Managing Users and Roles

About User Profiles

Cisco APIC-EM supports both internal and external user profiles.

- **Internal User Profiles—**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 is able to create user profiles for other users.

  Cisco APIC-EM controls access to the controller through role-based access control (RBAC). RBAC is a method of restricting or authorizing controller access for users based on their user roles. A role defines the privileges of a user on the controller. Available roles are Administrator (ROLE_ADMIN), Policy Administrator (ROLE_POLICY_ADMIN), Observer (ROLE_OBSERVER), and Installer (ROLE_INSTALLER). Only users with the administrative role (ROLE_ADMIN) can create user profiles and assign user roles.

- **External User Profiles—**External user profiles exist on an external AAA server. Cisco APIC-EM can discover and use credentials from this external AAA server to manage access to the controller. To enable this functionality, you need to configure external authentication for the Cisco APIC-EM. Once configured, you can view external user profiles and their roles in the **External Users** window.

Note You can only view the external user profiles and their roles in the **External Users** window. You cannot create, edit, or delete them from the controller. These tasks must be performed on the external AAA server.

About User Roles

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 is able to create user accounts for other users.

Note Only users with the administrative role (ROLE_ADMIN) can create users and assign user roles.

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

- Administrator (ROLE_ADMIN)—Provides full administrative privileges to all Cisco APIC-EM resources, including the ability to add or remove users and accounts. For more information, see Administrator Role, on page 2.

  Note We highly recommend that you configure at least two users with administrator (ROLE_ADMIN) privileges. 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_POLICY_ADMIN)—Allows you to create and manage policies. For more information, see Policy Administrator Role, on page 3.
- Observer (ROLE_OBSERVER)—Provides primarily read-only privileges to the Cisco APIC-EM. For information, see Observer Role, on page 3.
- Installer (ROLE_INSTALLER)—Allows an installer to use the Cisco Plug and Play Mobile App to remotely access the APIC-EM controller to deploy devices and view their status. An installer cannot directly access the Cisco APIC-EM GUI. For information, see Installer Role, on page 3.

Administrator Role

Users with the administrator role have full administrative privileges to all Cisco APIC-EM resources, including the ability to add or remove users and accounts. Users with the administrator role (ROLE_ADMIN) can perform the following tasks:

- Change their own password (by providing current password).
- Create a new user and assign any existing role to it.
- View all other users with their role and scope.
- Edit their own user role and the user role of any other user.
- Delete any user including themselves.

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.

For information about the specific resources available to the administrator role, see Cisco APIC-EM Resources and Permissions, on page 5.

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

Note We highly recommend that you configure at least two users with administrator (ROLE_ADMIN) privileges. 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

The policy administrator role has full read/write access to policy-administration functionality and APIs, including Discovery, Discovery Credentials (global and discovery-specific), Inventory, Topology, Path Trace, and EasyQoS. In particular, a user in this role can create, modify, and deploy application quality-of-service policies.

This role cannot access system-wide controller-administration functions, such as Network Settings (Trustpool, Controller Certificate, Proxy Certificate) and system-wide Controller Settings (Update, Backup & Restore, Logging Level, Auth Timeout, Password Policy, Telemetry Collection and Controller Proxy.) This role cannot create or delete any user accounts but it can change its own password and read its own account information. This role cannot access Prime Credentials.

Observer Role

The observer role provides read-only privileges to the Cisco APIC-EM. Users who are assigned the observer role (ROLE_OBSERVER) can change their own password (by providing current password).

They cannot perform the following tasks:

- Edit their role or scope
- Delete themselves
- View their own password

For information about the specific resources available to the observer role, see Cisco APIC-EM Resources and Permissions, on page 5.

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

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.

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

Users and Domains

You can create multiple users for the different domains (network or sub-networks) in your network. Each user can have a different role in a different domain. For example, a user can have an observer role in Network A and an administrator role in Network B.

About AAA

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. For a list of resources and the roles that are allowed access to them, see Cisco APIC-EM Resources and Permissions, on page 5.

