Manage Administrators and Admin Access Policies

- Role-Based Access Control, page 1
- Cisco ISE Administrators, page 1
- Cisco ISE Administrator Groups, page 2
- Administrative Access to Cisco ISE, page 9

Role-Based Access Control

Cisco ISE allows you to define role-based access control (RBAC) policies that allow or deny certain system-operation permissions to an administrator. These RBAC policies are defined based on the identity of individual administrators or the admin group to which they belong.

To further enhance security and control who has access to the Admin portal, you can:

- Configure administrative access settings based on the IP address of remote clients.
- Define strong password policies for administrative accounts.
- Configure session timeouts for administrative GUI sessions.

Cisco ISE Administrators

Cisco ISE administrators use the Admin portal to:

- Manage deployments, help desk operations, network devices and node monitoring and troubleshooting.
- Manage Cisco ISE services, policies, administrator accounts, and system configuration and operations.
- Change administrator and user passwords.

Administrators can access Cisco ISE through the command-line interface (CLI) or web-based interface. The username and password that you configure during Cisco ISE setup is intended only for administrative access to the CLI. This role is considered to be the CLI-admin user, also known as CLI administrator. By default, the username for the CLI-admin user is admin and the password is defined during setup. There is no default

password. This CLI-admin user is known as the default admin user. This default admin user account cannot be deleted, but can be edited by other administrators (which includes options to enable, disable, or change password for this account).

You can create an administrator or you can promote an existing user to an administrator role. Administrators can also be demoted to simple network user status by disabling the corresponding administrative privileges.

Administrators can be considered as users who have local privileges to configure and operate the Cisco ISE system.

Administrators are assigned to one or more admin groups.

Privileges of a CLI Administrator Versus a Web-Based Administrator

A CLI administrator can start and stop the Cisco ISE application, apply software patches and upgrades, reload or shut down the Cisco ISE appliance, and view all system and application logs. Because of the special privileges granted to a CLI administrator, we recommend that you protect the CLI administrator credentials and create web-based administrators for configuring and managing Cisco ISE deployments.

Create a New Cisco ISE Administrator

Cisco ISE administrators need accounts with specific roles assigned to it to perform specific administrative tasks. You can create administrator accounts and assign one or more roles to it based on the administrative tasks that an administrator has to perform.

You can use the Admin Users page to view, create, modify, delete, change the status, duplicate, or search for attributes of Cisco ISE administrators.

Step 1 Choose **Administration** > **System** > **Admin Access** > **Administrators** > **Admin Users** > **Add.**

Step 2 Choose one of the following:

- Create New User

  If you choose Create New User, a blank Admin User page appears that you must configure.

- Select from Network Access Users

  If you choose Select from Network Access Users, a list of current users appears from which you can click to choose a user, and the corresponding Admin User page appears.

Step 3 Enter values for the Administrator fields. Supported characters for the name field are # $ ’ ( ) * + - . / @ _.

Step 4 Click **Submit** to create the new administrator in the Cisco ISE internal database.

Cisco ISE Administrator Groups

Administrator groups, also called as role-based access control (RBAC) groups in Cisco ISE, contain a number of administrators who belong to the same administrative group. All administrators who belong to the same

group share a common identity and have the same privileges. An administrator's identity as a member of a specific administrative group can be used as a condition in authorization policies. An administrator can belong to more than one administrator group.

Read-only functionality is unavailable for any administrative access in Cisco ISE. Regardless of the level of access, any administrator account can modify or delete objects for which it has permission, on any page that the administrator can access.

The Cisco ISE security model limits administrators to creating administrative groups that contain the same set of privileges that the administrator has, which is based on the administrative role of the user as defined in the Cisco ISE database. In this way, administrative groups form the basis for defining privileges for accessing the Cisco ISE systems.

The following table lists the admin groups that are predefined in Cisco ISE and the tasks that members from these groups can perform.

