Manage Administrators and Admin Access Policies

- Role-Based Access Control, page 1
- Cisco ISE Administrators, page 1
- Cisco ISE Administrator Groups, page 3
- Administrative Access to Cisco ISE, page 13

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. These admin groups are pre-defined in the system for your convenience, as described in the following section.

Related Topics
   Cisco ISE Administrator Groups, on page 3

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.

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

<table>
<thead>
<tr>
<th>Admin Group Role</th>
<th>Access Level</th>
<th>Permissions</th>
<th>Restrictions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Device Admin</td>
<td>Manage Cisco ISE network devices and network device repository.</td>
<td>• Read and write permissions on network devices &lt;br&gt;• Read and write permissions on NDGs and all network resources object types &lt;br&gt;• View the Cisco ISE dashboard, livelogs, alarms, and reports &lt;br&gt;• Run all troubleshooting flows</td>
<td>Cannot perform any policy management or identity management or system-level configuration tasks in Cisco ISE</td>
</tr>
</tbody>
</table>

Cisco Identity Services Engine Administrator Guide, Release 2.3
<table>
<thead>
<tr>
<th>Admin Group Role</th>
<th>Access Level</th>
<th>Permissions</th>
<th>Restrictions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Admin</td>
<td>Create and manage policies for all Cisco ISE services across the network that are related to authentication, authorization, posture, profiler, client provisioning, and work centers.</td>
<td>• Read and write permissions on all the elements used in policies, such as authorization profiles, NDGs, and conditions &lt;br&gt; • Read and write permissions on identities, endpoints, and identity groups (user identity groups and endpoint identity groups) &lt;br&gt; • Read and write permissions on services policies and settings &lt;br&gt; • View the Cisco ISE dashboard, livelogs, alarms, and reports &lt;br&gt; • Run all troubleshooting flows &lt;br&gt; • Device Administration—Access to device administration work centers. Permission for TACACS Policy Conditions and results. Network Device permissions for TACACS proxy and proxy sequences.</td>
<td>Cannot perform any identity management or system-level configuration tasks in Cisco ISE &lt;br&gt; Device Administration—Access to the work center does not guarantee access to the subordinate links.</td>
</tr>
<tr>
<td>Admin Group Role</td>
<td>Access Level</td>
<td>Permissions</td>
<td>Restrictions</td>
</tr>
<tr>
<td>------------------</td>
<td>--------------</td>
<td>-------------</td>
<td>--------------</td>
</tr>
</tbody>
</table>
| 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 |
<table>
<thead>
<tr>
<th>Admin Group Role</th>
<th>Access Level</th>
<th>Permissions</th>
<th>Restrictions</th>
</tr>
</thead>
</table>
| Read-Only Admin  | Read-only access to the ISE GUI. | - View and use the functions of the dashboard, reports, and livelogs/sessions, such as filtering data, querying, saving options, printing, and exporting data.  
- Change passwords of their own accounts.  
- Query ISE using global search, reports, and livelog/sessions.  
- Filter and save data based on the attributes.  
- Export data pertaining to authentication policies, profile policies, users, endpoints, network devices, network device groups, identities (including groups), and other configurations.  
- Customize report queries, save, print, and export them.  
- Generate custom report queries, save, print, or export the results.  
- Save UI settings for future reference.  
- Download logs, such as ise-psc-log from the Operations > Troubleshoot > Download Logs page. | |
<table>
<thead>
<tr>
<th>Admin Group Role</th>
<th>Access Level</th>
<th>Permissions</th>
<th>Restrictions</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>• Perform any configuration changes such as create, update, delete, import, quarantine, and MDM actions of any objects, such as authorization policies, authentication policies, posture policies, profiler policies, endpoints, and users.</td>
<td>• Perform any system operations, such as backup/restore, registration/deregistration of nodes, sync-up of nodes, creating, editing and deleting of node groups, or upgrade/installation of patches.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Perform operations, such as CoA, endpoint debugging, modifying collection filters, bypassing suppression on live sessions data, modifying the PAN-HA failover settings, and editing the personas or services of any Cisco ISE node.</td>
<td>• Run commands that might negatively</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Import data pertaining to policies, network devices, network device groups, identities (including groups), and other configurations.</td>
<td></td>
</tr>
<tr>
<td>Admin Group Role</td>
<td>Access Level</td>
<td>Permissions</td>
<td>Restrictions</td>
</tr>
<tr>
<td>------------------</td>
<td>--------------</td>
<td>-------------</td>
<td>--------------</td>
</tr>
<tr>
<td>Super Admin</td>
<td>All Cisco ISE administrative functions. The default administrator account belongs to this group.</td>
<td>Create, read, update, delete, and eXecute (CRUDX) permissions on all Cisco ISE resources. <strong>Note</strong> 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. Device Administration—Access to device administration work centers. Permission for TACACS Policy Conditions and results. Network Device permissions for TACACS proxy and proxy sequences. In addition, permission to enable TACACS global protocol settings.</td>
<td>impact performance. For example, access to the TCP Dump in the Operations &gt; Troubleshoot &gt; Diagnostic Tools &gt; General Tools page is restricted. • Generate support bundles.</td>
</tr>
<tr>
<td>Admin Group Role</td>
<td>Access Level</td>
<td>Permissions</td>
<td>Restrictions</td>
</tr>
<tr>
<td>------------------</td>
<td>--------------</td>
<td>-------------</td>
<td>--------------</td>
</tr>
</tbody>
</table>
| 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  
  - Device Administration—Permission to enable TACACS global protocol settings. | Cannot perform any policy management or system-level configuration tasks in Cisco ISE |
<table>
<thead>
<tr>
<th>Admin Group Role</th>
<th>Access Level</th>
<th>Permissions</th>
<th>Restrictions</th>
</tr>
</thead>
<tbody>
<tr>
<td>External RESTful Services (ERS) Admin</td>
<td>Full access to all ERS API requests such as GET, POST, DELETE, PUT</td>
<td>• Create, Read, Update, and Delete ERS API requests</td>
<td>The role is meant only for ERS authorization supporting Internal Users, Identity Groups, Endpoints, Endpoint Groups, and SGT</td>
</tr>
<tr>
<td>External RESTful Services (ERS) Operator</td>
<td>Read-only access to ERS API, only GET</td>
<td>• Can only Read ERS API requests</td>
<td>The role is meant only for ERS authorization supporting Internal Users, Identity Groups, Endpoints, Endpoint Groups, and SGT</td>
</tr>
<tr>
<td>TACACSS+ Admin</td>
<td>Full access</td>
<td>Access to the:</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Device Administration Work Center</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Deployment—To enable TACACS+ services.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• External Identity Stores.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Operations &gt; TACACS Live Logs page.</td>
<td></td>
</tr>
</tbody>
</table>