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.
- External—External controller authentication based upon the usernames and passwords that exist on other servers, including:
  - AAA server authentication—Authentication performed with a pre-configured AAA server using the RADIUS protocol.

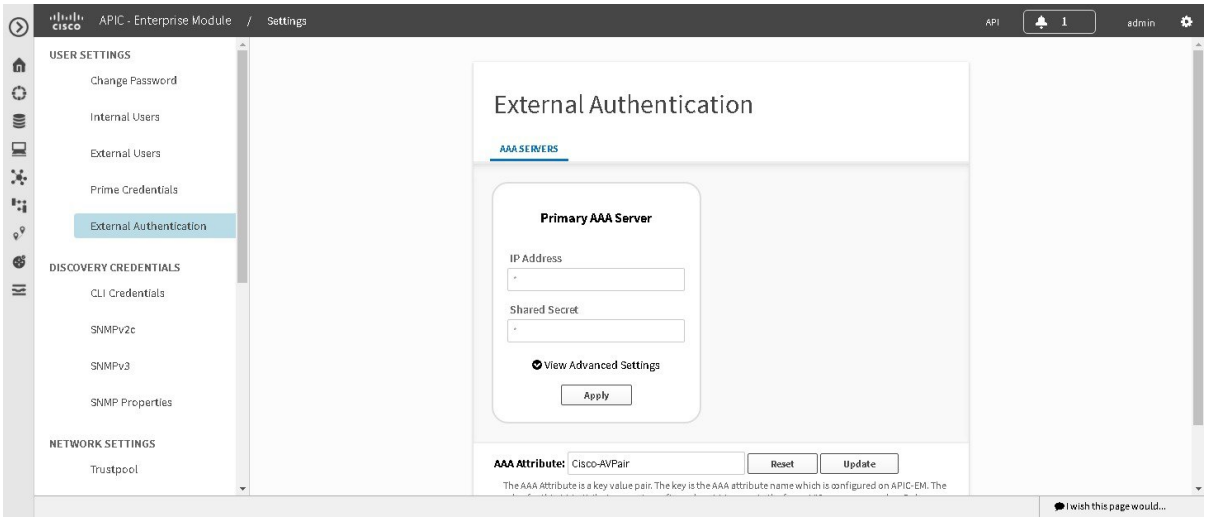
When performing user authentication, the controller attempts to authenticate the user in the following order:

1. Authenticate with AAA (RADIUS) server directory credentials (number of times attempted per user configuration using the APIs)
2. Authenticate with the user configured controller credentials (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.

You can configure external authentication parameters using the **External Authentication** window in the Cisco APIC-EM GUI. For information about prerequisites and the procedure to set up external authentication, see the *Cisco Application Policy Infrastructure Controller Enterprise Module*.

Figure 1: External Authentication Window



Cisco APIC-EM Resources and Permissions

The following table describes the role permissions that are required for each Cisco APIC-EM resource.

Note Depending upon your role and its permissions, certain Cisco APIC-EM GUI functionality will not display. To view the role behavior (for example, administrator and observer) side-by-side in the GUI, you need to either use multiple browsers or incognito mode in the browser. You will not be able to view the role behavior side-by-side in a single browser using tabs.

Table 1: Cisco APIC-EM Resources and Permissions

Resource	Role Permissions
Discovery: Scan	• Administrator • Policy Administrator
Inventory: Retrieving inventory list with device credentials	• Administrator • Policy Administrator

Resource	Role Permissions
Inventory: Adding tags	• Administrator • Policy Administrator • Observer
Inventory: Creating device roles	• Administrator • Policy Administrator • Observer
Inventory: Actions other than adding tags and creating device roles	• Administrator • Policy Administrator • Observer
Role-based access control: Creating and deleting users and security roles	• Administrator • Observer can view and change own password.
File Service	• Administrator • Policy Administrator
Host	• Administrator • Policy Administrator • Observer
Task ID	• Administrator • Policy Administrator • Observer
Telemetry	• Administrator • Policy Administrator • Observer

Resource	Role Permissions
Topology	• Administrator • Policy Administrator • Observer
Path Analysis	• Administrator • Policy Administrator • Observer

Accounting

As an administrator, you can access the content of logs for authenticated sessions. The following information about users, actions, and APIs are captured in these logs for security or troubleshooting purposes:

- Northbound API access data
- Authentication successes with the user name or failures for any method

Changing Your Password

You can change the password that you use to log into the Cisco APIC-EM.