Table 1: Cisco ISE Admin Groups, Access Levels, Permissions, and Restrictions

Admin Group Role	Access Level	Permissions	Restrictions
Customization Admin	Manage sponsor, guest, and personal devices portals	• Configure guest and sponsor access. • Manage guest access settings. • Customize end-user web portals.	• Cannot perform any policy management or identity management or system-level configuration tasks in Cisco ISE • Cannot view any reports
Helpdesk Admin	Query monitoring and troubleshooting operations	• Run all reports • Run all troubleshooting flows • View the Cisco ISE dashboard and livelogs • View alarms	Cannot create, update, or delete reports, troubleshooting flows, live authentications, or alarms

Admin Group Role	Access Level	Permissions	Restrictions
Identity Admin	• Manage user accounts and endpoints • Manage identity sources	• Add, edit, and delete user accounts and endpoints • Add, edit, and delete identity sources • Add, edit, and delete identity source sequences • Configure general settings for user accounts (attributes and password policy) • View the Cisco ISE dashboard, livelogs, alarms, and reports. • Run all troubleshooting flows.	Cannot perform any policy management or system-level configuration tasks in Cisco ISE
MnT Admin	Perform all monitoring and troubleshooting operations.	• Manage all reports (run, create, and delete) • Run all troubleshooting flows • View the Cisco ISE dashboard and livelogs • Manage alarms (create, update, view, and delete)	Cannot perform any policy management or identity management or system-level configuration tasks in Cisco ISE

Admin Group Role	Access Level	Permissions	Restrictions
Network Device Admin	Manage Cisco ISE network devices and network device repository.	• Read and write permissions on network devices • Read and write permissions on NDGs and all network resources object types • View the Cisco ISE dashboard, livelogs, alarms, and reports • Run all troubleshooting flows	Cannot perform any policy management or identity management or system-level configuration tasks in Cisco ISE
Policy Admin	Create and manage policies for all Cisco ISE services across the network that are related to authentication, authorization, posture, profiler, client provisioning.	• Read and write permissions on all the elements used in policies, such as authorization profiles, NDGs, and conditions • Read and write permissions on identities, endpoints, and identity groups (user identity groups and endpoint identity groups) • Read and write permissions on services policies and settings • View the Cisco ISE dashboard, livelogs, alarms, and reports • Run all troubleshooting flows	Cannot perform any identity management or system-level configuration tasks in Cisco ISE

Admin Group Role	Access Level	Permissions	Restrictions
RBAC Admin	All tasks under the Operations menu except for the Endpoint Protection Services Adaptive Network Control, and partial access to some menu items under Administration	• View the authentication details • Enable or disable Endpoint Protection Services Adaptive Network Control • Create, edit, and delete alarms; generate and view reports; and use Cisco ISE to troubleshoot problems in your network • Read permissions on administrator account settings and admin group settings • View permissions on admin access and data access permissions along with the RBAC policy page. • View the Cisco ISE dashboard, livelogs, alarms, and reports • Run all troubleshooting flows	Cannot perform any identity management or system-level configuration tasks in Cisco ISE

Admin Group Role	Access Level	Permissions	Restrictions
Super Admin	All Cisco ISE administrative functions. The default administrator account belongs to this group.	Create, read, update, delete, and eXecute (CRUDX) permissions on all Cisco ISE resources. **Note** The super admin user cannot modify the default system-generated RBAC policies and permissions. To do this, you must create new RBAC policies with the necessary permissions based on your needs, and map these policies to any admin group.	

Admin Group Role	Access Level	Permissions	Restrictions
System Admin	All Cisco ISE configuration and maintenance tasks.	Full access (read and write permissions) to perform all activities under the Operations tab and partial access to some menu items under the Administration tab. • Read permissions on administrator account settings and administrator group settings • Read permissions on admin access and data access permissions along with the RBAC policy page • Read and write permissions for all options under the Administration > System menu • View the authentication details • Enable or disable Endpoint Protection Services Adaptive Network Control • Create, edit, and delete alarms; generate and view reports; and use Cisco ISE to troubleshoot problems in your network •	Cannot perform any policy management or system-level configuration tasks in Cisco ISE
External RESTful Services (ERS) Admin	Full access to all ERS API requests such as GET, POST, DELETE, PUT	• Create, Read, Update, and Delete ERS API requests	The role is meant only for ERS authorization supporting Internal Users, Identity Groups, Endpoints, Endpoint Groups, and SGT

Admin Group Role	Access Level	Permissions	Restrictions
External RESTful Services (ERS) Operator	Read-only access to ERS API, only GET	• Can only Read ERS API requests	The role is meant only for ERS authorization supporting Internal Users, Identity Groups, Endpoints, Endpoint Groups, and SGT

Create Admin Groups

The Admin Groups page allows you to view, create, modify, delete, duplicate, or filter Cisco ISE network admin groups.

