Managing Users

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 19. For information about configuring external controller authentication, see Configuring External AuthenticationConfiguring External User Profiles, on page 25.

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.

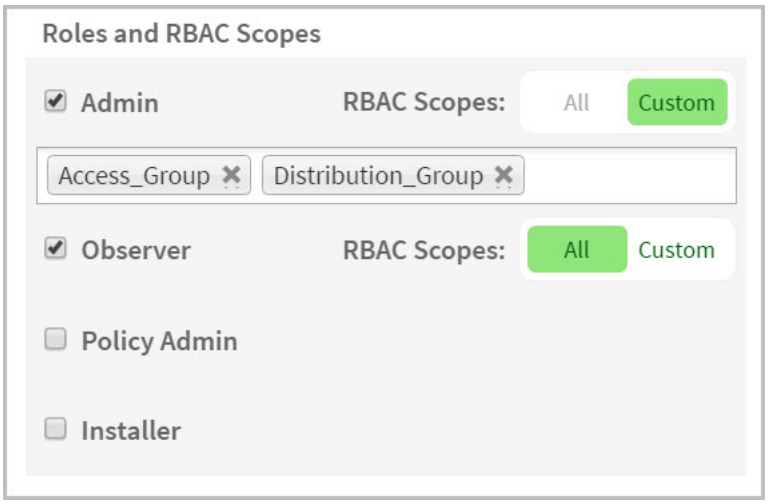
RBAC Scopes

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 1: 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.

Application Behavior Based on Role and RBAC Scope

A user who is assigned a role (for example, ROLE_ADMIN) and an RBAC scope set to ALL may perform the full range of the role's functions to all of the resources. However, if this same user is assigned a limited RBAC scope, the range of functions change, depending on the application. See the following table for a list of applications and the impact of a user's role and RBAC scope on the functions that they can perform.

For detailed application behavior based on limited RBAC scope, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Configuration Guide*.

Table 1: Application Behavior Based on Role and RBAC Scope

Function	Role	Full RBAC Scope	Limited RBAC Scope
Settings (Gear icon) menu			
Settings (Gear icon): • Settings • App Management • System Administration • Audit Logs • Change Password	Admin	Users can perform all of these functions.	Users can only change their own password.
	Policy Admin	Users have access to only these functions: Settings, Audit Logs, and Change Password. See **Discovery Credentials** and **Controller Settings** in this table for details about the functions that a policy admin can perform.	Users have access to only these functions: Settings, Audit Logs, and Change Password. See **Users and Groups** in this table for details about the functions that a policy admin with a limited RBAC scope can perform.
	Observer	Users have access to only these functions: Audit Logs, and Change Password.	Users have access to only these functions: Audit Logs, and Change Password.
Settings			
Users and Groups: • Change Password • Internal Users • External Users • External Authentication • Groups	Admin	Users can perform all of these functions	Users can create and edit internal users, external users, and groups, but they cannot configure external authentication.
	Policy Admin Observer	Users do not have permission to perform these functions.	Users do not have permission to perform these functions.
	Observer	Users do not have permission to view these functions.	Users do not have permission to view these functions.

Function	Role	Full RBAC Scope	Limited RBAC Scope
Discovery Credentials: • CLI Credentials • SNMPv2c • SNMPv3 • SNMP Properties • Device Controllability	Admin	Users can perform all of these functions	Users do not have permission to perform these functions.
	Policy Admin	Users can perform all of these functions	Users do not have permission to perform these functions.
	Observer	Users do not have permission to view these functions.	Users do not have permission to view these functions.
Network Settings: • Trustpool • Certificate • Proxy Gateway Certificate • PKI Certificate Management	Admin	Users can perform all of these functions	Users do not have permission to perform these functions.
	Policy Admin	Users do not have permission to perform these functions.	Users do not have permission to perform these functions.
	Observer	Users do not have permission to view these functions.	Users do not have permission to view these functions.
Controller Settings: • Update • Backup and Restore • Logging Level • Auth Timeout • Password Policy • Prime Credentials • Telemetry Collection • Controller Proxy	Admin	Users can perform all of these functions	Users do not have permission to perform these functions.
	Policy Admin	Users can configure only the logging level, prime credentials, and telemetry collection.	Users do not have permission to perform these functions.
	Observer	Users do not have permission to view these functions.	Users do not have permission to view these functions.
Discovery			

