



## CHAPTER 4

# Managing Identities and Admin Access

---

This chapter describes how Cisco Identity Services Engine manages its network identities and access to its resources using role-based access control policies, permissions, and settings. Cisco ISE allows you to limit access to a set of network resources or allows a certain type of system operation to be performed based on the identity of individual users, a user group or members, or an endpoint based on its corresponding role. Each role in Cisco ISE defines a set of access policies, permissions, or settings.

A user, user group or member, or an endpoint is recognized by the Cisco ISE network according to its network identity. Once identified, the network grants the access and privileges that are defined and associated with the identity. The following topics provide information and details necessary for understanding the concepts that affect how you manage identities and network access in Cisco ISE:

- [Configuring Access for Users, Endpoints, Admins, Groups, Permissions, and Accounts, page 4-2](#)
- [Understanding User Identities, Groups, and Admin Access, page 4-2](#)
- [Understanding Identity Management Terminology, page 4-4](#)
- [Network Access Users, page 4-9](#)
- [Endpoints, page 4-15](#)
- [Latest Network Scan Results, page 4-27](#)
- [Understanding Admin Access Terminology, page 4-27](#)
- [Managing Admin Access \(RBAC\) Policies, page 4-50](#)
- [Configuring Settings for Accounts, page 4-61](#)
- [Endpoint Identity Groups, page 4-71](#)



### Note

---

When you are ready to start configuring access for the Cisco ISE network users, endpoints, administrators, groups, permissions, and accounts, see [Configuring Access for Users, Endpoints, Admins, Groups, Permissions, and Accounts, page 4-2](#).

---

# Configuring Access for Users, Endpoints, Admins, Groups, Permissions, and Accounts

This section is the starting point for configuring access for Cisco ISE network access and sponsor users, endpoints, administrators, user groups, permissions, accounts, and endpoint groups as described in the following topics:

- [Configuring Network Access and Sponsor Users, page 4-9](#)
- [Configuring Endpoints, page 4-17](#)
- [Configuring Cisco ISE Administrators, page 4-34](#)
- [Configuring Admin Groups, page 4-37](#)
- [Configuring User Identity Groups, page 4-41](#)
- [Filtering, Creating, Editing, and Deleting Endpoint Identity Groups, page 4-73](#)
- [Configuring Menu Access Permissions, page 4-50](#)
- [Configuring Data Access Permissions, page 4-54](#)
- [Configuring Network Access for User Accounts, page 4-66](#)
- [Configuring Network Access User Accounts, page 4-68](#)

## Understanding User Identities, Groups, and Admin Access

Once identified and authenticated, each Cisco ISE user, group, or endpoint can access system resources or services and perform network management tasks for which they are authorized. Identification and authentication requires the use of credentials (such as usernames, passwords, certificates, or one-time passwords) that verify each administrator, network access user, user or admin group member, and endpoint as being legitimate and authorized to perform the tasks or activities associated with its identity.

**Note**

---

An identity role is a set of administrative tasks, each with an associated set of permissions that apply to network users, administrators, groups, or endpoints. For example, an administrator can have more than one predefined role, and a role can apply to multiple administrators.

---

Identity roles limit each network access user, administrator, or endpoint to a specific set of privileges and access, which is based on identity, type of administrative group in which they belong, or type of endpoint. Each member of an administrative group shares a common set of group-based privileges that are granted to that group. Cisco ISE supports a number of administrative groups, each with a unique set of privileges.

Groups are a collection of individual users or endpoints that share a common set of privileges that allow them to access a specific set of Cisco ISE services and functionality. For example, if you belong to the Change User Password admin group, you can change administrative passwords for other users.

Cisco ISE contains a variety of administrative groups, each with its own set of privileges. Whenever a user is assigned to an administrative group, that user is automatically promoted to an Admin user for that group, and shares the same privileges as every other member of that group.

**Note**

Only the administrator who creates an administrative group can add, delete, or modify the members of that group. Simply being a member of an administrative group does not give that member any administrative privileges over that group.

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.

Admin access is the mechanism by which the network resources, services, or functions are defined by your role, and this mechanism affects access for every user, group, or endpoint. 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 in which the entity belongs, and the corresponding permissions and settings based upon the role of the entity.

There are three functional groupings for identity management and admin access in Cisco ISE, with each group containing one or more components:

- **Identities**

- Users—Defined based on user data and assigned role (for details, see [Table 4-1](#)). This component is where you can configure a network access user identity for accessing resources and services in a Cisco ISE network.
- Endpoints—Defined based on the MAC address, device policy, and device identity group to which this endpoint belongs (for details, see [Table 4-1](#)). This component is where you can configure a network-capable device identity that can connect to and access resources and services in a Cisco ISE network.

**Note**

In a Cisco ISE network, endpoints represent the total number of supported users and devices. This endpoint can be any combination of users, personal computers, laptops, IP phones, smart phones, gaming consoles, printers, fax machines, or other types of network devices. A distinction is made only in the following identity definitions to differentiate between network access users and Cisco ISE network endpoints.

- **Groups**

- User Identity Groups—Defined based on group name, description, members, group type, and assigned role (for details, see [Table 4-1](#)). This component is where you can configure a user group by the group or role name that can access resources and services in a Cisco ISE network.
- Endpoint Identity Groups—Defined based on group name, description, parent group, and endpoint type (for details, see [Table 4-1](#)). This component is where you can configure an endpoint group by the group or device name that can access resources and services in a Cisco ISE network.

- **Admin Access**

- Policies—Role-based access control (RBAC) policies defined by rule name, groups, and permissions (for details, see [Table 4-10](#)). This component is where you can configure RBAC policies that allow admin groups to access resources and services in a Cisco ISE network.
- Administrators—Defined based on admin user data, admin group, and assigned role (for details, see [Table 4-10](#)). This component is where you can create and manage administrators who can access resources and services in a Cisco ISE network.

- Admin Groups—Defined based on group name, description, members, group type, and assigned role (for details, see [Table 4-10](#)). This component is where you can create and manage administrator groups who can access resources and services in a Cisco ISE network.
- Permissions—Defined based on group name and role, description, and menu and data access permissions (for details, see [Table 4-10](#)). This component is where you can create and manage menu and data access permissions for admin groups to access resources and services in a Cisco ISE network.
- Settings—Defined based on IP address access permissions, password policy, and session timeout values (for details, see [Table 4-10](#)). This component is where you can create and manage IP address-based access, password policy, and session timeout settings for users and groups to access resources and services in a Cisco ISE network.

**For more information:**

The following topics provide information about identity management and admin access terminology and the related user interface that is used in the Cisco ISE network:

- For more information on identity management terminology, see [Understanding Identity Management Terminology, page 4-4](#).
- For more information on managing user and group identities, see [Managing User Identity and Group Identity Types Using the User Interface, page 4-5](#).
- For more information on admin access terminology, see [Understanding Admin Access Terminology, page 4-27](#).

## Understanding Identity Management Terminology

[Table 4-1](#) defines and describes basic identity management terminology that applies to the users, groups, group members, and endpoints in Cisco ISE.

