **Settings** icon (gear) at the top right corner of the screen.

Step 2 Click the **Settings** link from the drop-down menu.

Step 3 In the **Settings** navigation pane, click **Changing the Logging Level** to view the **Changing Logging Level** window.

The **Logging Level** table appears with the following fields:

- **Services**
- **Logging Level**
- **Timeout**

Step 4 In the **Changing Logging Level** window, choose a service from the **Services** field to adjust its logging level.

Note The **Services** field displays any services that are currently configured and running on the controller.

Step 5 In the **Changing Logging Level** window, choose the new logging level for the service from the **Logging Level** field.

The following logging levels are supported on the controller:

- **Trace**—Trace messages
- **Debug**—Debugging messages
- **Info**—Normal but significant condition messages
- **Warn**—Warning condition messages
- **Error**—Error condition messages

Step 6 In the **Changing Logging Level** window, choose the time period for the logging level from the **Timeout** field for the logging level adjustment.

You configure logging level time periods in increments of 15 minutes up to an unlimited time period.

Step 7 Review your selection and click the **Apply** button.

To cancel your selection click the **Cancel** button.

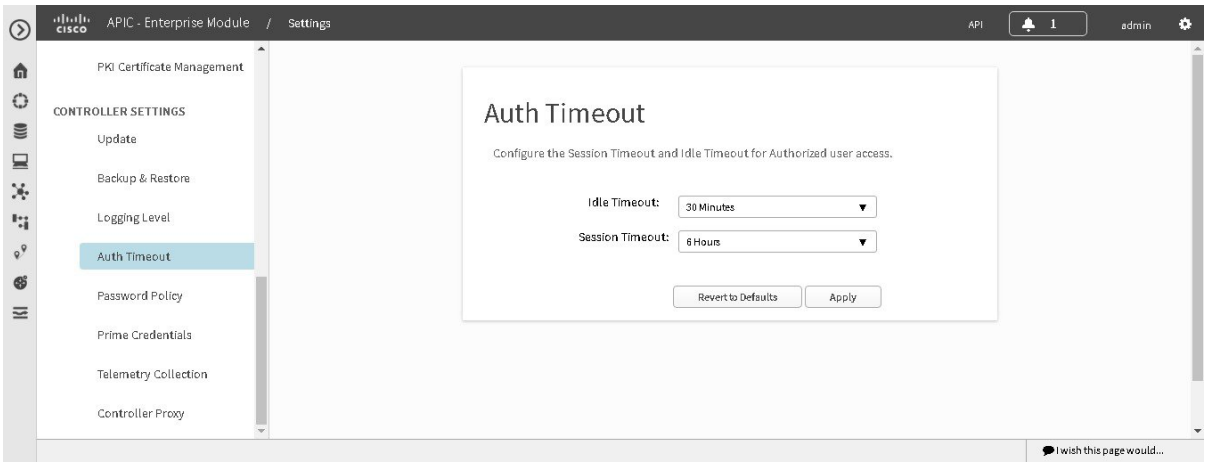
The logging level for the specified service is set.

Controller Settings

Configuring the Authentication Timeout

You can configure authentication timeouts that require the user to log back into the controller with their credentials (username and password) using the **Authentication Timeout** window in the Cisco APIC-EM GUI.

Figure 23: Authentication Timeout Window



The following authentication timeout values can be configured:

- Idle timeout—Time interval that you can configure before the controller requires re-authentication (logging back in with appropriate credentials) due to Cisco APIC-EM inactivity. Idle timeouts are API-based, meaning that idle timeout is the time the controller is idle between API usages and not GUI mouse clicks or drags.
- Session timeout—Time interval that you can configure before the controller requires re-authentication (logging back in with appropriate credentials). This is a forced re-authentication.

Note Approximately 2-3 minutes before your session is about to idle timeout, a pop-up warning appears in the GUI stating that your session is about to idle timeout and asking if you wish to continue with the current session. Click **Cancel** to ignore the warning and idle timeout of the session within approximately 2-3 minutes. Click **OK** to continue the session for another 30 minutes.

Before you begin

You must have successfully deployed the Cisco APIC-EM and it must be operational.

You must have administrator (ROLE_ADMIN) permissions and either access to all resources (RBAC scope set to ALL) or an RBAC scope that contains all of the resources that you want to group. For example, to create a group containing a specific set of resources, you must have access to those resources (custom RBAC scope set to all of the resources that you want to group).