Before You Begin

To configure an external administrator group type, you must have already specified one or more external identity stores.

Step 1 Choose **Administration** > **System** > **Admin Access** > **Administrators** > **Admin Groups**.

Step 2 Click **Add**, and enter a Name and Description. Supported special characters for the name field are: space, # $ & ‘ ( ) * + - . / @ _ .

Step 3 Specify the Type of administrator group you are configuring:

- Internal—Administrators assigned to this group type will authenticate against the credentials that are stored in the Cisco ISE internal database.
- External—Administrators that you assign to this group will authenticate against the credentials that are contained in the external identity store that you specify in the attribute selector. After choosing External, specify the identity store from which Cisco ISE should import the external group information.

Step 4 Click **Add** to add users to the Admin Group Users table. From the Users list, select the users to be added to the admin group.

Step 5 To delete users from the Admin Group Users table, check the check box corresponding to the user that you want to delete, and click **Remove**.

Step 6 Click **Submit** to save any changes made to the admin group that you created in the Cisco ISE database.

Administrative Access to Cisco ISE

Cisco ISE administrators can perform various administrative tasks based on the administrative group to which they belong. These administrative tasks are critical and you must ensure that administrative access is restricted to users who are authorized to administer Cisco ISE in your network.

Cisco ISE allows you to control administrative access to its web interface through the following options:

Role-Based Access Control in Cisco ISE

Role-based access control policies (known as admin access) are access control policies that you define to provide limited access to the Cisco ISE administrative interface. These admin access policies allow you to customize the amount and type of access on a per-administrator or per-admin group basis using specified role-based access permission settings that apply to an individual admin user or an admin group.

Role-based access determines what each entity can access, which is controlled with an access control policy. Role-based access also determines the administrative role that is in use, the admin group to which the entity belongs, and the corresponding permissions and settings that are applied based upon the role of the entity.

Role-Based Permissions

Cisco ISE allows you to configure permissions at the menu and data levels, called the menu access and data access permissions.

The menu access permissions allow you to show or hide the menu items of the Cisco ISE administrative interface. This feature lets you create permissions so that you can restrict or enable access at the menu level.

The data access permissions allow you to grant read/write, or no access to the following data in the Cisco ISE interface: Admin Groups, User Identity Groups, Endpoint Identity Groups, Locations, and Device Types.

RBAC Policies

RBAC policies determine if an administrator can be granted a specific type of access to a menu item or other identity group data elements. You can grant or deny access to a menu item or identity group data element to an administrator based on the admin group by using RBAC policies. When administrators log in to the Admin portal, they can access menus and data that are based on the policies and permissions defined for the admin groups with which they are associated.

RBAC policies map admin groups to menu access and data access permissions. For example, you can prevent a network administrator from viewing the Admin Access operations menu and the policy data elements. This can be achieved by creating a custom RBAC policy for the admin group with which the network administrator is associated.

Default Menu Access Permissions

Cisco ISE provides an out of the box set of permissions that are associated with a set of predefined admin groups. Having predefined admin group permissions allow you to set permissions so that a member of any admin group can have full or limited access to the menu items within the administrative interface (known as menu access) and to delegate an admin group to use the data access elements of other admin groups (known as data access). These permissions are reusable entities that can be further used to formulate RBAC policies for various admin groups. Cisco ISE provides a set of system defined menu access permissions that are already used in the default RBAC policies. The following table lists the default menu access permissions. Apart from the predefined menu access permissions, Cisco ISE also allows you to create custom menu access permissions that you can use in RBAC policies.