**Table 4-1** Cisco ISE Identity Management Terminology

Term	Description	Identity Role
User	<p>User identity is like a container that holds information elements about each user, which form network access credentials for this user. Each user's identity is defined by data that can include username, e-mail address, password, account description, associated administrative group, user group, and role.</p> <p>A user role is a set of permissions that determine what tasks a user can perform or what services can be accessed on the ISE network.</p>	User (for example, a network access user)
Group	<p>Group identity is composed of information elements that identify and describe a specific group of users that belong to the same administrative group. A group name is also a description of the functional role that the members of this group have. A group is a listing of the users that belong to this group.</p> <p>A group role is the set of permissions that determine the tasks each member of this group can perform or the services that can be accessed on the Cisco ISE network. Because common privileges are assigned to a group, any member of that group has that defined set of permissions.</p>	Group (for example, the System Admin group)

Table 4-1 Cisco ISE Identity Management Terminology (continued)

Term	Description	Identity Role
Group Member	<p>Group members are individual users that belong to a specific administrative group, and are listed in the Member User table for the group. The Member User table includes information about each member, including the user status (Enabled or Disabled), e-mail address, username, and user information (using the format: First Name, Last Name).</p> <p>Groups allow you to map individual users to a group, and in this way, confer a role-based identity and privileges associated with the group on each member. By using the Member User table, Cisco ISE allows you to filter entries in a group and add or remove entries in the table.</p> <p>Because group identity and privileges are shared by all members of the group, being a member of a group can also be used as a condition in authorization policies.</p> <p>A group member role is a set of permissions that determine the tasks a user (by virtue of being a member of a group) can perform or the services that can be accessed on the Cisco ISE network.</p>	Group member  (for example, a member of the Network Device Admin group)
Endpoints	<p>From the Cisco ISE network perspective, concurrent endpoints can be users, personal computers, laptops, IP phones, smart phones, gaming consoles, printers, fax machines, or any other devices supported by the Cisco ISE network.</p> <p>However, from the perspective of the identity role of a specific network device, an endpoint identity defines these items:</p> <ul style="list-style-type: none"> <li>• The network-capable device type</li> <li>• How the device connects to your Cisco ISE network</li> <li>• The network resources that can be used through wired, wireless network access devices (NADs), or by using a virtual private network (VPN) connection</li> </ul> <p>An endpoint role is a set of permissions that determine the tasks that the device can perform or services that can be accessed on the Cisco ISE network.</p>	Endpoint device  (for example, an iPhone device)

**For more information:**

- For more information on administrators and admin groups, see [Table 4-10](#).
- For more information on permissions and settings, see [Table 4-10](#).
- For more information on admin group role types, see [Table 4-11](#).

## Managing User Identity and Group Identity Types Using the User Interface

Use the Cisco ISE dashboard as your starting point for displaying and performing the operations that allow you to manage network access users, endpoints, user identity, and endpoint identity groups. You perform management operations by using the controls, tabs, and navigation pane options for the following tasks:

- To configure users—Choose **Administration > Identity Management > Identities**
- To configure endpoints—Choose **Administration > Identity Management > Identities > Endpoints**

- To configure user identity groups—Choose **Administration > Identity Management > Groups > User Identity Groups**
- To configure endpoint identity groups—Choose **Administration > Identity Management > Groups > Endpoint Identity Groups**

The following identifies the Cisco ISE user interface tab or menu option choices needed to perform tasks associated with users and endpoints:

- Identities—Users
  - Display the currently configured user identities.
  - Create new user identities.
  - Modify or delete existing user identities.
  - Change the status of existing user identities.
  - Import or export user identities using comma-separated value (.csv) files.
  - Duplicate an existing user identity (you can use this identity as a template to create other user identities).
  - Filter or search for existing user identities based on search criteria you configure.
- Identities—Endpoints
  - Display the currently configured endpoint identities.
  - Create new endpoint identities.
  - Modify or delete existing endpoint identities.
  - Import or export endpoint identities using .csv files.
  - Filter or search for existing endpoint identities based on search criteria you configure.

The following identifies the Cisco ISE user interface tab or menu option choices needed to perform tasks that are associated with User Identity Groups and Endpoint Identity Groups:

- Identity Groups—User Identity Groups
  - Display the currently configured user identity groups.
  - Create new user identity groups.
  - Modify or delete existing user identity groups.
  - Import or export user identity groups using .csv files.
  - Filter or search for existing user identity groups based on search criteria you configure.
- Identity Groups—Endpoint Identity Groups
  - Display the currently configured endpoint identity groups.
  - Create new endpoint identity groups.
  - Modify or delete existing endpoint identity groups.
  - Filter or search for existing endpoint identity groups based on search criteria you configure.

Table 4-2 lists the configurable user and group identity values you can set using the controls and options available on the Identities tab.

**Table 4-2 Cisco ISE User and Group Identity Values**

Tab or Sub Tab	User Interface Page Functions	Group Box	Values
<b>Identities: Users</b>			
<i>Your starting point for managing network access user values</i>	<ul style="list-style-type: none"> <li>• Edit</li> <li>• Add</li> <li>• Change Status</li> <li>• Import</li> <li>• Export</li> <li>• Delete</li> <li>• Duplicate</li> <li>• Filter</li> </ul>	Network Access User	<ul style="list-style-type: none"> <li>• Name*</li> <li>• E-mail</li> </ul>
		Password	<ul style="list-style-type: none"> <li>• Password*</li> <li>• Re-Enter Password*</li> </ul>
		User Information	<ul style="list-style-type: none"> <li>• First Name</li> <li>• Last Name</li> </ul>
		Account Options	<ul style="list-style-type: none"> <li>• Description</li> <li>• Password Change check box (change on next login)</li> </ul>
		User Groups	<ul style="list-style-type: none"> <li>• Group affiliation</li> </ul>
		Status	<ul style="list-style-type: none"> <li>• Enabled</li> <li>• Disabled</li> </ul>
<b>Identities: Endpoints</b>			
<i>Your starting point for managing endpoint values</i>	<ul style="list-style-type: none"> <li>• Edit</li> <li>• Create</li> <li>• Delete</li> <li>• Import</li> <li>• Export</li> <li>• Filter</li> </ul>	Endpoints	<ul style="list-style-type: none"> <li>• MAC Address*</li> <li>• Policy Assignment</li> <li>• Identity Group Assignment</li> </ul>

Table 4-2 Cisco ISE User and Group Identity Values (continued)

Tab or Sub Tab	User Interface Page Functions	Group Box	Values
<b>Groups: User Identity Groups</b>			
<i>Your starting point for managing user identity group and member values</i>	<ul style="list-style-type: none"> <li>• Edit</li> <li>• Add</li> <li>• Delete</li> <li>• Filter</li> <li>• Import</li> <li>• Export</li> </ul>	Identity Group	<ul style="list-style-type: none"> <li>• Name*</li> <li>• Description</li> </ul>
		Member Users	<ul style="list-style-type: none"> <li>• Users               <ul style="list-style-type: none"> <li>– Status</li> <li>– E-mail</li> <li>– Username</li> <li>– First Name</li> <li>– Last Name</li> </ul> </li> </ul>
<b>Groups: Endpoint Identity Groups</b>			
<i>Your starting point for managing endpoint identity group values</i>	<ul style="list-style-type: none"> <li>• Edit</li> <li>• Create</li> <li>• Delete</li> <li>• Filter</li> </ul>	Endpoint Group List	<ul style="list-style-type: none"> <li>• Name*</li> <li>• Description</li> <li>• Parent Group</li> </ul>
		Endpoints	<ul style="list-style-type: none"> <li>• Identity Group Endpoints               <ul style="list-style-type: none"> <li>– MAC Address</li> </ul> </li> </ul>

**Note**

Configurable values marked with an asterisk (\*) are required.