For information about user permissions and RBAC scopes required to perform tasks using the Cisco APIC-EM, see the chapter, "Managing Users".

Step 1 In the **Home** window, click either **admin** or the **Settings** icon (gear) at the top right corner of the screen.

Step 2 Click the **Settings** link from the drop-down menu.

Step 3 In the **Settings** navigation pane, click **Authentication Timeout** to view the **Authentication Timeout** window.

Step 4 (Optional) Configure the idle timeout value using the **Idle Timeout** drop-down menu.

You can configure the idle timeout value in increments of 5 minutes, up to an hour. The default value is 30 minutes.

Step 5 (Optional) Configure the session timeout value using the **Session Timeout** drop-down menu.

You can configure the session timeout value in increments of 30 minutes, up to 24 hours. The default value is six hours.

Step 6 Click the **Apply** button to apply your configuration to the controller.

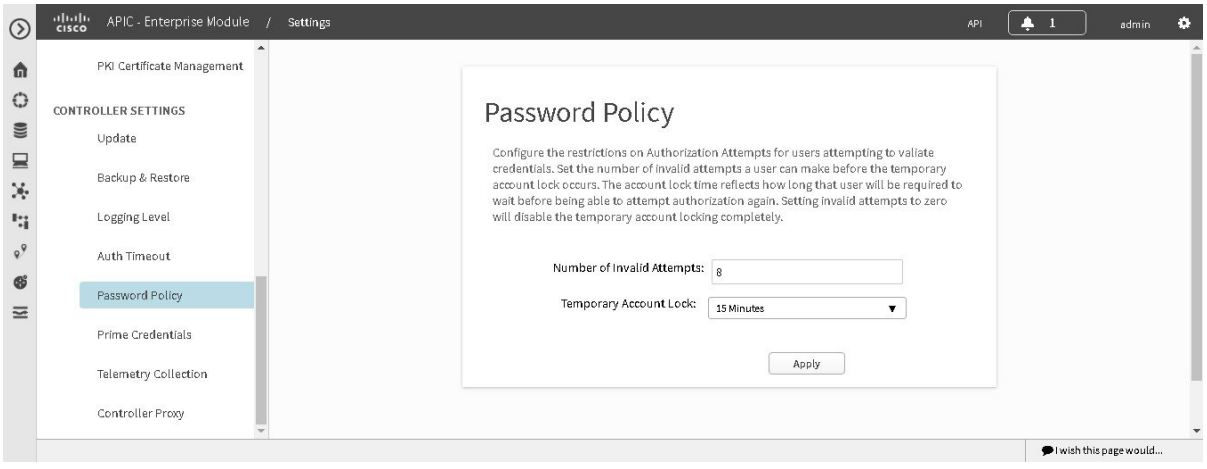
To restore the authentication timeout defaults to the controller, click the **Revert to Defaults** button.

Configuring Password Policies

As an administrator, you can control the number of consecutive, invalid user login attempts to the Cisco APIC-EM. Once a user crosses the threshold set by you as administrator, the user's account is locked and access is refused. Additionally, as an administrator, you can also configure the length of time that the user account is locked. The user account will remain locked until the configured time period expires.

You configure these controller access parameters for the Cisco APIC-EM using the **Password Policy** window.

Figure 24: Password Policy Window



The following password policy functionality is supported:

- As an administrator, you can set the number of consecutive, invalid user login attempts to the controller. These consecutive, invalid user login attempts can be set from 0 to 10 attempts, with 8 attempts being the default value. Setting invalid attempts to 0 will disable the feature of locking a user with invalid password attempts.
- As an administrator, you can set the length of time a user account is locked. Permitted lock time intervals for a user account range from 1-3600 seconds, with 900 seconds being the default value.
- When a user account is locked due to the number of consecutive, invalid login attempts, entering correct credentials will still result in a login failure until the expiration of the configured lock out time period.
- An administrator can unlock the user account at any time.

  We recommend that you create at least two administrator accounts for your deployment. With two administrator accounts, if one account is locked for whatever reason then the other account can be used to unlock that locked account.

Note For information about how to unlock a user account, see the Chapter 4, *Managing Users and Roles* in the *Cisco Application Policy Infrastructure Controller Enterprise Module Configuration Guide*.

- A locked user account is unlocked when the configured lock out time period expires.
- A user account can never be permanently locked, but to deny access permanently, an administrator can delete the account.

Before you begin

You must have successfully deployed the Cisco APIC-EM and it must be operational.