Note You can change only your own password. To change another user's password, you must have administrator privileges. Changing the password involves deleting the user from the controller database and then recreating the user as a new user 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:

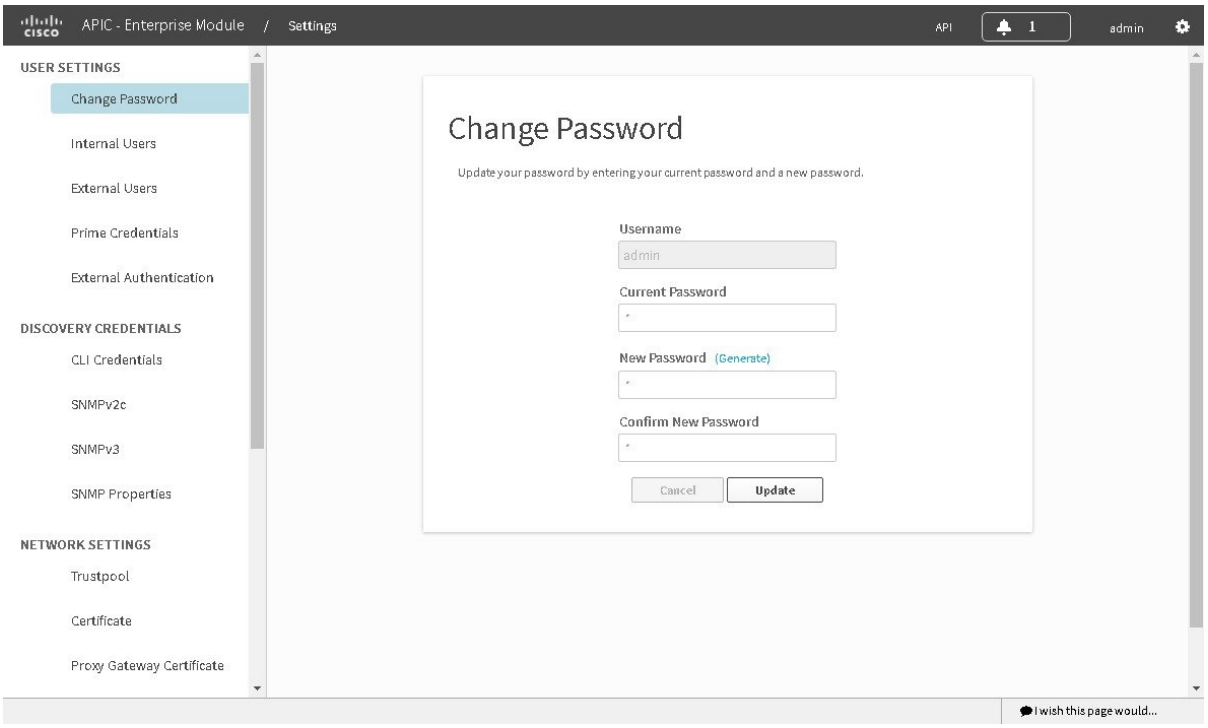
- Uppercase alphabet
- Lowercase alphabet
- Numerical digits
- Special characters—include the space character or any of the following characters or character combinations:

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

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*.



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 **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.