When you create an identity, you can configure or assign account options using the Account Options panel. To configure or assign account options, check the **Password Change** check box, which prompts each user to change their password at the next login.

**Note**

Only administrators that belong to the Identity Admin group are allowed to perform this same function for administrators.

To complete the configuration using your choices for user or endpoint identity types, click **Submit** to create these identities in the Cisco ISE database.

**For more information:**

- For more information on configuring users, see [Configuring Network Access and Sponsor Users, page 4-9](#).
- For more information on configuring endpoints, see [Endpoints, page 4-15](#).
- For more information on configuring user identity groups, see [Configuring User Identity Groups, page 4-41](#).
- For more information on configuring endpoint identity groups, see [Filtering, Creating, Editing, and Deleting Endpoint Identity Groups, page 4-73](#).
- For more information on configuring endpoints in an endpoint identity group, see [Filtering, Creating, Editing, and Deleting Endpoint Identity Groups, page 4-73](#).



# Network Access Users

A network user is a Cisco ISE user that is authorized to access the Cisco ISE network resources based on identity. The network access user identity contains information about the user and forms the network access credentials for the user (and can consist of username, e-mail address, password, account description, associated administrative group, user group, and role).

To support Cisco ISE sponsor groups, you must explicitly create a sponsor user to be associated with a predefined sponsor group. A sponsor user can be considered as another type of network access user and is created using the same process in the following procedure.

For specific details about sponsor users and sponsor groups, see the *Cisco Identity Services Engine Sponsor Portal User Guide, Release 1.1.x*.

## Configuring Network Access and Sponsor Users

The Network Access Users page lets you display, create, modify, delete, change the status, import or export users, duplicate, or search for attributes of Cisco ISE network access users.

This section covers the following topics:

- [Displaying Existing Network Access Users, page 4-9](#)
- [Creating a New Network Access or Sponsor User, page 4-10](#)
- [Modifying an Existing Network Access User, page 4-10](#)
- [Deleting an Existing Network Access User, page 4-11](#)
- [Changing the Status of an Existing Network Access User, page 4-11](#)
- [Importing or Exporting Existing Network Access Users, page 4-12](#)
- [Duplicating an Existing Network Access User, page 4-13](#)
- [Searching for Specific Attributes in an Existing Network Access User, page 4-13](#)



### Warning

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



### Note

You can change the order in which the user groups are listed, and the order is obeyed once it is saved. Be advised that the visual display reverts to alphabetical order, even though the user groups are processed in the newly specified order.

## Displaying Existing Network Access Users

You can view all locally defined network access users from the Cisco ISE GUI.

**To display existing network access users, complete the following steps:**

**Step 1** Choose **Administration > Identity Management > Identities > Users**.

The Network Access Users page appears listing all existing locally defined network access users.

- Step 2** (Optional) To create a new network access user, click the Action icon and choose **Create A Network Access User**.
- 

### Creating a New Network Access or Sponsor User

Use this procedure to create and configure new locally configured network access users or the required sponsor user that is necessary for Cisco ISE sponsor groups.

For specific details about sponsor users and sponsor groups, see the [Cisco Identity Services Engine Sponsor Portal User Guide, Release 1.1.x](#).

**To create a new network access user or sponsor user, complete the following steps:**

---

- Step 1** Choose **Administration > Identity Management > Identities > Users**.
- The Network Access Users page appears listing all locally configured network access users.
- Step 2** Click **Add (+)** to create a new network access user.
- The Network Access User page appears.
- Step 3** Enter values for the following Network Access User fields (for details, see Network Access Users in [Table 4-2 on page 4-7](#)).
- Network Access User and Status



**Note** Do not include spaces in network access user names.

---

- Password
- User Information
- Account Options
- User Groups



**Note** You can change the order in which the user groups are listed, and the order is obeyed once it is saved. Be advised that the visual display reverts to alphabetical order, even though the user groups are processed in the newly specified order.

---

- Step 4** Click **Submit** to create a new network access user or sponsor user in the Cisco ISE database.
- 

### Modifying an Existing Network Access User

Use this procedure to modify the configuration values for an existing locally configured network access user.

**To modify an existing network access user, complete the following steps:**

---

- Step 1** Choose **Administration > Identity Management > Identities > Users**.
- The Network Access Users page appears listing all locally configured network access users.

**Step 2** Check the check box that corresponds to the network access user that you want to modify, and click **Edit**. The corresponding Network Access User page appears.

**Step 3** Modify the values in the Network Access User fields that you want to change.

- Network Access User and Status
- Password
- User Information
- Account Options
- User Groups



**Note** You can change the order in which the user groups are listed, and the order is obeyed once it is saved. Be advised that the visual display reverts to alphabetical order, even though the user groups are processed in the newly specified order.

**Step 4** Click **Save** to save your modified network access user in the Cisco ISE database.

---

### Deleting an Existing Network Access User

Use this procedure to delete an existing locally configured network access user.

**To delete an existing network access user, complete the following steps:**

---

**Step 1** Choose **Administration > Identity Management > Identities > Users**.

The Network Access Users page appears listing all locally configured network access users.

**Step 2** Check the check box that corresponds to the network access user that you want to delete.

**Step 3** Click **Delete** to delete the network access user you selected.

**Step 4** Click **OK** in the confirmation dialog to confirm that you want to delete this network access user. The Network Access User page appears with the modified status.

---

### Changing the Status of an Existing Network Access User

Use this procedure to change the status of an existing locally configured network access user.

**To change the status of an existing network access user, complete the following steps:**

---

**Step 1** Choose **Administration > Identity Management > Identities > Users**.

The Network Access Users page appears listing all locally configured network access users.

**Step 2** Check the check box that corresponds to the network access user whose status you want to change, and choose **Change Status > Change Status of Selected**.

The Network Access User page appears with the modified status.

---

## Importing or Exporting Existing Network Access Users

Use the following procedures to import or export locally configured network access users.

### To import existing network access users, complete the following steps:

---

**Step 1** Choose **Administration > Identity Management > Identities > Users**.

The Network Access Users page appears listing all locally configured network access users.

**Step 2** Click **Import** to import network access users from a comma-delimited text file.

The Import Users from File page appears.

- In the File text box, enter the filename containing the network access users to import, or click **Browse** and navigate to the location where the file resides.
- Check the **Create new user(s) and update existing user(s) with new data** check boxes if you want to both create new network access users and update existing network access users.



---

**Note** If this check box option is not selected during the import process, only a new user (or users) is created and existing users are not affected by any updates.

---

**Step 3** (Optional) If you do not have a comma-delimited text file, click **Generate a Template** to create this type of file, which includes the following data fields:

- User Name
- First Name
- Last Name
- E-mail
- User Details
- Password
- Is Password Encrypted True/False
- Enable User Yes/No

**Step 4** (Optional) Click **Go Back** to return to the previous window if you decide not to perform an import operation.

**Step 5** Click **Save** to save your changes to the Cisco ISE database.

Use this procedure to import locally configured network access users.

---

### To export existing network access users, complete the following steps:

---

**Step 1** Choose **Administration > Identity Management > Identities > Users**.

The Network Access Users page appears listing all locally configured network access users.

**Step 2** Check the check box that corresponds to the network access user(s) that you want to export.

**Step 3** Click **Export Selected**.

The Export Network Access User dialog is displayed, where you are required to enter a key for encrypting the password in the Key field.