**Related Topics**

Cisco ISE Administrators, on page 1

**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.

Note
If an internal user is configured with an external identity store for authentication, while logging in to the ISE Admin portal, the internal user must select the external identity store as the Identity Source. Authentication will fail if Internal Identity Source is selected.

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 and submenu 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, read only, 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. 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. The key icon represents menu access privileges for the menus and submenus and the key with a close icon represents no access for different RBAC groups.

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.

Prerequisites for Granting Data Access Permissions

When an RBAC admin has Full Access permission to an object (for example, Employee in the User Identity Groups data type), the admin can view, add, update, and delete users who belong to that group. Ensure that the admin has menu access permission granted for the Users page (Administration > Identity Management > Identities > Users). This is applicable for Network Devices and Endpoints objects (based on the permissions granted to the Network Device Groups and Endpoint Identity Groups data types).

You cannot enable or restrict data access for network devices that belong to the default network device group objects—All Device Types and All Locations. All network devices are displayed if Full Access data permission is granted to an object created under these default network device group objects. Therefore, it is recommended that you create a separate hierarchy for the Network Device Groups data type, which is independent of the default network device group objects. You should assign the network device objects to the newly created Network Devices Groups to create restricted access.

**Note**
You can enable or restrict data access permissions only for the User Identity Groups, Network Device Groups, and Endpoint Identity Groups. It is not applicable for Admin Groups.

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. 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.