Table 2: Default Menu Access Permissions

Menu Access Name	RBAC Group	Permissible Set of Menu Items
Super Admin Menu Access	Super Admin	Operations > All menu items Policy > All menu items Administration > All menu items
Policy Admin Menu Access	Policy Admin	Operations > All menu items Policy > All menu items Administration >Identity Management > All menu items System > Settings
Helpdesk Admin Menu Access	Helpdesk Admin	Operations > All menu items
Identity Admin Menu Access	Identity Admin	Operations > All menu items Administration >Identity Management > All menu items
Network Device Menu Access	Network Device Admin	Operations > All menu items Administration >Network Resources > All menu items
System Admin Menu Access	System Admin	Operations > Authentications, Alarms, Reports, and Troubleshoot Administration >System > All menu items
RBAC Admin Menu Access	RBAC Admin	Operations > All menu items exceptEndpoint Protection Services Adaptive Network Control Administration >Admin Access > All menu items
MnT Admin Menu Access	MnT Admin	Operations > All menu items

Note For Super Admin User, all the menu items are available. For other Admin Users, all the Menu Items in this column are available for Standalone deployment and Primary Node in Distributed Deployment. For Secondary Node in Distributed Deployment, the Menu Items under the Administration tab are not available.

Configure Menu Access Permissions

Cisco ISE allows you to create custom menu access permissions that you can map to an RBAC policy. Depending on the role of the administrators, you can allow them to access only specific menu options.

Step 1 Choose **Administration** > **System** > **Admin Access** > **Authorization** > **Permissions** > **Menu Access**.

Step 2 Click **Add**, and enter values for the Name and Description fields.

a) Click to expand the menu item up to the desired level, and click the menu item(s) on which you want to create permissions.

b) In the Permissions for Menu Access area, click **Show**.

Step 3 Click **Submit**.

Default Data Access Permissions

Cisco ISE comes with a set of predefined data access permissions. The data access permissions enable multiple administrators to have the data access permissions within the same user population. You can enable or restrict the use of data access permissions to one or more admin groups. This process allows autonomous delegated control to administrators of one admin group to reuse data access permissions of the chosen admin groups through selective association. Data access permissions range from full access to no access for viewing selected admin groups or the network device groups. The following table lists the default data access permissions. RBAC policies are defined based on the administrator (RBAC) group, menu access, and data access permissions. You first create menu access and data access permissions and then create an RBAC policy that associates an admin group with the corresponding menu access and data access permissions. The RBAC policy takes the form:If admin_group=Super Admin then assign SuperAdmin Menu Access permission + SuperAdmin Data Access permission. Apart from the predefined data access permissions, Cisco ISE also allows you to create custom data access permissions that you can associate with an RBAC policy.

Table 3: Default Data Access Permissions

Data Access Name	RBAC Group	Permissible Admin Groups	Permissible Network Device Groups
Super Admin Data Access	Super Admin	Admin Groups, User Identity Groups, Endpoint Identity Groups	All Locations, All Device Types
Policy Admin Data Access	Policy Admin	User Identity Groups, Endpoint Identity Groups	None
Identity Admin Data Access	Identity Admin	User Identity Groups, Endpoint Identity Groups	None
Network Admin Data Access	Network Device Admin	None	All Locations, All Device Types

Data Access Name	RBAC Group	Permissible Admin Groups	Permissible Network Device Groups
System Admin Data Access	System Admin	Admin Groups	None
RBAC Admin Data Access	RBAC Admin	Admin Groups	None

Configure Data Access Permissions

Cisco ISE allows you to create custom data access permissions that you can map to an RBAC policy. Based on the role of the administrator, you can choose to provide them access only to select data.

Step 1 Choose **Administration** > **System** > **Admin Access** > **Authorization** > **Permissions**.

Step 2 Choose **Permissions** > **Data Access**.

Step 3 Click **Add**, and enter values for the Name and Description fields.

a) Click to expand the admin group and select the desired admin group.

b) Click **Full Access**.

Step 4 Click **Save**.

Configure Admin Access Policies

An Admin Access (RBAC) policy is represented in an if-then format, where if is the RBAC Admin Group value and then is the RBAC Permissions value.

The RBAC policies page contains a list of default policies. These default policies cannot be modified or deleted. This page also allows you to create custom RBAC policies for an admin group specifically for your work place, and apply to personalized admin groups.

Before You Begin

- Ensure that you have created all admin groups for which you want to define the RBAC policies.
- Ensure that these admin groups are mapped to the individual admin users.
- Ensure that you have configured the RBAC permissions, such as menu access and data access permissions.