**Step 4** Click **Start Export** to create a users.csv file with the network access user(s) that you selected to export. The Opening users.csv dialog box appears with two options to choose.

- a. Click the **Open with** radio button and choose the application to use to open the users.csv file from the drop-down list (the default is Microsoft Office Excel).

Click **Other** to display additional choices.

- b. Once you have made your choice, click the **Save File** radio button to save the users.csv file in the format you selected.



---

**Note** Check the **Do this automatically for files like this from now on** check box to standardize this process.

---

- c. Click **OK** to export the users.csv file containing the network access users you selected.
- 

### Duplicating an Existing Network Access User

Use this procedure to duplicate an existing network access user.

**To duplicate an existing network access user, complete the following steps:**

---

**Step 1** Choose **Administration > Identity Management > Identities > Users**.

The Network Access Users page appears listing all locally configured network access users.

**Step 2** Check the check box that corresponds to the network access user that you want to duplicate, and click **Duplicate**.

The Network Access Users page appears with the duplicated status.

**Step 3** Modify the duplicated network access user as necessary.

**Step 4** Click **Submit** to save this new network access user.

---

### Searching for Specific Attributes in an Existing Network Access User

Use this procedure to search for an existing network access user based on specific attributes.

**To search for an existing network access user using specific attributes, complete the following steps:**

---

**Step 1** Choose **Administration > Identity Management > Identities > Users**.

The Network Access Users page appears listing all locally configured network access users.

**Step 2** Click the Show drop-down list, and choose from one of the following options:

- Quick Filter (see Step 3)
- Advanced Filter (see Step 4)

**Step 3** To perform a Quick Filter, perform the following:

- a. Enter search criteria in one or more of the following attribute fields:
  - Status

- Name
- Description
- First Name
- Last Name
- User Identity Groups
- Admin

b. To filter, click **Go** in each field.

Network access user entries that match the specified attribute(s) are displayed in the Network Access Users page.

**Step 4** To perform an Advanced Filter, perform the following:

a. Create a matching rule in the Filter drop-down list by choosing one of the following options:

- **Admin**
- **Description**
- **First Name**
- **Last Name**
- **Name**
- **Status**
- **User Identity Groups**

b. In the second drop-down list, choose one of the following options:

- **Contains**
- **Does not contain**
- **Does not equal**
- **Ends with**
- **Is empty**
- **Is exactly (or equals)**
- **Is greater than**
- **Is greater than or equal to**
- **Is less than**
- **Is less than or equal to**
- **Is not empty**
- **Starts with**

c. In the text box, enter your desired search value.

d. Click **Go** to launch the filter process, or click plus (+) to add additional search criteria.

e. Click **Clear Filter** to reset the filter process.

---

# Endpoints

An endpoint is typically a network-capable device that connects to your network and uses the resources on your network through wired and wireless NADs and VPNs. Endpoints can be personal computers, laptops, IP phones, smart phones, gaming consoles, printers, and fax machines.

The MAC address of an endpoint, expressed in hexadecimal form, is always used to represent the endpoint on your network. An endpoint can be profiled statically when you create the endpoint by using its MAC address, and associating a profile to it along with an endpoint identity group in Cisco ISE.

When endpoints are discovered on your network, they can be profiled dynamically based on the configured endpoint profiling policies, and assigned to the matching endpoint identity groups depending on their profiles.

Endpoints page displays the list of all the endpoints and their associated profiles, MAC addresses, and the status of static assignment as true or false. When Cisco ISE updates endpoints in the Endpoints list page, you may not find associated endpoint profiles for some of the endpoints in the Administration ISE node as you buffer endpoint attributes data in the Policy Service nodes for a minute. This delays writing endpoint data to the Administration ISE node by one minute. The Administration ISE node may not have the most recent endpoint attributes collected for a minute, and after a minute, the endpoint attributes are updated in the Endpoints list page.

For more information, see [Global Setting for Endpoint Attribute Filter, page 18-15](#).

## Policy Assignment

If you do not have a matching profiling policy, you can assign an unknown profiling policy. The endpoint is therefore profiled as Unknown. The endpoint that does not match any profile is grouped within the Unknown identity group. The endpoint profiled to the Unknown profile requires that you create a profile with an attribute or a set of attributes collected for that endpoint.

## Identity Group Assignment

You can assign an endpoint to an identity group when you create an endpoint statically, or when you do not want to use the Create matching identity group option during evaluation of the endpoint profiling policy for an endpoint. If you do not choose the Static Group Assignment option, then the endpoint is automatically assigned to the matching identity group the next time during evaluation of the endpoint profiling policy.

## Static Assignment

You can change the assignment of an endpoint from static to dynamic or from dynamic to static on the Endpoints page. The Endpoints page displays the static assignment status of endpoints as true when an endpoint is created statically, or false when the Static Assignment check box is unchecked during editing an endpoint in the Endpoints page.

## Static Group Assignment

You can assign an endpoint to an identity group statically. In such cases, the profiling service does not change the identity group the next time during the policy evaluation for these endpoints, which are previously assigned dynamically to endpoint identity groups in Cisco ISE.

The following section describes the procedure on how to manage endpoints in Cisco ISE:

[Configuring Endpoints, page 4-17](#)

**Related Topics:**

[Endpoint Identity Groups](#), page 4-71

**Note**

---

For more information on endpoints and endpoint profiling in Cisco ISE networks, see [Chapter 18](#), “Configuring Endpoint Profiling Policies”.

---



## Configuring Endpoints

The Endpoints page allows you to display, configure, and manage endpoints on your network, which provides an option to filter endpoints. You can create an endpoint statically in the Endpoints page. The

This section describes the basic operations that allow you to manage an endpoint, an identity that accesses your network, and contains the following topics:

- [Filtering Endpoints, page 4-17](#)
- [Creating an Endpoint, page 4-19](#)
- [Editing an Endpoint, page 4-20](#)
- [Deleting an Endpoint, page 4-21](#)
- [Importing Endpoints, page 4-22](#)
- [Importing Endpoints from an LDAP Server, page 4-23](#)
- [Exporting Endpoints, page 4-26](#)

## Filtering Endpoints

You can use the Show drop-down list, or the filter icon to both invoke a quick filter and close it in the Endpoints page. A quick filter is a simple filter that you can use to filter endpoints in the Endpoints page. The quick filter filters endpoints based on field descriptions, such as the endpoint profile, MAC address, and the static status that is assigned to endpoints when they are created in the Endpoints page.

You can use the Show drop-down list to invoke an advanced filter. An advanced filter is a complex filter that you can preset for use later and retrieve, along with the filtering results, in the Endpoints page. The advanced filter filters endpoints based on a specific value associated with the field description. You can add or remove filters, as well as combine a set of filters into a single advanced filter.

You can use the Manage Preset Filters option, which lists all the preset filters. This option allows you to manage preset filters. Once you have created and saved a preset filter, you can choose a preset filter from the list of filtered results in the Endpoints page. You can also edit preset filters and remove them from the preset filters list.

**To filter endpoints in the Endpoints page, complete the following steps:**

---

**Step 1** Choose **Administration > Identity Management > Identities > Endpoints**.

The Endpoints page appears, which lists all the endpoints that are discovered on your network.

**Step 2** In the Endpoints page, click the Show drop-down list to choose the filter option.

Here, you can choose a Quick Filter, an Advanced Filter for filtering, or the Manage Preset Filters option, which allows you to manage preset filters for filtering. See [Table 4-3](#).