Function	Role	Full RBAC Scope	Limited RBAC Scope
Discovery Credentials Discovery Jobs Discovery Results	Admin Policy Admin	Users can define discovery credentials and create discovery jobs. **Note** Once saved, discovery credentials are not visible to any user. Users can also view discovery results.	Only users with access to all resources (RBAC scope set to ALL) can define discovery credentials, perform discovery and view discovery results. **Note** Once saved, discovery credentials are not visible to any user.
	Observer	Users can view discovery results.	Users cannot view discovery results. Only users with access to all resources (RBAC scope set to ALL) can view discovery results.
Device and Host Inventory			
Device Roles	Admin Policy Admin	Users can change device roles for all devices.	Users can change device roles, however only for the devices defined in their custom RBAC scope. Resources that are not in the user's scope are not displayed.
	Observer	Users can view device roles for all devices but cannot make any changes.	Users can view device roles, however only for the devices defined in their custom RBAC scope. Resources that are not in the user's RBAC scope are not displayed.
Device Tags Policy Tags Location Tags and Markers	Admin Policy Admin	Users can create and change device tags, policy tags, and location tags and markers for all devices.	Users can create and change device tags, policy tags, and location tags and markers, however only for the devices defined in their custom RBAC scope. Resources that are not in the user's scope are not displayed.
	Observer	Users can view device and policy tags for all devices but cannot make any changes.	Users can view device and policy tags, however only for the devices defined in their custom RBAC scope. Resources that are not in the user's RBAC scope are not displayed.

Function	Role	Full RBAC Scope	Limited RBAC Scope
Config Display	Admin Policy Admin Observer	Users can view configuration files for all devices and hosts.	Users can view configuration files, however only for the devices defined in their custom RBAC scope. Resources that are not in the user's scope are not displayed.
Topology			
Topology Map Topology Map Layout Saving Topology Map Layout	Admin Policy Admin	Users can view all devices on the topology map, and they can change and save the topology map layout.	Users can view the topology map, and they can change and save the topology map layout. The full network topology is shown. However, resources that are not in the user's RBAC scope are dimmed and labeled as unauthorized. No information or only basic information about the dimmed resources is displayed.
	Observer	Users can view all of the devices on the topology map but cannot save a changed topology map layout.	Users can view all of the devices on the topology map, but details are displayed only for the resources defined in their custom RBAC scope. Resources that are not in the user's RBAC scope are dimmed and labeled as unauthorized. No information or only basic information about the dimmed resources is displayed. Users cannot save a changed topology map layout.

Function	Role	Full RBAC Scope	Limited RBAC Scope
Device Roles Device Tags Policy Tags	Admin Policy Admin	Users can view and change device roles, device tags, and policy tags for all devices.	Users can view and change device roles, device tags, and policy tags, however only on the resources defined in their custom RBAC scope. The full network topology is shown. However, resources that are not in the user's RBAC scope are dimmed and labeled as unauthorized. No information or only basic information about the dimmed resources is displayed.
	Observer	Users can view all of the devices on the topology map but cannot change the topology map layout.	Users can view all of the devices on the topology map but cannot change the topology map layout. However, details are displayed only for the resources defined in their custom RBAC scope. Resources that are not in the user's RBAC scope are dimmed and labeled as unauthorized. No information or only basic information about the dimmed resources is displayed.
EasyQoS			

Function	Role	Full RBAC Scope	Limited RBAC Scope
Policy Scopes	Admin Policy Admin	Users can view and create policy scopes. When displaying policy scopes, users can view all devices in policy scopes.	Users can create policy scopes, however they can only contain devices that are in their custom RBAC scope. When displaying policy scopes, users can view only the resources defined in their RBAC scope. Resources that are not in the user's RBAC scope are dimmed and shown as locked.
	Observer	Users can view all of the policy scopes. When displaying policy scopes, users can view all devices in policy scopes.	Users can view EasyQoS information, however only for the resources defined in their custom RBAC scope. Users can view information about only the devices defined in their RBAC scope. Devices that are not in the user's RBAC scope are locked and labeled as unauthorized.
Application Registry	Admin Policy Admin	Users have the full application registry functionality. Users can view the applications in the registry, including details about each application, and they can sort the display of applications. They can mark applications as favorites, create custom applications, and edit both custom and NBAR (default) applications.	Users can view the applications in the registry, including details about each application, and they can sort the display of applications. They cannot mark applications as favorites or create custom applications. They cannot edit custom or NBAR (default) applications.
	Observer	Users can view the applications in the registry, including details about each application, and they can sort the display of applications.	Same as an observer with full RBAC scope.

