Manage Administrators and Admin Access Policies

- Cisco ISE Administrators, on page 1
- Cisco ISE Administrator Groups, on page 2
- Administrative Access to Cisco ISE, on page 11

Cisco ISE Administrators

Administrators can 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.

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 that are 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.

The username and password that you configure during 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 a CLI admin user is admin, and the password is defined during setup. There is no default password. This CLI admin user is the default admin user, and this user account cannot be deleted. However, it can be edited by other administrators, including options to enable, disable, or change password for this account.

You can either 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 are users who have local privileges to configure and operate the Cisco ISE system.

Administrators are assigned to one or more admin groups.

Related Topics
- Cisco ISE Administrator Groups, on page 2
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 the 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 Administrator

Cisco ISE administrators need accounts with specific roles assigned to them to perform specific administrative tasks. You can create administrator accounts and assign one or more roles to these admins based on the administrative tasks that these admins have to perform.

You can use the Admin Users window 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  From the drop-down, choose one of the following options:

  • Create an Admin User

    If you choose Create an Admin User, a New Administrator window appears where you can configure account information for the new admin user.

  • Select from Network Access Users

    If you choose Select from Network Access Users, a list of current users appears, from which you can choose a user. The Admin User window corresponding to this user appears.

Step 3  Enter values in the fields. The characters supported for the Name field are # $ ’ ( ) * + - . / @ _.
Step 4  Click Submit to create a new administrator in the Cisco ISE internal database.

Related Topics
  Read-Only Admin Policy
  Create an Internal Read-Only Admin
  Customize Menu Access for the Read-Only Administrator
  Map External Groups to the Read-Only Admin Group

Cisco ISE Administrator Groups

Administrator groups are role-based access control (RBAC) groups in Cisco ISE. All the 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.

An administrator account with any level of access can be used to modify or delete objects for which it has permission, on any window it has access to.
The Cisco ISE security model limits administrators to creating administrative groups that contain the same set of privileges that the administrator has. The privileges given are based on the administrative role of the user, as defined in the Cisco ISE database. Thus, administrative groups form the basis for defining privileges to access 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

<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, identity management, or system-level configuration tasks in Cisco ISE.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Manage guest access settings.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Customize end-user web portals.</td>
<td>• Cannot view any reports.</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 live logs.</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. | 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 live logs.  
                   • Manage alarms (create, update, view, and delete). | Cannot perform any policy management, 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</td>
<td>Cannot perform any policy management, identity management, or system-level configuration tasks in Cisco ISE.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Read and write permissions on Network Device Groups and all network resources object types.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• View the Cisco ISE dashboard, live logs, alarms, and reports.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Run all troubleshooting flows.</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>
| Policy Admin     | Create and manage policies for all Cisco ISE services across the network, which are related to authentication, authorization, posture, profiler, client provisioning, and work centers. | • Read and write permissions on all the elements that are 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, live logs, alarms, and reports.  
• Run all troubleshooting flows.  
• Device Administration—Access to device administration work centers. Permission for TACACS policy conditions and results. Network device permissions for TACACS proxy and proxy sequences. | Cannot perform any identity management or system-level configuration tasks in Cisco ISE.  
Device Administration—Access to the work center does not guarantee access to the subordinate links. |
<table>
<thead>
<tr>
<th>Admin Group Role</th>
<th>Access Level</th>
<th>Permissions</th>
<th>Restrictions</th>
</tr>
</thead>
</table>
| RBAC Admin       | All the tasks under the Operations menu, except for 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, live logs, alarms, and reports.  
• Run all the 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>
<tbody>
<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. 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 an admin group.</td>
<td>- Device Administration—Access to the work center does not guarantee access to the subordinate links. - Only an admin user from the default Super Admin Group can modify or delete other admin users. Even an externally mapped user who is part of an Admin Group cloned with the Menu and Data Access privileges of the Super Admin Group cannot modify or delete an admin user.</td>
</tr>
</tbody>
</table>

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.
<table>
<thead>
<tr>
<th>Admin Group Role</th>
<th>Access Level</th>
<th>Permissions</th>
<th>Restrictions</th>
</tr>
</thead>
</table>
| System Admin     | All Cisco ISE configuration and maintenance tasks. | Full access (read and write permissions) to perform all the 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 window.  
  • Read and write permissions for all options under Administration > System.  
  • View 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. |
### Create an Admin Group

The **Admin Groups** window 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.

<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</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>TACACS+ Admin</td>
<td>Full access</td>
<td>Access to:</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 window.</td>
<td></td>
</tr>
</tbody>
</table>

**Related Topics**

[Cisco ISE Administrators](#), on page 1
• **Internal**: Administrators assigned to this group type authenticate against the credentials that are stored in the Cisco ISE internal database.

• **External**: Administrators assigned to this group authenticate against the credentials stored in the external identity store that you select in the Administration > System > Admin Access > Authentication > Authentication Method window. You can specify the external groups, if required.

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.

**Step 4**  
Click **Add** in the **Member Users** area to add users to this admin group.

**Step 5**  
Click **Submit**.

To delete users from the admin group, check the check box corresponding to the user that you want to delete, and click **Remove**.

---

**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. Grant administrative access only 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.

**Administrative Access Methods**

You can connect to the Cisco ISE servers in several ways. The PAN runs the Administrators portal, which requires the admin password to log in. Other ISE persona servers are accessible through SSH or the console, where you run the CLI. This section describes the process and password options available for each connection type.