For more information, see the [To filter endpoints by using the Quick Filter option, complete the following steps](#), page 4-18 and the [“To filter endpoints by using the Advanced Filter option, complete the following steps:”](#) section on page 4-18.



**Note** To return to the endpoints list, choose **All** from the Show drop-down list to display all the endpoints without filtering.

---

#### To filter endpoints by using the Quick Filter option, complete the following steps:

A quick filter filters endpoints based on each field description in the Endpoints page. When you click inside any field, and as you enter the search criteria in the field, it refreshes the page with the results in the Endpoints page. If you clear the field, it displays the list of all the endpoints in the Endpoints page.

- 
- Step 1** To filter, click **Go** within each field to refresh the page with the results that are displayed in the Endpoints page.
  - Step 2** To clear the field, click **Clear** within each field.
- 

#### To filter endpoints by using the Advanced Filter option, complete the following steps:

An advanced filter enables you to filter endpoints by using variables that are more complex. It contains one or more filters that filter endpoints based on the values that match the field descriptions. A filter on a single row filters endpoints based on each field description and the value that you define in the filter. Multiple filters can be used to match the value(s) and filter endpoints by using any one or all of the filters within a single advanced filter.

- 
- Step 1** To choose the field description, click the drop-down arrow.
  - Step 2** To choose the operator, click the drop-down arrow.
  - Step 3** Enter the value for the field description that you selected.
  - Step 4** Click **Add Row** (plus [+] sign) to add a filter, or click **Remove Row** (minus [-] sign) to remove a filter.
  - Step 5** Choose **All** to match the value in each filter, or **Any** to match the value in any one of the filters.
  - Step 6** Click **Go** to start filtering.
  - Step 7** Click the **Save** icon to save the filter.

The Save a Preset Filter dialog appears. Enter a file name to save the filter, and click **Save**. Do not include spaces when creating the name for a preset filter. Click **Cancel** to clear the filter without saving the current filter.



**Note** Any preset filter that you create and save is browser-based only and is only accessible using the same browser type (preset filters are not saved in the Cisco ISE database). For example, any preset filter you create and save using a Firefox Version 3.6.x browser will not be accessible by a Microsoft Internet Explorer (IE8) browser (or vice versa).

- 
- Step 8** Click **Clear Filter** after filtering.
-

Table 4-3 describes the fields that allow you to filter endpoints in the Endpoints page.

**Table 4-3 Filtering Endpoints**

Filtering Method	Filtering Field	Filtering Field Description
Quick Filter	Endpoint Profile	This field enables you to filter endpoints by the name of the endpoint profile.
	MAC Address	This field enables you to filter endpoints by the MAC address of the endpoint.
	Static Assignment	This field enables you to filter endpoints by the endpoint static assignment status.
Advanced Filter	Choose the field description from the following: <ul style="list-style-type: none"> <li>Endpoint Profile</li> <li>MAC address</li> <li>Static Assignment</li> </ul>	Click the drop-down arrow to choose the field description.
	Operator	From the Operator field, click the drop-down arrow to choose an operator that can be used to filter endpoints.
	Value	From the Value field, choose the value for the field description that you selected against which the endpoints are filtered.

## Creating an Endpoint

You can create a new endpoint statically by using the MAC address of an endpoint in the Endpoints page. You have an option to choose an endpoint profiling policy, and an identity group in the Endpoints page for static assignment. Cisco ISE does not reassign the profiling policy and the identity group for statically assigned endpoints.

**To create an endpoint in the Endpoints page, complete the following steps:**

---

**Step 1** Choose **Administration > Identity Management > Identities > Endpoints**.

The Endpoints page appears.

**Step 2** From the Endpoints page, choose **Create**.

The New Endpoint page appears.

**Step 3** Modify the values in the New Endpoint page, as shown in [Table 4-4](#).

**Step 4** Click **Submit**.

The endpoint that you create appears in the Endpoints page.

**Step 5** Click **Cancel** to return to the Endpoints page.

Alternatively, you can click the **Endpoint List** link from the New Endpoint page to return to the Endpoints page.

---

Table 4-4 describes the fields that allow you to create an endpoint in the Endpoints page.

**Table 4-4** *Creating Endpoints*

Field Name	Description
MAC Address	Enter the MAC address in hexadecimal form (for example, nn:nn:nn:nn:nn:nn).  If you do not enter the MAC address in hexadecimal form, this field prompts you with the following message:  Invalid MAC address. Please enter MAC address as nn:nn:nn:nn:nn:nn
Policy Assignment	From the Policy Assignment field, click the drop-down arrow to view the predefined endpoint profiling policies that can be assigned.  Choose an endpoint profiling policy.
Identity Group Assignment	From the Identity Group Assignment field, click the drop-down arrow to view existing identity groups in the system.  Choose an identity group.

## Editing an Endpoint

You can only edit the endpoint profiling policy that is assigned to endpoints and the identity group while editing endpoints.

**To edit an endpoint in the Endpoints page, complete the following steps:**

---

**Step 1** Choose **Administration > Identity Management > Identities > Endpoints**.

The Endpoints page appears.

**Step 2** From the Endpoints page, choose an endpoint, and then choose **Edit**.

Here, you can edit the endpoint profiling policy and the identity group for the selected endpoint. The Attribute List displays the attributes captured for that selected endpoint when created.




---

**Note** Click **Delete** to delete an endpoint from the edit page, which removes the endpoint in the Endpoints page. Click **Yes** to delete the endpoint, or click **No** to return to the edit page from the dialog.

---

**Step 3** Modify the values in the edit page, as shown in Table 4-5.




---

**Note** You can only edit the endpoint profiling policy and the identity group for an endpoint.

---

**Step 4** Click **Submit**.

The endpoint that you edit appears in the Endpoints page.

**Step 5** Click **Cancel** to return to the Endpoints page.

Alternatively, you can click the **Endpoint List** link to return to the Endpoints page.

---

Table 4-5 describes the fields that allow you to edit an endpoint in the Endpoints page.

**Table 4-5** *Editing Endpoints*

Field Name	Description
MAC address	The MAC address of the selected endpoint is displayed in hexadecimal form.
Policy Assignment	From the Policy Assignment field, click the drop-down arrow to view the predefined endpoint profiling policies that can be assigned. Choose an endpoint profiling policy.
Static Assignment	To change the dynamic status that is assigned to the endpoint, check the <b>Static Assignment</b> check box.
Identity Group Assignment	From the Identity Group Assignment field, click the drop-down arrow to view existing identity groups in the system. Choose an identity group.
Static Group Assignment	To change a dynamic assignment of an endpoint identity group to static, check the <b>Static Group Assignment</b> check box. If the check box is not checked, then the endpoint identity group is dynamic as assigned by the profiler based on policy configuration.

## Deleting an Endpoint

You can delete all the endpoints or only the endpoints that you choose from the list in the Endpoints page. The Delete menu has two options: Delete All, which allows you to delete all the endpoints from the list in the Endpoints page, or Delete Selected, which allows you to delete endpoints that you choose from the list in the Endpoints page.

You can also delete an endpoint from the edit page of an endpoint.