Function	Role	Full RBAC Scope	Limited RBAC Scope
Policies (create, abort, restore, preview, reset, apply, clone, show history for, and delete)	Admin Policy Admin	Users can perform all of the policy-related functions.	Users can perform all of the policy-related functions, but only on policies whose policy scopes contain devices defined in the user's custom RBAC scope. If a policy's policy scope contains any devices that are not in the user's custom RBAC scope, the user will not be allowed to perform any functions on that policy. The policy will be locked and will indicate that the user does not have permission to perform any functions to the policy. A user can view policies whether or not they contain devices in the user's RBAC scope. If a policy contains devices that are not in the user's RBAC scope, the devices details are not displayed. The device is locked and labled as an unauthorized device.
	Observer		Same behavior as an observer with full RBAC scope.

Function	Role	Full RBAC Scope	Limited RBAC Scope
		Users can view all of the policy-related functions, but only on policies whose policy scopes contain devices defined in their custom RBAC scope. If a policy's policy scope contains any devices that are not in the user's custom RBAC scope, the user will not be allowed to perform any functions on that policy. The policy will be locked and will indicate that the user does not have permission to modify the policy. A user can view policies whether or not they contain devices in the user's RBAC scope, but the devices details are not displayed. The device is locked and labeled as an unauthorized device.	
Bandwidth Profile	Admin Policy Admin	Users can create, edit, and delete custom bandwidth profiles for all resources.	Users can only view custom bandwidth profiles.
	Observer	Users can only view custom bandwidth profiles.	Users can only view custom bandwidth profiles.
SP Profile	Admin Policy Admin	Users can create custom SP profiles and edit existing SP profiles for all resources.	Users can view the existing NBAR and custom SP profiles for resources that are in their custom scope, but cannot edit them.
	Observer	Users can view the existing NBAR and custom SP profiles for all resources, but cannot edit them.	Users can view the existing NBAR and custom SP profiles for all resources, but cannot edit them.

Function	Role	Full RBAC Scope	Limited RBAC Scope
Dynamic QoS	Admin Policy Admin	Users can enable and disable dynamic QoS and view dynamic QoS troubleshooting information about all devices.	Users can enable and disable dynamic QoS and view dynamic QoS troubleshooting information about all devices.
	Observer	Users cannot enable or disable dynamic QoS. However, they can view dynamic QoS information about all devices.	Users cannot enable or disable dynamic QoS. However, they can view dynamic QoS information about all devices.
Path Trace			
Basic Path Trace ACL Path Trace Path Trace with QoS, interface, device, and performance monitor statistics	Admin Policy Admin	Users can perform all types of path traces on all resources.	Users can perform ACL traces and traces that gather QoS, interface, device and performance monitor statistics, however, only for the resources defined in their RBAC scope. When the results of a path trace are displayed, the resources that are not in the user's RBAC scope are locked and labeled as unauthorized.
	Observer	Users can perform ACL traces and traces that gather QoS, interface, and device statistics. However, they are unable to perform path traces that gather Performance Monitor statistics. Performance Monitor traces require performance monitoring to be enabled for all flows on all network devices in the path, and an observer does not have permission to make changes on devices.	Users can perform ACL traces and traces that gather QoS, interface, and device statistics. However, they are unable to perform path traces that gather Performance Monitor statistics. Performance Monitor traces require performance monitoring to be enabled for all flows on all network devices in the path, and observers do not have permission to make changes or to access all devices. When the results of a path trace are displayed, the resources that are not in the user's RBAC scope are locked and labeled as unauthorized.
Cisco IWAN			

Function	Role	Full RBAC Scope	Limited RBAC Scope
All Cisco IWAN functions	Admin	Users can perform the full range of functions for all devices.	Not applicable.
	Policy Admin Observer	Not applicable.	Not applicable.
Cisco Network PnP			
All Cisco Network PnP functions	Admin	Users can perform the full range of functions for all devices.	Not applicable.
	Policy Admin Observer	Not applicable.	Not applicable.

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 19.
- 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 AuthenticationConfiguring External User Profiles, on page 25.

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 Internal User Profiles

Configuring Groups for User Access

The Cisco APIC-EM supports the configuration of groups.