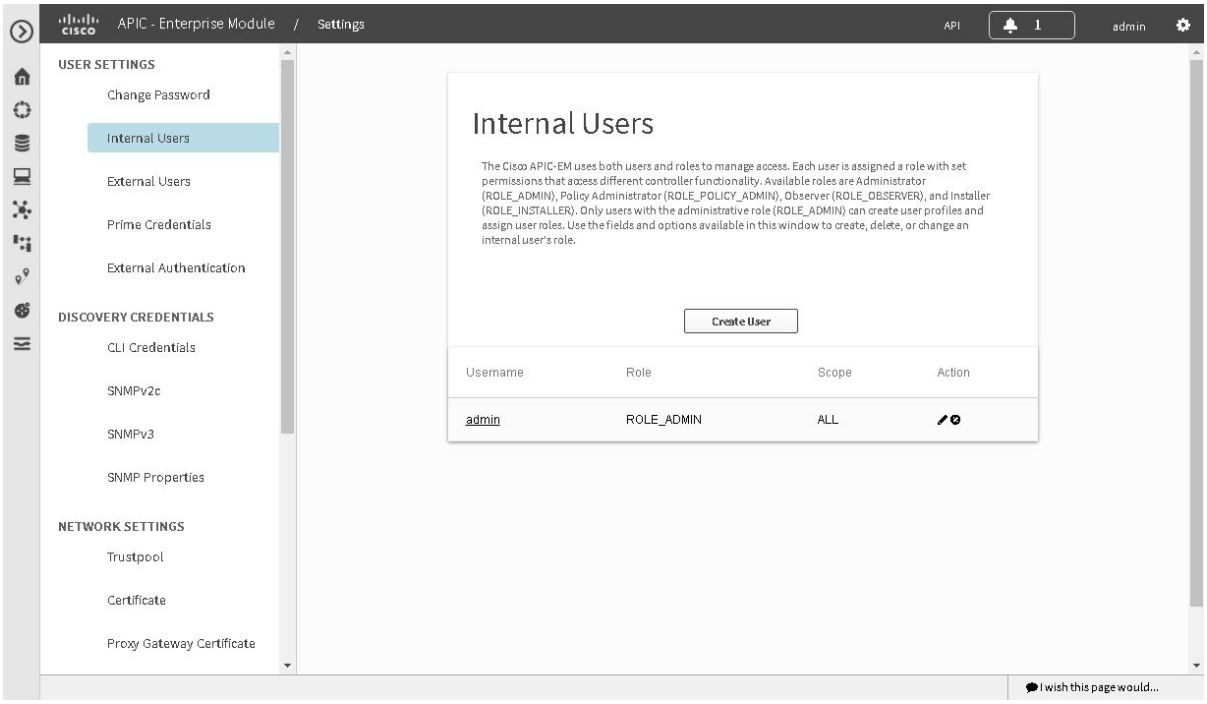
- **Confirm New Password—**Your new password entered a second time as confirmation.

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

Configuring Users and Roles

To access the **Users** window, from the **Global** toolbar click the **Settings** icon. Then from the navigation pane on the Settings window, click **Users**.