Step 1 Choose **Administration** > **System** > **Admin Access** > **Authorization** > **Policy**.
The RBAC Policies page contains a set of ready-to-use predefined policies for default admin groups.

Step 2 Click **Actions** next to any of the default RBAC policy rule.

Here, you can insert new RBAC policies, duplicate an existing RBAC policy, and delete an existing RBAC policy.

Step 3 Click **Insert new policy**.

Step 4 Enter values for the Rule Name, RBAC Group(s), and Permissions fields.
You cannot select multiple menu access and data access permissions when creating an RBAC policy.

Step 5 Click **Save**.

Administrator Access Settings

Cisco ISE allows you to define some rules for administrator accounts to enhance security. You can restrict access to the management interfaces, force administrators to use strong passwords, regularly change their passwords, and so on. The password policy that you define under the Administrator Account Settings in Cisco ISE applies to all administrator accounts.

Cisco ISE does not support administrator passwords with UTF-8 characters.

Configure the Maximum Number of Concurrent Administrative Sessions and Login Banners

You can configure the maximum number of concurrent administrative GUI or CLI (SSH) sessions and login banners that help and guide administrators who access your administrative web or CLI interface. You can configure login banners that appear before and after an administrator logs in. By default, these login banners are disabled.

Before You Begin

To perform the following task, you must be a Super Admin or System Admin.

Step 1 Choose **Administration** > **System** > **Admin Access** > **Settings** > **Access** > **Session**.

Step 2 Enter the maximum number of concurrent administrative sessions that you want to allow through the GUI and CLI interfaces. The valid range for concurrent administrative GUI sessions is from 1 to 20. The valid range for concurrent administrative CLI sessions is 1 to 10.

Step 3 If you want Cisco ISE to display a message before an administrator logs in, check the **Pre-login banner** check box and enter your message in the text box.

Step 4 If you want Cisco ISE to display a message after an administrator logs in, check the **Post-login banner** check box and enter your message in the text box.

Step 5 Click **Save**.

Allow Administrative Access to Cisco ISE from Select IP Addresses

Cisco ISE allows you to configure a list of IP addresses from which administrators can access the Cisco ISE management interfaces.

The administrator access control settings are only applicable for Cisco ISE nodes that assume the Administration, Policy Service, or Monitoring personas. These restrictions are replicated from the primary to the secondary nodes. These restrictions are not applicable for the Inline Posture nodes.

Before You Begin

To perform the following task, you must be a Super Admin or System Admin.

Step 1 Choose **Administration** > **System** > **Admin Access** > **Settings** > **Access** > **IP Access**.

Step 2 From the Configure IP List for Access Restriction area, click **Add**.

Step 3 Enter IP addresses in the classless interdomain routing (CIDR) format in the IP address field.

Step 4 Enter the subnet mask in the Netmask in CIDR format field.

Step 5 Click **OK**. Repeat the process to add more IP address ranges to this list.

Step 6 Click **Save** to save the changes.

Configure a Password Policy for Administrator Accounts

Cisco ISE also allows you to create a password policy for administrator accounts to enhance security. You can define whether you want a password based or client certificate based administrator authentication. The password policy that you define here is applied to all administrator accounts in Cisco ISE.

Note Cisco ISE does not support administrator passwords with UTF-8 characters.

Before You Begin

- To perform the following task, you must be a Super Admin or System Admin.
- Make sure that the auto-failover configuration, if enabled in your deployment, is turned off. When you change the authentication method, you will be restarting the application server processes. There might be a delay while these services restart. Due to this delay in restart of services, auto-failover of secondary Administration node might get initiated.

Step 1 Choose **Administration** > **System** > **Admin Access** > **Authentication**.

Step 2 Select either of these authentication methods:

- Password Based—If you want to use the standard user ID and password credentials for an administrator login, choose the **Password Based** option and specify either the “Internal” or “External” authentication type.

  Note If you have configured an external identity source such as LDAP and want to use that as your authentication source to grant access to the admin user, you must select that particular identity source from the Identity Source list box.

- Client Certificate Based—If you want to specify a certificate-based policy, choose the **Client Certificate Based** option, and select an existing Certificate Authentication Profile.

Step 3 Click the **Password Policy** tab and enter the values.