- **Admin password**: The Cisco ISE Admin user that you created during installation times out in 45 days by default. You can prevent that by turning off the password lifetime on Administration > System > Admin Settings. Click the Password Policy tab, and uncheck Administrative passwords expire under Password Lifetime.

  If you do not do this, and the password expires, you can reset the admin password in the CLI by running the **application reset-passwd** command. You can reset the Admin password by connecting to the console to access the CLI, or by rebooting the ISE image file to access the boot options menu.

- **CLI password**: You must enter a CLI password during installation. If you have a problem logging in to the CLI because of an invalid password, you can reset the CLI password. Connect to the console and run the **password CLI** command to rest the password. See the **ISE CLI Reference** for more information.

- **SSH access to the CLI**: You can enable SSH access either during installation or after, using the **service sshd** command. You can also force SSH connections to use a key. Note that when you do this, SSH connections to all the network devices also use that key, See **SSH Key Validation**. You can force the SSH key to use the Diffie-Hellman Algorithm. Note that ECDSA keys are not supported for SSH keys.
Role-Based Admin Access Control in Cisco ISE

Cisco ISE provides role-based access control (RBAC) policies that ensure security by restricting administrative privileges. RBAC policies are associated with default admin groups to define roles and permissions. A standard set of permissions (for menu as well as data access) is paired with each of the predefined admin groups, and is thereby aligned with the associated role and job function.

Some features in the user interface require certain permissions for their use. If a feature is unavailable, or you are not allowed to perform a specific task, your admin group may not have the necessary permissions to perform the task that utilizes the feature.

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

Note
Only system-defined admin users with SuperAdmin or ReadOnlyAdmin permissions can see the identity-based users who are not a part of a user group. Admins you create without these permissions cannot see these users.

Role-Based Permissions

Cisco ISE allows you to configure permissions at the menu and data levels: these are called 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 and write, read only, or no access to the Admin Groups, User Identity Groups, Endpoint Identity Groups, Locations, and Device Types data in the Cisco ISE interface.

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 that network administrator is associated.

Note
If you are using customized RBAC policies for admin access, ensure that you provide all relevant menu access for a given data access. For example, to add or delete endpoints with data access of Identity or Policy Admin, you must provide menu access to Work Center > Network Access and Administration > Identity Management.
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 a Super Admin user, all the menu items are available. For other admin users, all the menu items in the Menu Access Privileges column are available for standalone deployment and primary node in a distributed deployment. For secondary nodes in a 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) Expand the ISE Navigation Structure menu to the desired level, and click the option(s) for which you want to create permissions.
b) In the Permissions for Menu Access pane, click Show.

Step 3
Click Submit.

Default Data Access Permissions

Cisco ISE comes with a set of predefined data access permissions. These 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 network device groups. RBAC policies are defined based on the administrator (RBAC) group, menu access, and data access permissions. You should 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 for a data type (for example, Endpoint Identity Groups), you will not be able to perform CRUD operations on that data type. If you have read-only permission for an object (for example, GuestEndpoints), you cannot perform edit or delete operations on that object.

Figure 1: The following image describes how Data Access Privileges apply at the second-level or third-level menu that contains additional submenus or options for different RBAC groups.
<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Denotes full access for the User Identity Groups data type.</td>
</tr>
<tr>
<td>2</td>
<td>Denotes that Endpoint Identity Groups derive the maximum permission (full access) that is granted to its child (Asia).</td>
</tr>
<tr>
<td>3</td>
<td>Denotes no access for the object (Blacklist).</td>
</tr>
<tr>
<td>4</td>
<td>Denotes that the parent (Continents) derives the maximum access permission granted to its child (Asia).</td>
</tr>
<tr>
<td>5</td>
<td>Denotes Read Only access for the object (Australia).</td>
</tr>
<tr>
<td>6</td>
<td>Denotes that when Full Access is granted to the parent (Network Device Groups), it results in the children automatically inheriting permissions.</td>
</tr>
<tr>
<td>7</td>
<td>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.</td>
</tr>
</tbody>
</table>

**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**.

**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. 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 that administrator cannot modify the portal.

Note
Admin users can move endpoint MAC addresses from the Endpoint Identity Groups they have read-only access to, to the Endpoint Identity Groups they have full access to. The other way around is not possible.

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.

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.

Related Topics
Allow Administrative Access to Cisco ISE from Select IP Addresses, on page 17

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 Choose Administration > System > Admin Access > Settings > Access > IP Access.
Step 2 Select Allow only listed IP addresses to connect.
Note Connection on Port 161 (SNMP) is used for Administrative access. However, when IP Access restrictions are configured, the snmpwalk fails if the node from which it was performed is not configured for Administrative access.

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.
Note This IP address can range from IPv4 and IPv6. You can now configure multiple IPv6 addresses for an ISE node.

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.
Step 8 Click Reset to refresh the IP Access page.
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

- Email notifications for internal Admin users are sent to root@host. You cannot configure the email address, and many SMTP servers reject this email.
  
  You can follow open defect CSCui5583, which is an enhancement to allow you to change the email address.

- 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, on page 19
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 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**.

**Related Topics**

Session Timeout and Session Information Settings

Terminate an Active Administrative Session

Cisco 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**.

---

**Related Topics**

- Session Timeout and Session Information Settings

---

**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.

Administrators who belong to a Super Admin group, and are configured to authenticate and authorize using an external identity store, can also authenticate with the external identity store for CLI access.

---

**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.

**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.

**Related Topics**

Administrator Password Policy Settings

**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.

**Step 2** Click Add.

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

---

**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.