There are three data access permissions namely, Full Access, No Access, and Read Only access that can be granted to admin groups.

The Read Only permission can be granted to the following admin groups:

- Administration > Admin Access > Administrators > Admin Groups
- Administration > Groups > User Identity Group
- Administration > Groups > Endpoint Identity Groups
- Network Visibility > Endpoints
- Administration > Network Resources > Network Device Groups
- Administration > Network Resources > Network Devices
- Administration > Identity Management > Identities
- Administration > Identity Management > Groups > User Identity Groups
- Administration > Identity Management > Groups > Endpoint Identity Groups

If you have Read Only permission on a data type (for example, Endpoint Identity Groups), you will not be able to perform CRUD operations on the data type. If you have Read Only permission on an object (for example, GuestEndpoints), you cannot perform edit/delete operations on the object.

The image below describes how the Data Access Privileges apply at the second- or third-level menu that contains additional submenus or options for different RBAC groups.
**Label** | **Description**
--- | ---
1 | Denotes full access for the User Identity Groups data type.
2 | Denotes that Endpoint Identity Groups derives the maximum permission (full access) that is granted to its child (Asia).
3 | Denotes no access for the object (Blacklist).
4 | Denotes that the parent (Continents) derives the maximum access permission granted to its child (Asia).
5 | Denotes Read Only access for the object (Australia).
6 | Denotes that when Full Access is granted to the parent (Network Device Groups), it results in the children automatically inheriting permissions.
Denotes that when Full Access is granted to the parent (Asia), it results in the objects inheriting the Full Access permission, unless permissions are explicitly granted to the objects.

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, Read Only Access, or No Access.

Step 4
Click Save.

The Read-Only Admin Policy
The default Read-Only Admin policy is available in the Administration > System > Admin Access > Authorization > Policy page. This policy is available for both new installation and upgraded deployment. The Read-Only Admin policy is applicable to the Read-Only Admin group. By default, Super Admin Menu Access and Read-Only Data Access permissions are granted to Read-Only administrators.

Note
The default read-only policy is mapped to the Read Only Admin group. You cannot create custom RBAC policy using the Read Only Admin group.

Customize Menu Access for the Read-Only Administrator
By default, Read-Only Administrators are given Super Admin Menu Access and Read Only Admin Data Access. However, if the Super Admin requires that the Read-Only Administrator view only the Home and Administration tabs, the Super Admin can create a custom menu access or customize the default Permissions...
to, for example, MnT Admin Menu Access or Policy Admin Menu Access. The Super Admin cannot modify the Read Only Data Access mapped to the Read Only Admin Policy.

Step 1  Log in to the Admin Portal as a Super Admin.
Step 2  Navigate to the Administration > System > Admin Access > Authorization > Permissions > Menu Access page.
Step 3  Click Add and enter a Name (for example, MyMenu) and Description.
Step 4  In the Menu Access Privileges section, you can select the Show/Hide option to choose the required options (for example, Home and Administration tabs) that should be displayed for the Read-Only Administrator.
Step 5  Click Submit. The custom menu access permission is displayed in the Permissions drop-down corresponding to the Read-Only Admin Policy displayed in the Administration > System > Admin Access > Authorization > Policy page.
Step 7  Click the Permissions drop-down corresponding to the Read-Only Admin Policy.
Step 8  Select a default (MnT Admin Menu Access) or custom menu access permission (MyMenu) that you have created in the Administration > System > Admin Access > Authorization > Permissions > Menu Access page.
Step 9  Click Save. You will encounter an error if you choose Data Access permissions for the Read-Only Admin policy.

Note   When you log in to the Read-Only Admin portal, a Read-Only icon appears at the top of the screen and you can view only the specified menu options without data access.

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 (Administration > System > Admin Access > Authorization > Policy) contains a list of default policies. You cannot edit or delete these default policies. However, you can edit the data access permissions for the Read-Only Admin policy. The RBAC policies page also allows you to create custom RBAC policies for an admin group specifically for your work place, and apply to personalized admin groups.