Step 4 Click **Save** to save the administrator password policy.

Note If you are using an external identity store to authenticate administrators at login, remember that even if this setting is configured for the password policy applied to the administrator profile, the external identity store will still validate the administrator's username and password.

Configure Session Timeout for Administrators

Cisco ISE allows you to determine the length of time an administration GUI session can be inactive and still remain connected. You can specify a time in minutes after which Cisco ISE logs out the administrator. After a session timeout, the administrator must log in again to access the Cisco ISE Admin portal.

Before You Begin

To perform the following task, you must be a Super Admin or System Admin.

Step 1 Choose **Administration** > **System** > **Admin Access** > **Settings** > **Session** > **Session Timeout**.

Step 2 Enter the time in minutes that you want Cisco ISE to wait before it logs out the administrator if there is no activity. The default value is 60 minutes. The valid range is from 6 to 100 minutes.

Step 3 Click **Save**.

Terminate an Active Administrative Session

Cisco ISE displays all active administrative sessions from which you can select any session and terminate at any point of time, if a need to do so arises. The maximum number of concurrent administrative GUI sessions is 20. If the maximum number of GUI sessions is reached, an administrator who belongs to the super admin group can log in and terminate some of the sessions.

Before You Begin

To perform the following task, you must be a Super Admin.

Step 1 Choose **Administration** > **System** > **Admin Access** > **Settings** > **Session** > **Session Info**.

Step 2 Check the check box next to the session ID that you want to terminate and click **Invalidate**.

Change Administrator Name

Cisco ISE allows you to change your username from the GUI.

Before You Begin

To perform the following task, you must be a Super Admin or System Admin.

Step 1 Log in to the Admin portal.
Step 2 Click your username that appears as a link at the upper right corner of the Cisco ISE UI.
Step 3 Enter the new username in the Admin User page that appears.
Step 4 Edit any other details about your account that you want to change.
Step 5 Click **Save**.

Administrative Access to Cisco ISE Using an External Identity Store

In Cisco ISE, you can authenticate administrators via an external identity store such as Active Directory, LDAP, or RSA SecureID. There are two models you can use to provide authentication via an external identity store:

- External Authentication and Authorization—There are no credentials that are specified in the local Cisco ISE database for the administrator, and authorization is based on external identity store group membership only. This model is used for Active Directory and LDAP authentication.
- External Authentication and Internal Authorization—The administrator's authentication credentials come from the external identity source, and authorization and administrator role assignment take place using the local Cisco ISE database. This model is used for RSA SecurID authentication. This method requires you to configure the same username in both the external identity store and the local Cisco ISE database.

During the authentication process, Cisco ISE is designed to "fall back" and attempt to perform authentication from the internal identity database, if communication with the external identity store has not been established or if it fails. In addition, whenever an administrator for whom you have set up external authentication launches a browser and initiates a login session, the administrator still has the option to request authentication via the Cisco ISE local database by choosing "Internal" from the **Identity Store** drop-down selector in the login dialog.

Note You can configure this method of providing external administrator authentication only via the Admin portal. The Cisco ISE Command Line Interface (CLI) does not feature these functions.

If your network does not already have one or more existing external identity stores, ensure that you have installed the necessary external identity stores and configured Cisco ISE to access those identity stores.

External Authentication and Authorization

By default, Cisco ISE provides internal administrator authentication. To set up external authentication, you must create a password policy for the external administrator accounts that you define in the external identity stores. You can then apply this policy to the external administrator groups that eventually become a part of the external administrator RBAC policy.

In addition to providing authentication via an external identity store, your network may also require you to use a Common Access Card (CAC) authentication device.

To configure external authentication, you must:

- Configure password-based authentication using an external identity store.
- Create an external administrator group.
- Configure menu access and data access permissions for the external administrator group.
- Create an RBAC policy for external administrator authentication.

External Authentication Process Flow

When the administrator logs in, the login session passes through the following steps in the process:

1. The administrator sends an RSA SecurID challenge.
2. RSA SecurID returns a challenge response.
3. The administrator enters a user name and the RSA SecurID challenge response in the Cisco ISE login dialog, as if entering the user ID and password.
4. The administrator ensures that the specified Identity Store is the external RSA SecurID resource.
5. The administrator clicks **Login**.