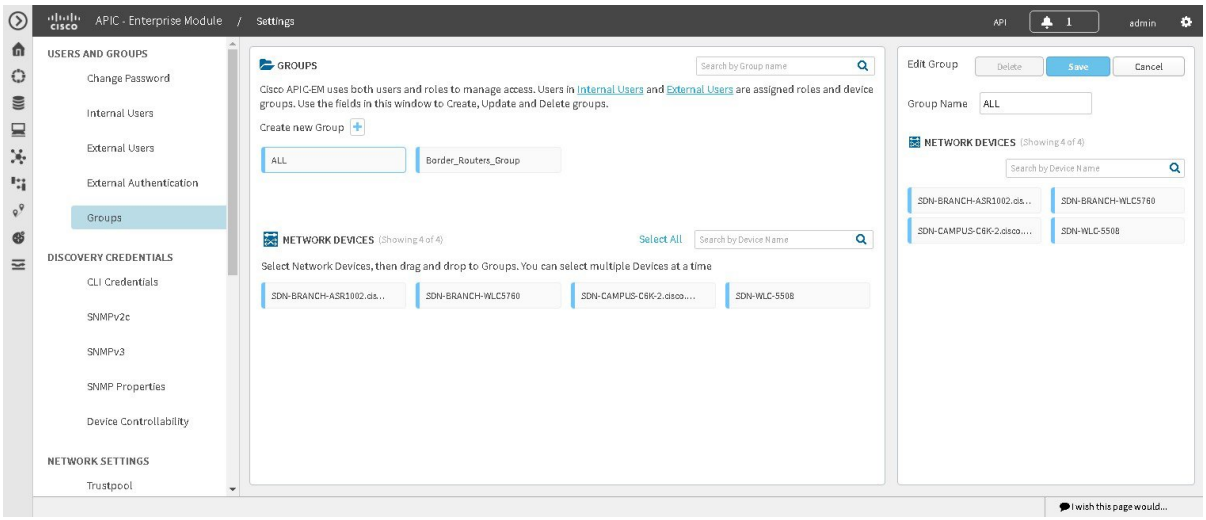
A group is a named entity that represents a specific set of resources for access-control purposes. You assign users to groups using RBAC scope. Assigning a user to a group with RBAC scope enables that user to access the resources in that group; if the user is not assigned to a particular group, the user 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 2: 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.

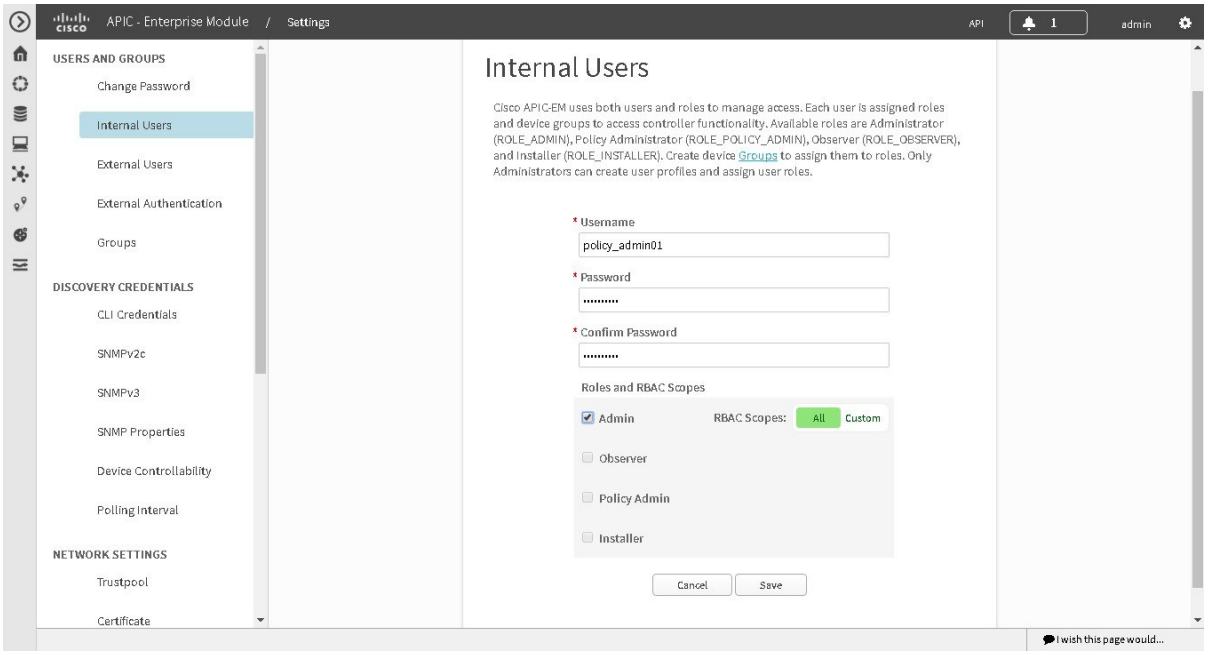
Creating Internal Users

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 3: 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.