You must have administrator (ROLE_ADMIN) permissions and either access to all resources (RBAC scope set to ALL) or an RBAC scope that contains all of the resources that you want to group. For example, to create a group containing a specific set of resources, you must have access to those resources (custom RBAC scope set to all of the resources that you want to group).

For information about user permissions and RBAC scopes required to perform tasks using the Cisco APIC-EM, see the chapter, "Managing Users".

Step 1 In the **Home** window, click either **admin** or the **Settings** icon (gear) at the top right corner of the screen.

Step 2 Click the **Settings** link from the drop-down menu.

Step 3 In the **Settings** navigation pane, click **Password Policy** to view the **Password Policy** window.

Step 4 (Optional) Configure the number of permitted consecutive, invalid password attempts by choosing from the **Number of Invalid Attempts** drop-down menu.

Step 5 (Optional) Configure the time interval for locking a user account by choosing from the **Temporary Account Lock** drop-down menu.

Step 6 Click the **Apply** button to apply your configuration to the controller.

Related Topics

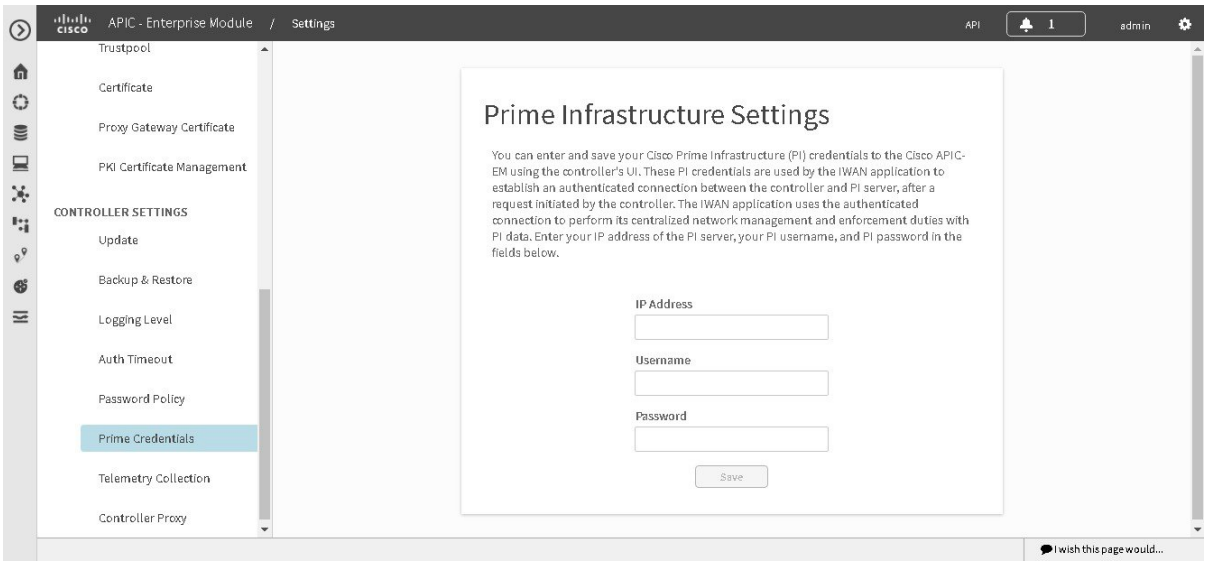
Password Requirements

Configuring the Prime Infrastructure Settings

You can enter and save your Cisco Prime Infrastructure (PI) settings to the Cisco APIC-EM using the controller's UI. These PI settings are used by the IWAN application to establish an authenticated connection between the controller and PI server, after a request initiated by the controller. The IWAN application uses the authenticated connection to perform its centralized network management and enforcement duties with PI data.

You can configure the PI settings using the **Prime Infrastructure Settings** window in the Cisco APIC-EM GUI.

Figure 25: Prime Infrastructure Settings Window



Before you begin

You must have successfully deployed the Cisco APIC-EM and it must be operational.

You must have administrator (ROLE_ADMIN) permissions and either access to all resources (RBAC scope set to ALL) or an RBAC scope that contains all of the resources that you want to group. For example, to create a group containing a specific set of resources, you must have access to those resources (custom RBAC scope set to all of the resources that you want to group).

For information about user permissions and RBAC scopes required to perform tasks using the Cisco APIC-EM, see the chapter, "Managing Users".