**To delete an endpoint from the Endpoints page, complete the following steps:**

- 
- Step 1** Choose **Administration > Identity Management > Identities > Endpoints**.  
The Endpoints page appears.
  - Step 2** From the Endpoints page, choose **Delete**.  
The Delete Selected and Delete All options appear.
  - Step 3** From the Endpoints page, choose endpoints that you want to delete from the list.
  - Step 4** Choose **Delete Selected** or **Delete All**.  
A confirmation dialog appears. If endpoints are filtered in the Endpoints page, only those filtered endpoints are deleted from the Endpoints page when you are using the **Delete All** option.
  - Step 5** Click **OK** to delete endpoints or click **Cancel** to return to the Endpoints page.
-

## Importing Endpoints

You can import endpoints from a comma-separated values (CSV) file in which the list of endpoints appears with the MAC address and the endpoint profiling policy details separated by a comma. The CSV file contains a header row that has two columns that list the MAC address of endpoints in one column, and endpoint profiling policies assigned to those endpoints in the next column.

If the CSV file contains endpoints that have their MAC addresses, and their assigned endpoint profiling policy is the Unknown profile, then those endpoints are immediately reprofiled in Cisco ISE to the matching endpoint profiling policies. However, they are not statically assigned to the Unknown profile. If endpoints do not have profiles assigned to them in the CSV file, then they are assigned to the Unknown profile and reprofiled to the matching endpoint profiling policies.

For example, [Table 4-6](#) shows how Cisco ISE reprofiles Unknown profiles that match the Xerox\_Device profile during import. It also shows how Cisco ISE reprofiles an endpoint that is unassigned.

**Table 4-6** Unknown Profiles: Import From a File

MAC	Endpoint Profiling Policy Assigned Before Import in Cisco ISE	Endpoint Profiling Policy Assigned After Import in Cisco ISE
00:00:00:00:01:02	Unknown	Xerox-Device
00:00:00:00:01:03	Unknown	Xerox-Device
00:00:00:00:01:04	Unknown	Xerox-Device
00:00:00:00:01:05	If there is no profile assigned to an endpoint, then it is assigned to the Unknown profile, and also reprofiled to the matching profile.	Xerox-Device

If the CSV file contains endpoints that have their MAC addresses, and their assigned endpoint profiling policy is the static assignment, then they are not reprofiled during import. If endpoints are assigned to invalid profiles in the CSV file, then they are not imported because there are no matching profiles in Cisco ISE.

For example, [Table 4-7](#) shows how Cisco ISE retains the Cisco-Device profile, the static assignment of an endpoint during import. It also shows that endpoints are not imported when they are assigned to invalid profiles in the CSV file.

**Table 4-7** Static Assignment: Import From a File

MAC	Endpoint Profiling Policy Assigned Before Import in Cisco ISE	Endpoint Profiling Policy Assigned After Import in Cisco ISE
00:00:00:00:01:02	Cisco-Device	Cisco-Device
00:00:00:00:01:03	Unknown	Xerox-Device
00:00:00:00:01:04	Unknown	Xerox-Device
00:00:00:00:01:05	If an endpoint such as 00:00:00:00:01:05 is assigned to an invalid profile other than the profiles in Cisco ISE, then Cisco ISE displays a warning message that the policy name is invalid and the endpoint will not be imported.	The endpoint is not imported because there is no matching profile in Cisco ISE.

## Generating a Template

By default, you can use the Generate a Template link to create a CSV file in the Microsoft Office Excel application and save the file locally on your system. When you click the Generate a Template link, the Cisco ISE server displays the Opening template.csv dialog.

This dialog allows you to open the template.csv file, or save the template.csv file locally on your system. If you choose to open the template.csv file from the dialog, the file opens in the Microsoft Office Excel application. The file contains a header row that displays the MAC and Endpoint Policy columns.

Table 4-8 displays the header row in the template.csv file that is created by using the Generate a Template link:

**Table 4-8** CSV Template File

MAC	Endpoint Policy
00:1f:f3:4e:c1:8e	Cisco-Device

To import endpoints from a CSV file in the Endpoints page, complete the following steps:

---

**Step 1** Choose **Administration > Identity Management > Identities > Endpoints**.

The Endpoints page appears.

**Step 2** From the Endpoints page, choose **Import**.

**Step 3** From Import, choose **Import From File** and browse to locate the file that you have already exported from the Cisco ISE server.

The file format has to be in the format as specified so that the list of endpoints appears as follows: MAC, Endpoint Policy.

You can also use the Generate a Template link to create a template and save the file. When you use this link, a default template .csv file is created with the following values: 00:22:5e:4d:fe:01, Unknown. You must update the MAC address of endpoints and their profiles and save the file with a different file name. You can use this saved file for importing endpoints. The Microsoft Office Excel application is the default application to open the .csv files.




---

**Note** Format the file so that your list of endpoints appears as follows: MAC, Endpoint Policy. For example, 00:22:5e:4d:fe:01, Unknown.

---

**Step 4** Perform one of the following tasks:

- Click **Submit**, and the endpoints that are imported appear in the Endpoints page.
  - Click **Cancel** to return to the Endpoints page.
  - Click the **Endpoint List** link from the Import Endpoints page to return to the Endpoints page.
- 

## Importing Endpoints from an LDAP Server

### Prerequisite:

Before you import from an LDAP sever, ensure that you have installed the LDAP server.

To import endpoints from an LDAP server, complete the following tasks:

- 
- Step 1** Deploy the Cisco ISE for your network.
- Step 2** Start the LDAP server.
- Step 3** Configure the following connection settings:
- a. Choose **Administration > Identity Management > Identities > Endpoints > Import > Import From LDAP**.
  - b. Enter the value for the fields for the connection settings, as shown in [Table 4-9 on page 4-25](#).
    - Host
    - Port
    - Enable Secure Connection
    - Root CA Certificate Name
    - Anonymous Bind
    - Admin DN
    - Password
    - Base DN




---

**Note** You enable either the Anonymous Bind check box, or enter the LDAP administrator credentials from the slapd.conf configuration file.

---

- c. Enter the value for the fields for the query settings, as shown in [Table 4-9 on page 4-25](#).
    - MAC Address objectClass
    - MAC Address Attribute Name
    - Profile Attribute Name
    - Time Out
- 

The Lightweight Directory Access Protocol (LDAP) is an application protocol that uses an LDAP directory to query and import data from the LDAP directory. LDAP is an external identity store in Cisco ISE. A directory is a set of objects with attributes that are organized in a logical and hierarchical manner. It is a tree of directory entries that contains a set of attributes. An attribute has a name, and one or more values that are defined in the schema and stored in an LDAP Data Interchange Format (LDIF) file that you use to import the attribute.

Cisco ISE allows you to import MAC addresses and the associated profiles of endpoints securely from an LDAP server. You can use an LDAP server to import endpoints and the associated profiles, by using either the default port 389, or securely over SSL, by using the default port 636.

You have to configure the connection settings and query settings to import from an LDAP server. If the connection settings or query settings are configured incorrectly in Cisco ISE, then the “LDAP import failed:” error message appears.

#### Root CA Certificate Name

The root certificate authority (CA) certificate name refers to the trusted CA certificate that is required to connect to an LDAP server. You can add (import), edit, delete, and export trusted CA certificates.



## Configuring Importing of Endpoints from an LDAP server over SSL

You can import MAC addresses and the associated profiles of endpoints securely from an LDAP server.