Deleting a User

A user with the administrator role (ROLE_ADMIN) can delete a user from the Cisco APIC-EM.

Before You Begin

You must have administrator (ROLE_ADMIN) permissions and access to all devices (RBAC Scope set to ALL) to perform this procedure.

Step 1 From the **Global** toolbar, click the **Administrative Functions** (Gear) icon > **Settings**.

Step 2 From the navigation pane in the **Settings** window, click **Users**.
The **Users** window is displayed with the following information about the users:

- **Username—**Username assigned to the user.
- **Role—**Role that defines the user's privileges within the APIC-EM. Valid roles are ROLE_ADMIN, ROLE_POLICY_ADMIN, ROLE_OBSERVER, or ROLE_INSTALLER.
- **Scope—**Domain or tenancy that the user is allowed to access. In this release, the scope is set to ALL and cannot be changed.
- **Actions—**Icons that allow you to edit user information or delete a user.

Step 3 Locate the user that you want to delete and, in the **Actions** column, click the **Delete** icon.
The user is deleted from the Cisco APIC-EM database and is unable to access the controller.

Note You cannot delete the default administrative user. The Cisco APIC-EM requires at least one administrative user who can log into the controller.

Viewing and Editing User Information

You can view and change user information.

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

Before You Begin

You must have administrator (ROLE_ADMIN) permissions and access to all devices (RBAC Scope set to ALL) to perform this procedure.

Step 1 From the **Global** toolbar, click the **Administrative Functions** (Gear) icon > **Settings**.

Step 2 From the navigation pane in the **Settings** window, click **Users**.
The **Users** window is displayed with the following information about the uses:

- **Username—**Username assigned to the user.
- **Role—**Role that defines the user's privileges within the APIC-EM. Valid roles are ROLE_ADMIN, ROLE_POLICY_ADMIN, ROLE_OBSERVER, or ROLE_INSTALLER.
- **Scope—**Resources that the user is allowed to access.
- **Actions—**Icons that allow you to edit user information or delete a user.

Step 3 If you want to edit a user's information, from the **Actions** column, click the **Edit** icon.
The username and scope are configured by default so you cannot change their settings. However, you can change the role setting. Valid roles are ROLE_ADMIN, ROLE_POLICY_ADMIN, ROLE_OBSERVER, or ROLE_INSTALLER.

Step 4 When you are finished editing the user information, click **Update**.

Changing Your Password

You can change only your own Cisco APIC-EM password, unless you have administrator privileges (ROLE_ADMIN). With administrative privileges, you can change another user's password by deleting and then recreating the user profile with a new password.

You can use the password generator provided in the **Change Password** window or the following guidelines to create a secure password.

Create a password of at least 8 characters and one that contains characters from at least three of the following four classes:

- Uppercase alphabet
- Lowercase alphabet
- Numerical digits

- Special characters—include the space character or any of the following characters or character combinations:

  ! @ # $ % ^ & * ( ) - = + _ { } [ ] \\ | ; : " ' , < . > ? / :: #! ./ ;; >> << () **

In addition to a complex password, you should also ensure that user names do not create security vulnerabilities. To avoid user names that can create security vulnerabilities, the following rules should be followed:

- All users should have unique user names and passwords.
- Do not allow users to use the admin login and password

To avoid creating security vulnerabilities, we recommend that you follow the Cisco APIC-EM password policies when creating a password. For information, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide*.

Step 1 From the **Global** toolbar, click the **Administrative Functions** (Gear) icon > **Settings**.

Step 2 From the navigation pane in the **Settings** window, click **Change Password**.

Step 3 In the **Change Password** window, enter the appropriate values in the following fields:

- **Username—**Your user name appears in this field by default.
- **Current Password—**Your current password.
- **New Password—**Your new password. Create your own or, to create a stronger password, click **Generate**, enter a seed phrase, and click **Generate**. You can apply the generated password by clicking **Apply Password**, or you can copy and paste it or any part of it before or after your new password entry.