Step 1 In the **Home** window, click either **admin** or the **Settings** icon (gear) at the top right corner of the screen.

Step 2 Click the **Settings** link from the drop-down menu.

Step 3 In the **Settings** navigation pane, click **Prime Credentials** to view the **Prime Infrastructure Settings** window.

Step 4 Enter either the IP address of the PI server or the DNS domain name of the PI server.

Step 5 Enter the PI credentials username.

Step 6 Enter the PI credentials password.

Step 7 Click the **Save** button to save the PI credentials to the Cisco APIC-EM database.

What to do next

Proceed to configure the discovery credentials for your network.

Telemetry Collection

The Cisco APIC-EM uses telemetry to collect information about the user experience with the controller. This information is collected for the following reasons:

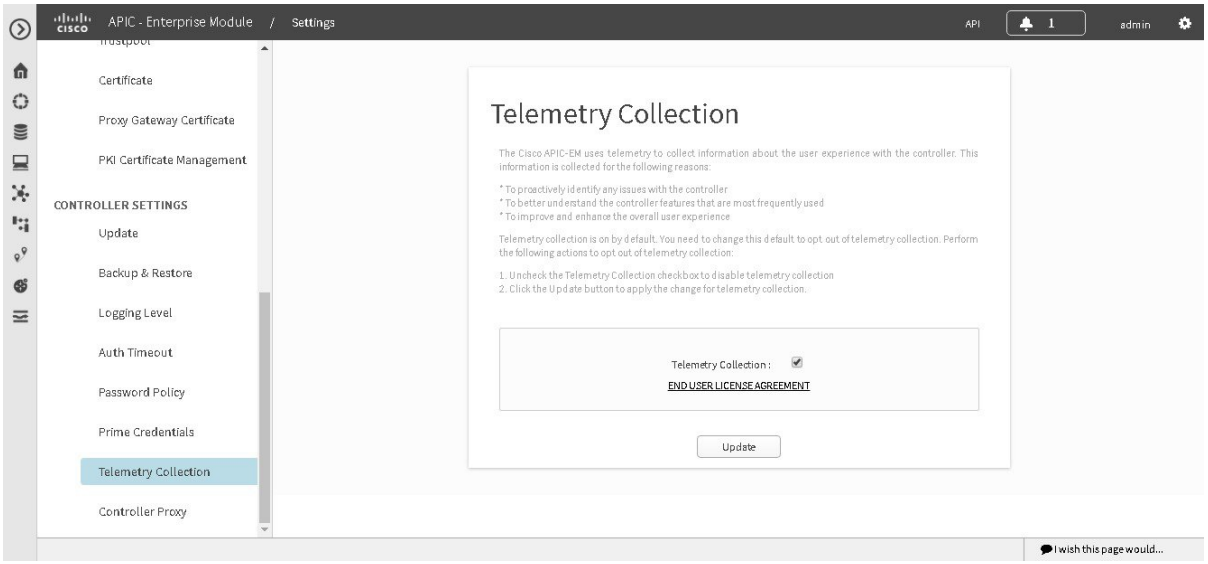
- To proactively identify any issues with the controller
- To better understand the controller features that are most frequently used
- To improve and enhance the overall user experience

You are able to view some of the collected telemetry data by viewing the logs using the Cisco APIC-EM GUI. For information about this method, see *Searching the Services Logs* in Chapter 6, Configuring the Cisco APIC-EM Settings.

Telemetry is enabled with a telemetry service that collects data from the many other controller services. The telemetry service supports Data Access Service (DAS). The telemetry service uploads data to the Cisco Clean Access Agent (CAA) infrastructure on the Cisco cloud using HTTPS.

Telemetry collection is on by default. If you wish to opt out of telemetry collection, then perform the steps in the following procedure.

Figure 26: Telemetry Collection Window



Before you begin

You must have successfully deployed the Cisco APIC-EM and it must be operational.

You must have administrator (ROLE_ADMIN) permissions and either access to all resources (RBAC scope set to ALL) or an RBAC scope that contains all of the resources that you want to group. For example, to create a group containing a specific set of resources, you must have access to those resources (custom RBAC scope set to all of the resources that you want to group).

For information about user permissions and RBAC scopes required to perform tasks using the Cisco APIC-EM, see the chapter, "Managing Users".

Step 1 In the **Home** window, click either **admin** or the **Settings** icon (gear) at the top right corner of the screen.

Step 2 Click the **Settings** link from the drop-down menu.