Figure 2: Users Window



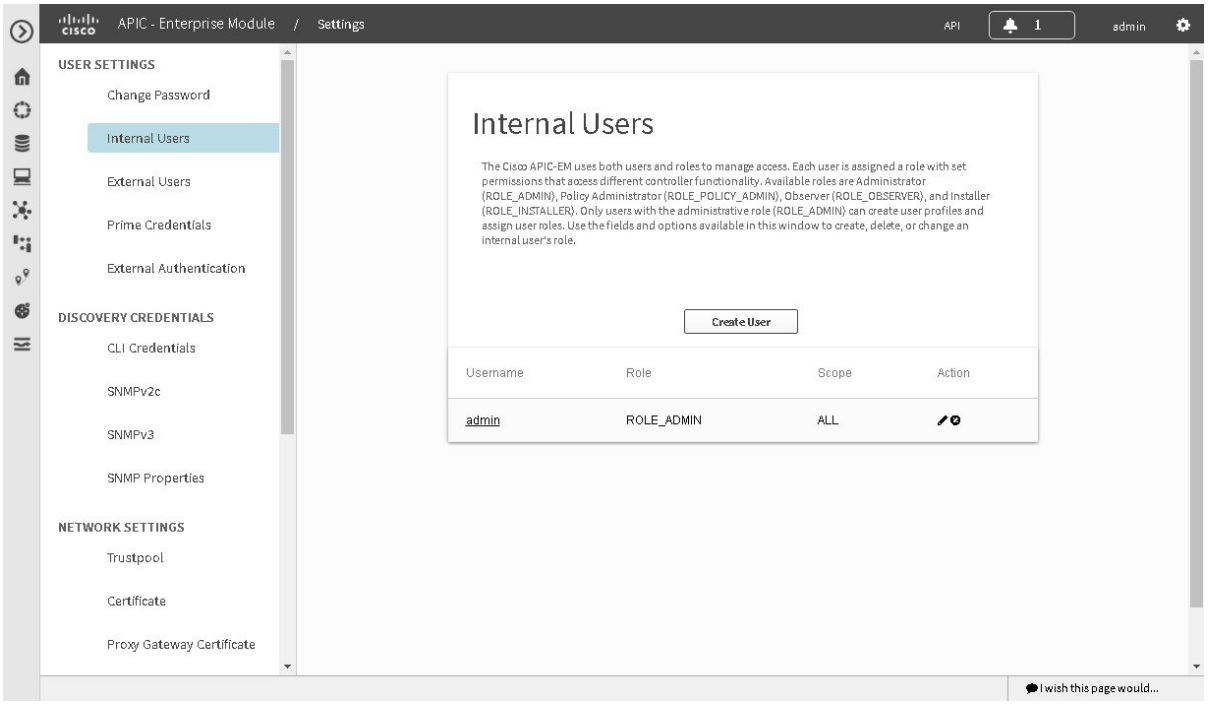
Name	Description
Username	Displays the user's current access status.
Create User	Allows you to add a new user. You must have administrator (ROLE_ADMIN) permissions to perform this procedure.
Edit	Allows you to change the user role settings. You cannot change any other settings. You must have administrator (ROLE_ADMIN) permissions to perform this procedure.
Delete	Removes the user from the Cisco APIC-EM database. The deleted user is no longer able to log into the controller. You must have administrator (ROLE_ADMIN) permissions to perform this procedure.

Adding a User

Only a user with the administrator role (ROLE_ADMIN) can add a user to 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. 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.



Before You Begin

You must be an administrator (ROLE_ADMIN).

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 Click **Create User**.

Step 4 In the **Create User** dialog box, enter the username, password (twice), and role of the new user. The scope is set to **SCOPE ALL** by default.

Step 5 Click **Add**.
The new user appears in the **Users** window.

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 to perform this procedure.

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 to perform this procedure.

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:

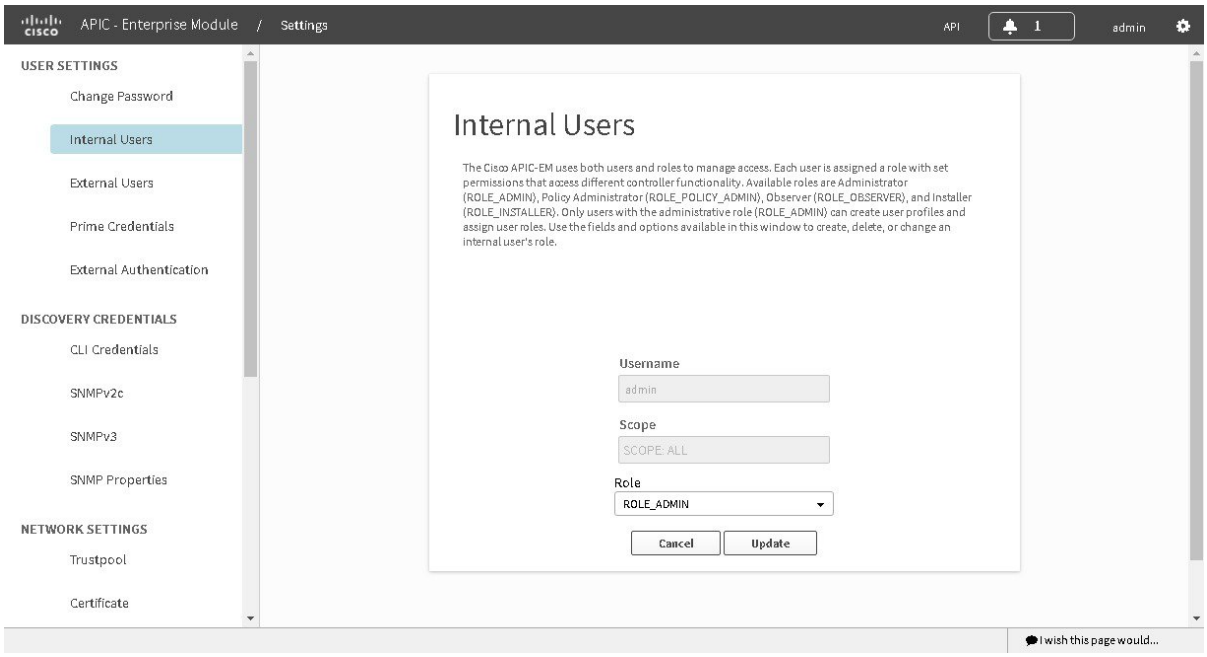
- **Username—**Username assigned to the user.
- **Role—**Role that defines the user's privileges within the APIC-EM. Valid roles are ROLE_ADMIN, ROLE_POLICY_ADMIN, ROLE_OBSERVER, or ROLE_INSTALLER.
- **Scope—**Domain or tenancy that the user is allowed to access.
- **Actions—**Icons that allow you to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