To import endpoints from an LDAP server over SSL, complete the following steps:

- 
- Step 1** Choose **Administration > Identity Management > Identities > Endpoints**.  
The Endpoints page appears.
- Step 2** From the Endpoints page, choose **Import**.
- Step 3** From Import, choose **Import From LDAP**.
- Step 4** Modify the values in the Import Endpoints from LDAP page, as shown in [Table 4-9](#).
- Step 5** Perform one of the following tasks:
- Click **Submit** and the endpoints, which are imported from an LDAP server, appear in the Endpoints page.
  - Click **Cancel** to return to the Endpoints page.
  - Click the **Endpoint List** link from the Import Endpoints from LDAP page to return to the Endpoints page.
- 

[Table 4-9](#) describes the fields that allow you to import endpoints from an LDAP server in the Endpoints page.

**Table 4-9** *Importing from LDAP*

Field Name	Description
Host	Enter the hostname or the IP address of an LDAP server.
Port	Enter the port number of an LDAP server. You can use the default port 389 to import from an LDAP server, and the default port 636 to import from an LDAP server over SSL. <b>Note</b> Cisco ISE supports any configured port number. The configured value should match the LDAP server connection details.
Enable Secure Connection	To import from an LDAP server over SSL, check the <b>Enable Secure Connection</b> check box.
Root CA Certificate Name	Click the drop-down arrow to view the trusted CA certificates.
Anonymous Bind	To enable the anonymous bind, check the <b>Anonymous Bind</b> check box.
Admin DN	Enter the distinguished name (DN) configured for the LDAP administrator in the slapd.conf configuration file. Admin DN format example: cn=Admin, dc=cisco.com, dc=com
Password	Enter the password configured for the LDAP administrator in the slapd.conf configuration file.
Base DN	Enter the distinguished name of the parent entry. Base DN format example: dc=cisco.com, dc=com
MAC Address objectClass	Enter the query filter from the LDIF file, which is used for importing the MAC address, for example, ieee802Device.

**Table 4-9** *Importing from LDAP (continued)*

Field Name	Description
MAC Address Attribute Name	Enter the returned attribute name from the LDIF file, which you use for import. For example, macAddress.
Profile Attribute Name	<p>(Optional). Enter the name of the LDAP attribute. This attribute holds the policy name for each endpoint entry that is defined in the LDAP server.</p> <p>When you configure the Profile Attribute Name field, consider the following:</p> <ul style="list-style-type: none"> <li>• If you do not specify this LDAP attribute in the Profile Attribute Name field or configure this attribute incorrectly, then endpoints are marked “Unknown” during an import operation, and these endpoints are profiled separately to the matching endpoint profiling policies.</li> <li>• If you configure this LDAP attribute in the Profile Attribute Name field, the attribute values are validated to ensure that the endpoint policy matches with an existing policy in Cisco ISE, and endpoints are imported. If the endpoint policy does not match with an existing policy, then those endpoints will not be imported.</li> </ul>
Time Out [seconds]	Enter the time in seconds between 1 and 60 seconds.

## Exporting Endpoints

You can export selected or all the endpoints from the Cisco ISE server to different Cisco ISE servers.

**To export endpoints in the Endpoints page to a CSV file, do the following:**

- 
- Step 1** Choose **Administration > Identity Management > Identities > Endpoints**.  
The Endpoints page appears.
- Step 2** Choose one or more endpoints, and choose **Export**.  
The Export Selected and Export All options appear.
- Step 3** Choose an option to export selected endpoints, or export all the endpoints from the Endpoints list page. If endpoints are filtered in the Endpoints page, only those filtered endpoints are exported when you are using the **Export All** option.
- Step 4** Choose the **Open with** option.  
By default, the profiler\_endpoints.csv is a Microsoft Office Excel CSV file. For example, the Opening profiler\_endpoints.csv dialog box appears, which allows you to open or save the profiler\_endpoints.csv file. The Microsoft Office Excel application is the default application to open the .csv files.
- Step 5** From the Opening profiler\_endpoints.csv dialog box, click **OK**.  
The exported list of endpoints appears in the profiler\_endpoints.csv file, which opens in the Microsoft Office Excel application. The CSV file displays the header information in two separate columns such as the MAC address and Endpoint Policy. You can save this CSV file locally on your system, as well as use it for importing endpoints.

**Step 6** From the Opening profiler\_endpoints.csv dialog box, choose **Cancel** to return to the Endpoints page.

## Latest Network Scan Results

The most recent network scan results are stored in **Administration > Identity Management > Identities > Latest Network Scan Results**.

The Latest Network Scan Results Endpoints page displays only the most recent endpoints that are detected, along with their associated endpoint profiles, their MAC addresses, and their static assignment status, when you perform a manual network scan on any subnet. This page allows you to edit endpoints that are detected from the subnet for better classification, if required.

For more information on how to edit endpoints in the Latest Network Scan Results Endpoints page, see [Editing an Endpoint, page 4-20](#).

Cisco ISE allows you to perform the manual network scan from the Policy Service nodes that are enabled to run the profiling service. You must choose the Policy Service node from the primary Administration ISE node user interface in your deployment, and run the manual network scan from the Policy Service node. During the manual network scan on any subnet, the Network Scan probe detects endpoints on the specified subnet, their operating systems, and check UDP ports 161 and 162 for an SNMP service.

For more information on the manual network scan, see [Chapter 18, “Configuring the Network Scan \(NMAP\) Probe.”](#)


## Understanding Admin Access Terminology

[Table 4-10](#) defines and describes some basic admin access terminology that applies to role-based access policies, administrators, admin groups, permissions, and settings in Cisco ISE.

**Table 4-10** Cisco ISE Admin Access Terminology

Term	Description
Policies	Role-based access policies (known as Admin access) are access control policies that you define that allow you to restrict the network access privileges for any user or group. Role-based access policies are defined when you configure specific access control policies and permissions. These admin access policies allow you to customize the amount and type of access on a per-user or per-group basis using specified role-based access permission settings that apply to a group or an individual user.
Administrators	An individual who manages or performs a specific type of administrative task using the Cisco ISE user interface is considered an admin (or administrator). Administrators are dependent upon the admin role assigned to them, which limits the network access or tasks they can perform (a role-based access approach). Using the Cisco ISE user interface, administrator roles can perform the following tasks: <ul style="list-style-type: none"> <li>• Change admin or user passwords</li> <li>• Manage deployments, helpdesk operations, monitoring and troubleshooting nodes, and network devices</li> <li>• Manage Cisco ISE services policies and admin access, Cisco ISE administrator accounts and roles, Cisco ISE administrative functions, and Cisco ISE system configuration and operations</li> </ul>

Table 4-10 Cisco ISE Admin Access Terminology (continued)