Step 3 In the **Settings** navigation pane, click **Telemetry Collection** to view the **Telemetry Collection** window.

When accessing the **Telemetry Collection** window for the first time, the GUI displays a blue box with a check that indicates that telemetry collection is enabled.

Step 4 (Optional) Click the **End User License Agreement** to review the agreement for telemetry collection.

Step 5 (Optional) Uncheck the **Telemetry Collection** blue box to disable telemetry collection.

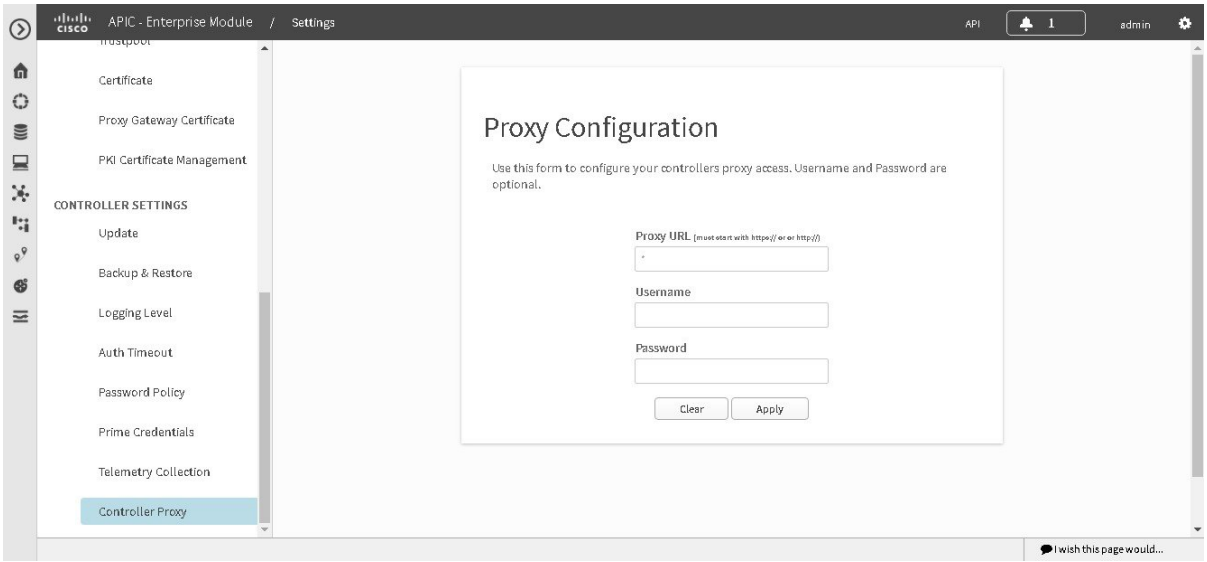
Step 6 (Optional) Click the **Update** button to apply the change for telemetry collection.

Configuring the Proxy

If the Cisco APIC-EM is unable to communicate directly with the telemetry server in the Cisco cloud, then a message will appear in the controller GUI (for an admin user) requesting that you configure access to the proxy. This message will contain a direct link to the **Proxy Configuration** window where you can configure this access. To configure access, enter the appropriate settings for the proxy server that exists between the controller and the telemetry server.

You configure these settings using the **Proxy Configuration** window in the Cisco APIC-EM GUI.

Figure 27: Proxy Configuration Window



Before you begin

You must have successfully deployed the Cisco APIC-EM and it must be operational.

You must have administrator (ROLE_ADMIN) permissions and either access to all resources (RBAC scope set to ALL) or an RBAC scope that contains all of the resources that you want to group. For example, to create a group containing a specific set of resources, you must have access to those resources (custom RBAC scope set to all of the resources that you want to group).

For information about user permissions and RBAC scopes required to perform tasks using the Cisco APIC-EM, see the chapter, "Managing Users".

Step 1 In the **Home** window, click either **admin** or the **Settings** icon (gear) at the top right corner of the screen.

Step 2 Click the **Settings** link from the drop-down menu.

Step 3 In the **Settings** navigation pane, click **Controller Proxy** to view the **Proxy Configuration** window.

Step 4 Enter the proxy server's URL address.

Step 5 (Optional) If the proxy server requires authentication, then enter the username for access to the proxy server.

Step 6 (Optional) If the proxy server requires authentication, then enter the password that is required for access to the proxy server.

Step 7 Click the **Apply** button to apply your proxy configuration settings to the controller.