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 to perform this procedure.

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.
- **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 At—Date and time user account was locked
- 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 Authentication

The Cisco APIC-EM supports external authentication and authorization for users from a 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 log into 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 only if both authentication and authorization is successful.

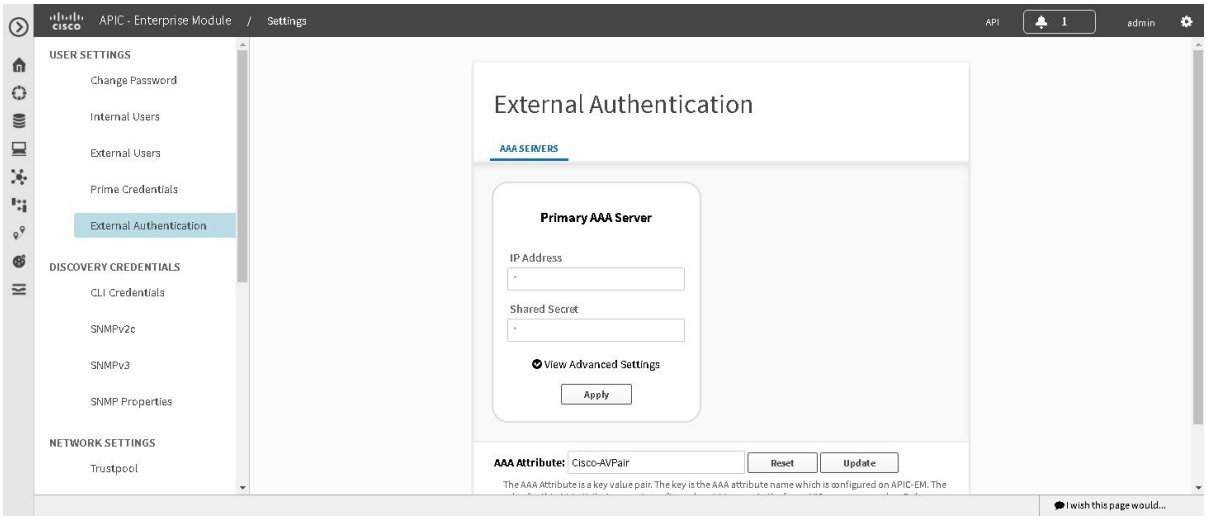
When authentication/authorization is attempted using a AAA server, the response from that AAA server may be either a timeout or rejection:

- 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.

Note External authentication is only supported for the Cisco APIC-EM UI and not the Grapevine console UI.

Figure 4: 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 to perform this procedure.