When you assign limited menu access, make sure that the data access permissions allow the administrator to access the data that is required to use the specified menus. For example, if you give menu access to the MyDevices portal, but don't allow data access to Endpoint Identity Groups, then the administrator cannot modify the portal.

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. You cannot edit or delete these default policies. However, you can edit the data access permissions for the default Read-Only Admin policy.

**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.

**Before You Begin**

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

**Step 1**

**Step 2**
Select Allow only listed IP addresses to connect.

**Step 3**
From the Configure IP List for Access Restriction area, click Add.

**Step 4**
Enter IP addresses in the classless interdomain routing (CIDR) format in the IP address field.

**Step 5**
Enter the subnet mask in the Netmask in CIDR format field.

**Step 6**
Click OK. Repeat the process to add more IP address ranges to this list.

**Step 7**
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.

---

**Related Topics**

- [Administrator Password Policy Settings](#)
- [Configure Account Disable Policy for Administrator Accounts](#)
- [Configure Lock or Suspend Settings for Administrator Accounts](#)

---

### Configure Account Disable Policy for Administrator Accounts

Cisco ISE allows you to disable the administrator account if the administrator account is not authenticated for the configured consecutive number of days.

### Step 1
Choose Administration > System > Admin Access > Authentication > Account Disable Policy.

### Step 2
Check the **Disable account after n days of inactivity** check box and enter the number of days. This option allows you to disable the administrator account if the administrator account was inactive for the consecutive number of days. However, you can exclude individual administrator account from this account disable policy using the **Inactive Account Never Disabled** option available at Administration > System > Admin Access > Administrators > Admin Users.

### Step 3
Click **Save** to configure the global account disable policy for administrators.
Configure Lock or Suspend Settings for Administrator Accounts

Cisco ISE allows you to lock or suspend administrator accounts (including password-based Internal Admin accounts and certificate-based Admin accounts) that have more than a specified number of failed login attempts.

**Step 1** Choose Administration > System > Admin Access > Authentication > Lock/Suspend Settings.

**Step 2** Check the Suspend or Lock Account With Incorrect Login Attempts checkbox and enter the number of failed attempts after which action should be taken. The valid range is between 3 and 20.

- **Suspend Account For n Minutes**—Select this option to suspend an account that exceeds a specified number of incorrect login attempts. The valid range is between 15 and 1440.
- **Lock Account**—Select this option to lock an account that exceeds a specified number of incorrect login attempts.

You can enter a custom e-mail remediation message, such as asking the end user to contact helpdesk to unlock the account.

**Note** The Lock/Suspend settings were available in the Password Policy tab in the earlier releases of Cisco ISE.

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.

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Choose Administration &gt; System &gt; Admin Access &gt; Settings &gt; Session &gt; Session Info.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Check the check box next to the session ID that you want to terminate and click Invalidate.</td>
</tr>
</tbody>
</table>

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.

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

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.
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.

The External Groups Mapped column displays the number of external groups that are mapped to internal RBAC roles. You can click the number corresponding to a admin role to view the external groups (for example, if you click 2 displayed against Super Admin, the names of two external groups are displayed).

**Step 2** Click Add.

**Step 3** Enter a name and optional description.

**Step 4** 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 5** 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 6** Click Save.
Create an Internal Read-Only Admin

Step 1  Choose Administration > System > Admin Access > Administrators > Admin Users.
Step 2  Click Add and select Create An Admin User.
Step 3  Check the Read Only check box to create a Read-Only administrator.

Map External Groups to the Read-Only Admin Group

Step 1  Choose Administration > Identity Management > External Identity Sources to configure the external authentication source. See the Manage Users and External Identity Sources chapter for more information.
Step 2  Click the required external identity source, such as Active Directory or LDAP, and then retrieve the groups from the selected identity source.
Step 3  Choose Administration > System > Admin Access > Authentication to map the authentication method for the admin access with the identity source.
Step 4  Choose Administration > System > Admin Access > Administrators > Admin Groups and select Read Only Admin group.
Step 5  Check the Type External check box and select the required external groups for whom you intend to provide read-only privileges.
Step 6  Click Save.

Note
An external group that is mapped to a Read-Only Admin group cannot be assigned to any other admin group.

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.