Upon logging in, the administrator sees only the menu and data access items that are specified in the RBAC policy.

Configure a Password-Based Authentication Using an External Identity Store

You must first configure password-based authentication for administrators who authenticate using an external identity store such as Active Directory or LDAP.

Step 1 Choose **Administration** > **System** > **Admin Access** > **Authentication**.

Step 2 On the Authentication Method tab, select **Password Based** and choose one of the external identity sources you should have already configured. For example, the Active Directory instance that you have created.

Step 3 Configure any other specific password policy settings that you want for administrators who authenticate using an external identity store.

Step 4 Click **Save**.

Create an External Administrator Group

You will need to create an external Active Directory or LDAP administrator group. This ensures that Cisco ISE uses the username that is defined in the external Active Directory or LDAP identity store to validate the administrator username and password that you entered upon login.

Cisco ISE imports the Active Directory or LDAP group information from the external resource and stores it as a dictionary attribute. You can then specify that attribute as one of the policy elements when it is time to configure the RBAC policy for this external administrator authentication method.

Step 1 Choose **Administration** > **System** > **Admin Access** > **Administrators** > **Admin Groups** > **Add**.

Step 2 Enter a name and optional description.

Step 3 Choose the External radio button.
If you have connected and joined to an Active Directory domain, your Active Directory instance name appears in the Name field.

Step 4 From the External Groups drop-down list box, choose the Active Directory group that you want to map for this external administrator group.
Click the "+" sign to map additional Active Directory groups to this external administrator group.

Step 5 Click **Save**.

Configure Menu Access and Data Access Permissions for the External Administrator Group

You must configure menu access and data access permissions that can be assigned to the external administrator group.

Step 1 Choose **Administration** > **System** > **Admin Access** > **Permissions**.

Step 2 Click one of the following:

- Menu Access—All administrators who belong to the external administrator group can be granted permission at the menu or submenu level. The menu access permission determines the menus or submenus that they can access.
- Data Access—All administrators who belong to the external administrator group can be granted permission at the data level. The data access permission determines the data that they can access.

Step 3 Specify menu access or data access permissions for the external administrator group.

Step 4 Click **Save**.

Create an RBAC Policy for External Administrator Authentication

In order to configure Cisco ISE to authenticate the administrator using an external identity store and to specify custom menu and data access permissions at the same time, you must configure a new RBAC policy. This policy must have the external administrator group for authentication and the Cisco ISE menu and data access permissions to manage the external authentication and authorization.

Note You cannot modify an existing (system-preset) RBAC policy to specify these new external attributes. If you have an existing policy that you would like to use as a "template," be sure to duplicate that policy, rename it, and then assign the new attributes.

Step 1 Choose **Administration** > **System** > **Admin Access** > **Authorization** > **Policy**.

Step 2 Specify the rule name, external administrator group, and permissions.
Remember that the appropriate external administrator group must be assigned to the correct administrator user IDs. Ensure that the administrator in question is associated with the correct external administrator group.

Step 3 Click **Save**.
If you log in as an administrator, and the Cisco ISE RBAC policy is not able to authenticate your administrator identity, Cisco ISE displays an "unauthenticated" message, and you cannot access the Admin portal.

Configure Admin Access Using an External Identity Store for Authentication with Internal Authorization

This method requires you to configure the same username in both the external identity store and the local Cisco ISE database. When you configure Cisco ISE to provide administrator authentication using an external RSA SecurID identity store, administrator credential authentication is performed by the RSA identity store. However, authorization (policy application) is still done according to the Cisco ISE internal database. In addition, there are two important factors to remember that are different from external authentication and authorization:

- You do not need to specify any particular external administrator groups for the administrator.
- You must configure the same username in both the external identity store and the local Cisco ISE database.

Step 1 Choose **Administration** > **System** > **Admin Access** > **Administrators** > **Admin Users**.

Step 2 Ensure that the administrator username in the external RSA identity store is also present in Cisco ISE. Ensure that you click the **External** option under Password.

Note You do not need to specify a password for this external administrator user ID, nor are you required to apply any specially configured external administrator group to the associated RBAC policy.

Step 3 Click **Save**.