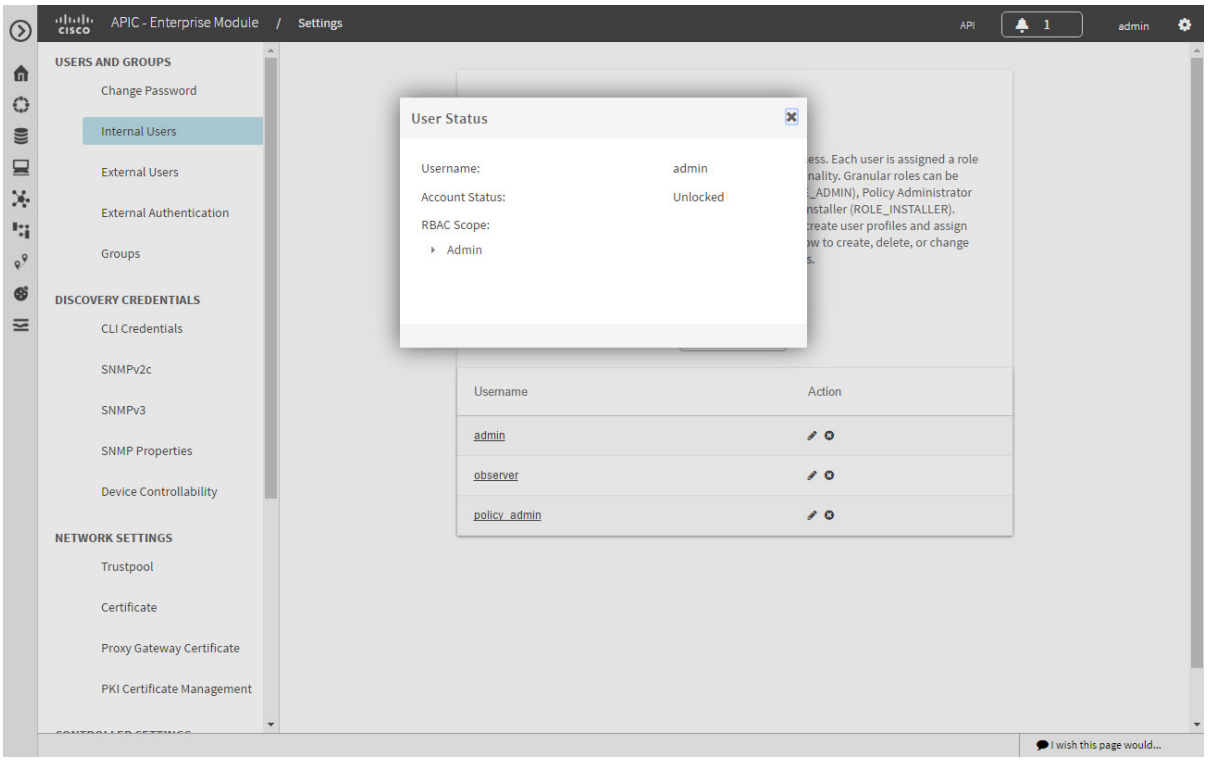
  Note We highly recommend that you use the password generator to create a stronger password.

- **Confirm New Password—**Your new password entered a second time as confirmation.

Step 4 When you are finished, click **Update** to update and save the new password.
Click **Cancel** to cancel the password change.

Viewing User Access Status

As an administrator, you can display the access status of a Cisco APIC-EM user.



Before You Begin

You must have administrator (ROLE_ADMIN) permissions and access to all devices (RBAC Scope set to ALL) to perform this procedure.

Step 1 From the **Global** toolbar, click the**Administrative Functions** (Gear) icon > **Settings**.

Step 2 From the navigation pane in the **Settings** window, click **Users**.
The **Users** window is displayed with the following information about the users:

- **Username—**Username assigned to the user.
- **Role—**Role that defines the user's privileges within the APIC-EM. Valid roles are ROLE_ADMIN, ROLE_POLICY_ADMIN, ROLE_OBSERVER, or ROLE_INSTALLER.
- **Scope—**Resources that the user is allowed to access.
- **Actions—**Icons that allow you to edit user information or delete a user.

Step 3 Click the individual username (link) to view the user's current access status.
The **User Status** dialog box opens, displaying the following information:

- Username
- Account status—Locked or unlocked
- Account Locked Expiration—Time until user account is unlocked

If you are an administrator, you can unlock the user account by clicking **Unlock**.

Note See the *Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide* for information about configuring a password policy for user access to the controller.

Step 4 When you are finished viewing or editing the user information, click **Close**.