For information about the user permissions required to perform tasks using the Cisco APIC-EM, see the chapter, *Managing Users and Roles* in the *Cisco Application Policy Infrastructure Controller Enterprise Module Configuration Guide*.

You must have a 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, proceed with the following additional steps:

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

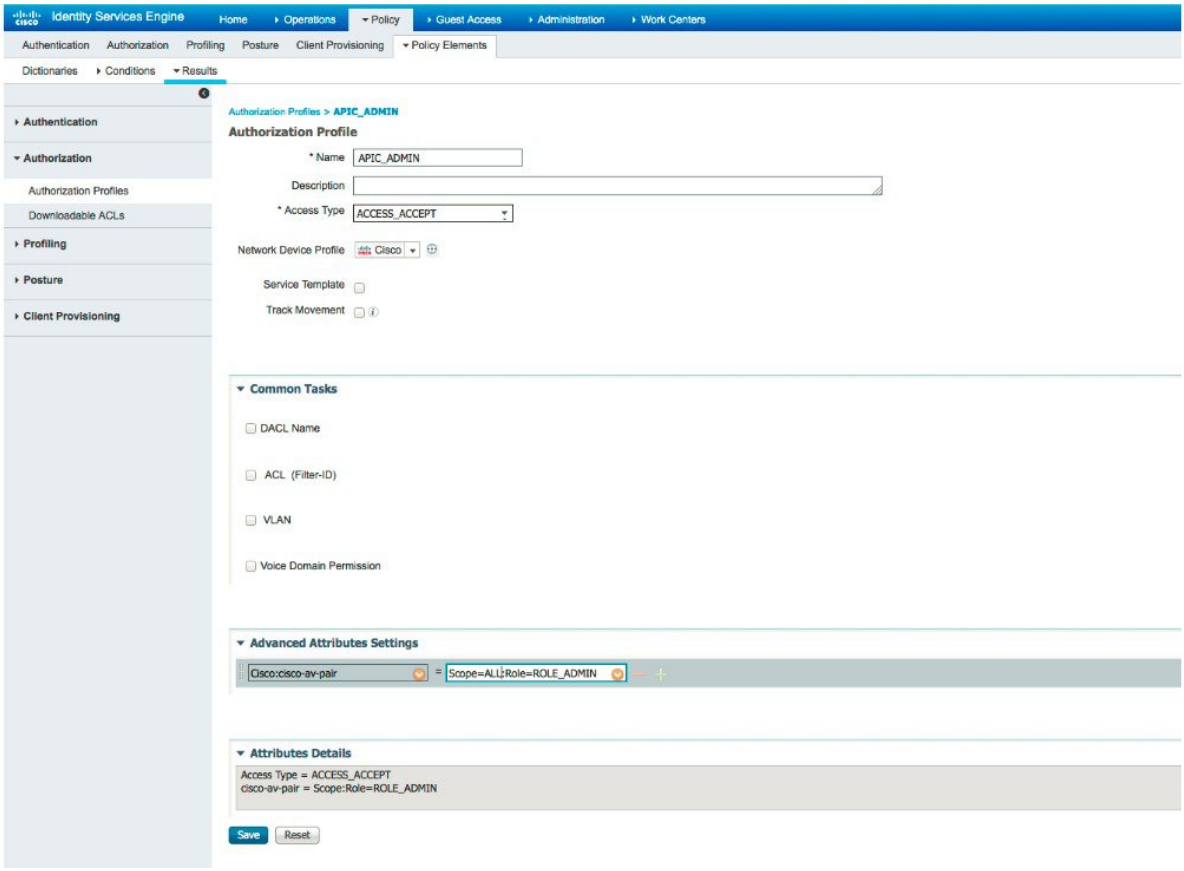
  Note This could also involve configuring a shared-secret on both the AAA server and Cisco APIC-EM controller.

- 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:

- **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

Figure 3: AAA Server Configuration Example (Cisco ISE GUI)



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 **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 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.

Note 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) requires the following format: Scope=*scope_value*:Role=*role_value*

For example: Scope=ALL:Role=ROLE_ADMIN

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.