Configuring External Users

Configuring External AuthenticationConfiguring External User Profiles

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:

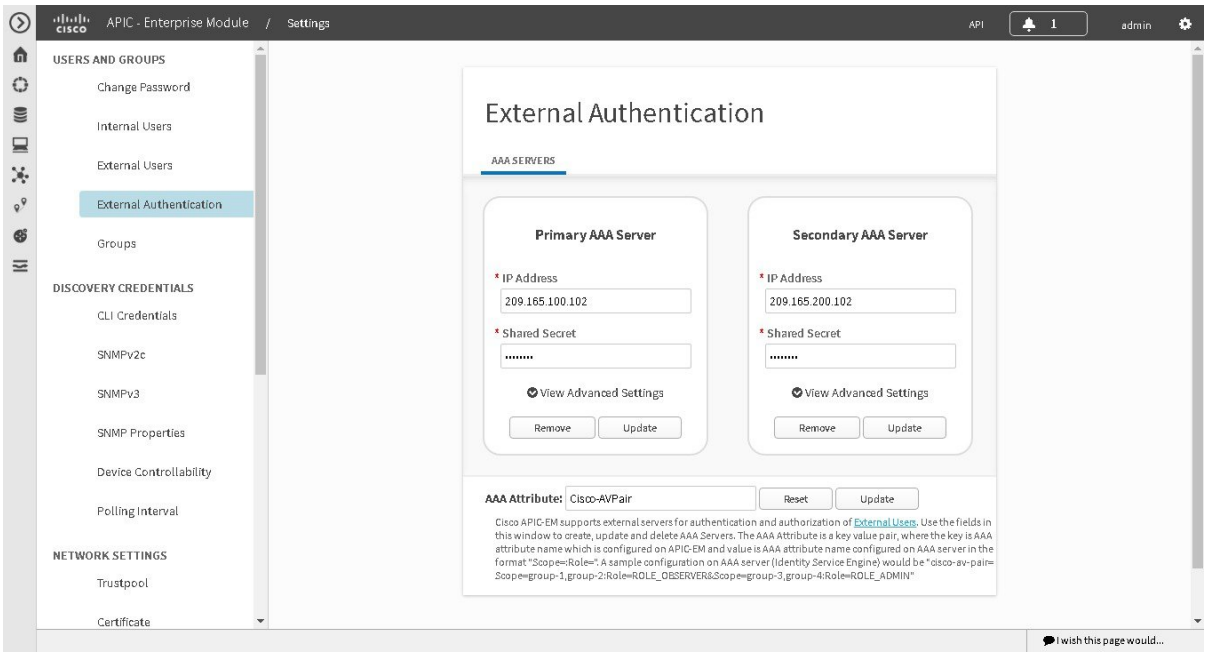
1. Authenticate/authorize with the user's credentials on a primary AAA server.
2. Authenticate/authorize with the user's credentials on a redundant or secondary AAA server.
3. Authenticate/authorize with the user's credentials managed by the Cisco APIC-EM.

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 5: 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:

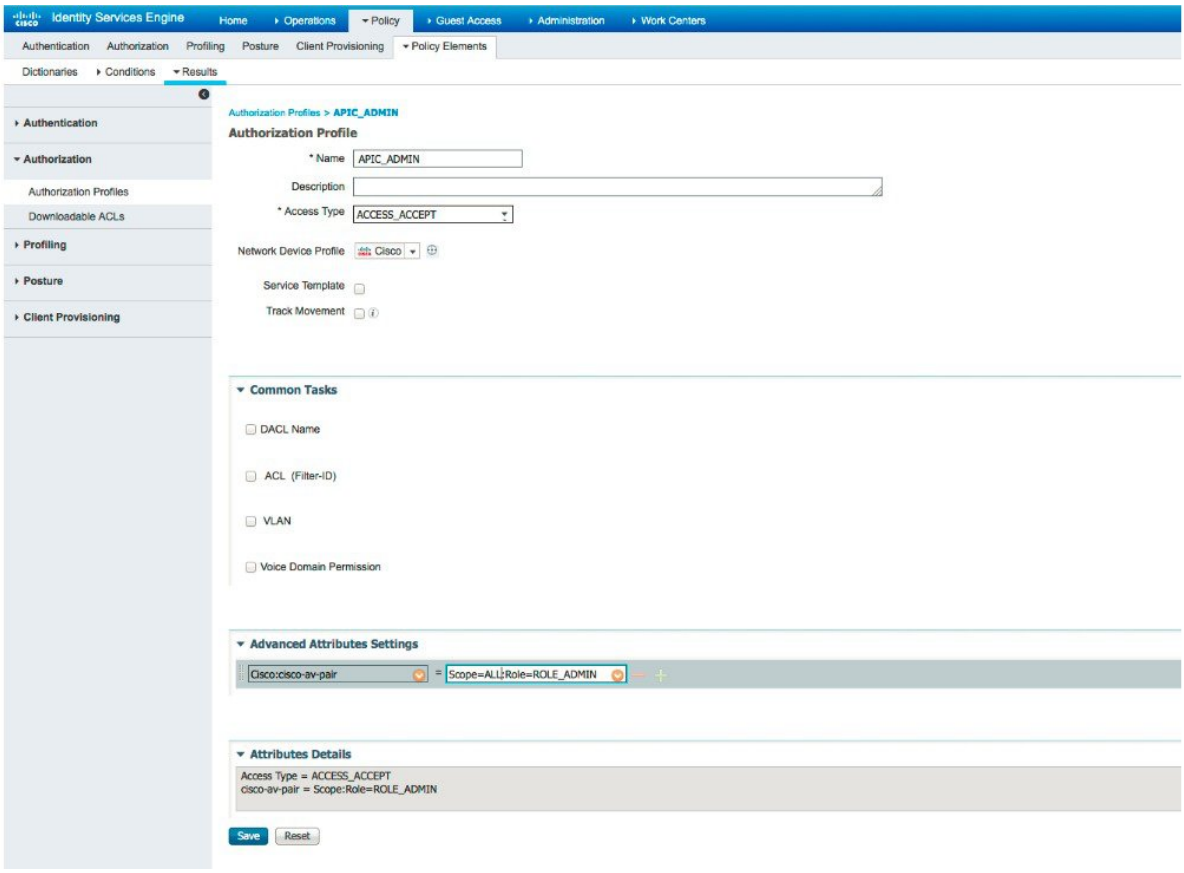
- **Name**: Enter a name for the authorization profile. We recommend that you enter a name similar to the role to be used for the profile. For example, for an admin (ROLE_ADMIN) use a name with "admin" within it, such as "APIC_ADMIN".
- **Description**: Enter a description for the profile
- **Access 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 4: 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.

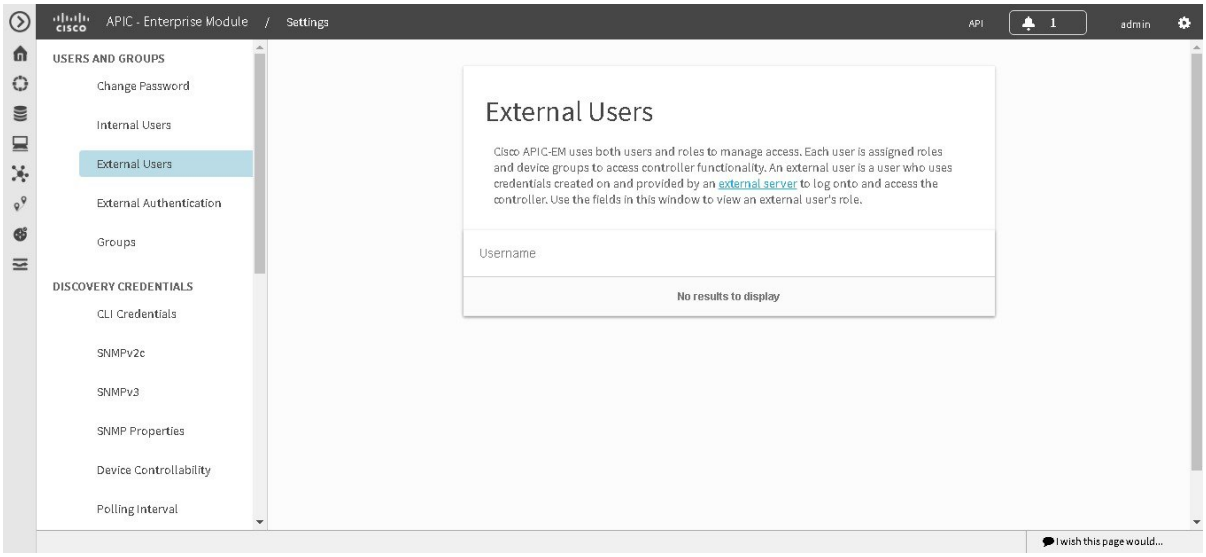
Note If the authentication/authorization is successful and access is granted, then the user's external authentication/authorization is saved in the controller's database. All users successfully granted access can be viewed in the **External Users** window.

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 AuthenticationConfiguring External User Profiles, on page 25.

Figure 6: 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).