Term	Description
Admin Groups	<p>These are groups that contain a number of users that all belong to the same administrative group. Each user that belongs to an administrative group is listed in the Member User table for that group, which includes information about each member, such as the name of the user, user status (Enabled or Disabled), e-mail address, First Name, and Last Name.</p> <p>Cisco ISE allows you to filter entries in a group, and add or remove entries from the Member User table. Applying role-based access information to groups directly maps these limits to any individual user who belongs to that group, because all group members share a common identity and the privileges assigned to that role (for example, users with the Network Device Admin role).</p> <p>A user's identity as a member of a specific administrative group can also be used as a condition in authorization policies. The supported Cisco ISE admin group roles and the tasks each role type can manage are listed and described in <a href="#">Table 4-11 on page 4-29</a>.</p>
Permissions	<p>Cisco ISE uses this process to control permissions or access rights to specific users or groups of users. Permissions allow you to control the ability of an individual user or group to access or manage any network service or resource. The Cisco ISE user interface provides two options: menu access and data access. Cisco ISE allows you to create, modify, duplicate, or delete permission privilege settings that limit access to Cisco ISE menus and Cisco ISE data.</p>
Settings	<p>Cisco ISE uses this process to configure three key settings that affect admin access:</p> <ul style="list-style-type: none"> <li>• Access</li> <li>• Password Policy</li> <li>• Session Timeout</li> </ul> <p>The Access settings allow you to configure access connection restrictions with two options (allow all IP addresses or allow only listed IP addresses). This option allows you to configure a list of IP addresses with a subnet mask that you configure for access. You can also edit or delete any IP addresses with a subnet mask in the configured list.</p> <p>The Password Policy settings consist of two tabs (Password Policy and Advanced) that you can use to create an admin access password policy. On the Password Policy tab, you can choose from eight check boxes and two text boxes to configure a password policy.</p> <p> <b>Note</b> Cisco ISE does not support administrator passwords with UTF-8 characters.</p> <p>On the Advanced tab, you can define a password history setting in a text field or use two check boxes and text fields to define the lifetime of an admin access password.</p> <p>The Session Timeout setting allows you to define a session idle timeout period in minutes. After this period elapses, the session times out and access is no longer possible during this session.</p>

Administrative users are users of Cisco ISE that can be assigned to one or more admin-level groups. You can create an administrative user when you first configure Cisco ISE users or you can promote an existing user to this role. Administrative users can also be demoted to simple network user status by disabling the corresponding administrative privileges.

**Note**

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

**Table 4-11 Cisco ISE Admin Group Roles and Responsibilities**

Admin Group Role	Description
Helpdesk Admin	<p>This role provides access for querying all monitoring and troubleshooting operations and within the Cisco ISE administrative console, and can perform the following tasks:</p> <ul style="list-style-type: none"> <li>• Run all reports</li> <li>• Run all troubleshooting flows</li> <li>• View the Cisco ISE dashboard and livelogs</li> <li>• View alarms</li> </ul> <p>This role cannot create, update, or delete reports, troubleshooting flows, live authentications, or alarms.</p>
Identity Admin	<p>This role provides access for managing all of the internal user identities that use the Cisco ISE administrative console across the Cisco ISE network. This role has read and write permissions on identities, endpoints, and identity groups (user identity groups and endpoint identity groups).</p>
Monitoring Admin	<p>This role provides access to all monitoring and troubleshooting operations within the Cisco ISE administrative console, and can perform the following tasks:</p> <ul style="list-style-type: none"> <li>• Manage all reports (run, create, and delete)</li> <li>• Run all troubleshooting flows</li> <li>• View the Cisco ISE dashboard and livelogs</li> <li>• Manage alarms (create, update, view, and delete)</li> </ul>
Network Device Admin	<p>This role provides access for Cisco ISE administrators that manage only the Cisco ISE network device repository and perform tasks such as adding, updating, or deleting devices. This role has the following permissions:</p> <ul style="list-style-type: none"> <li>• Read and write permissions on network devices</li> <li>• Read and write permissions on NDGs and all network resources object types</li> </ul>
Policy Admin	<p>This role provides access for Cisco ISE policy administrators who are responsible for creating and managing the policies for all Cisco ISE services across the network that are related to authentication, authorization, posture, profiler, and client provisioning. This role has the following permissions:</p> <ul style="list-style-type: none"> <li>• Read and write permissions on all the elements used in policies, such as authorization profiles, NDGs, and conditions</li> <li>• Read and write permissions on identities, endpoints, and identity groups (user identity groups and endpoint identity groups)</li> <li>• Read and write permissions on services policies</li> </ul>

Table 4-11 Cisco ISE Admin Group Roles and Responsibilities (continued)

Admin Group Role	Description
RBAC Admin	<p>This role provides 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. This role has the following permissions:</p> <ul style="list-style-type: none"> <li>• View the authentication details</li> <li>• Enable or disable endpoint protection service</li> <li>• Create, edit, and delete alarms; generate and view reports; and use Cisco ISE to troubleshoot problems in your network</li> <li>• Read permissions on administrator account settings and admin group settings</li> <li>• View permissions on admin access and data access permissions along with the RBAC policy page.</li> </ul>
Super Admin	<p>This role provides access to every Cisco ISE administrative function. This role is assigned to the default administrator account, and has create, read, update, delete, and eXecute (CRUDX) permissions on all Cisco ISE resources.</p> <p><b>Note</b> 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.</p>
System Admin	<p>This role provides access for Cisco ISE administrators who are responsible for Cisco ISE configuration and operations.</p> <p>This role provides 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. This role has the following permissions:</p> <ul style="list-style-type: none"> <li>• Read permissions on administrator account settings and administrator group settings</li> <li>• Read permissions on admin access and data access permissions along with the RBAC policy page.</li> <li>• Read and write permissions for all options under the Administration &gt; System menu.</li> <li>• View the authentication details</li> <li>• Enable or disable endpoint protection service</li> <li>• Create, edit, and delete alarms; generate and view reports; and use Cisco ISE to troubleshoot problems in your network</li> </ul>

## Managing Admin Access Types Using the User Interface

Use the Cisco ISE dashboard as your starting point for displaying and performing admin access management operations that allow you to manage policies, administrators, admin groups, permissions, and settings. You perform management operations by using the controls, tabs, and navigation pane options to perform the following tasks:

- Configure RBAC policies—Choose **Administration > System > Admin Access > Authorization > Policy**
- Configure administrators—Choose **Administration > System > Admin Access > Administrators > Admin Users**

- Configure admin groups—Choose **Administration > System > Admin Access > Administrators > Admin Groups**
- Configure permissions—Choose **Administration > System > Admin Access > Authorization > Permissions**
- Configure settings—Choose **Administration > System > Admin Access > Settings**

Table 4-12 lists the admin access types and configurable values you can set using the Admin Access tab.

**Table 4-12 Cisco ISE Admin Access Types and Values**

Tab: Sub Tab	User Interface Page Functions	Panel	Values
<b>Admin Access: Policies</b>			
<i>Your starting point for managing RBAC policies and values</i>	Create role-based admin access policies	RBAC	<ul style="list-style-type: none"> <li>• Rule</li> <li>• RBAC Groups</li> <li>• Permissions</li> </ul>
<b>Admin Access: Local Administrators</b>			
<i>Your starting point for managing Administrators</i>	<ul style="list-style-type: none"> <li>• Add</li> <li>• Edit</li> <li>• Change Status</li> <li>• Delete</li> <li>• Duplicate</li> <li>• Filter</li> </ul>	New Administrator (or Edit)	Admin User <ul style="list-style-type: none"> <li>• Name</li> <li>• E-mail</li> <li>• Status (Enabled or Disabled)</li> </ul> <hr/> Password <ul style="list-style-type: none"> <li>• Password*</li> <li>• Re-Enter Password*</li> </ul> <hr/> User Information <ul style="list-style-type: none"> <li>• First Name</li> <li>• Last Name</li> </ul> <hr/> Account Options <ul style="list-style-type: none"> <li>• Description</li> </ul> <hr/> Admin Groups

Table 4-12 Cisco ISE Admin Access Types and Values (continued)

Tab: Sub Tab	User Interface Page Functions	Panel	Values
<b>Admin Access: Admin Groups</b>			
<i>Your starting point for managing Admin Groups</i>	<ul style="list-style-type: none"> <li>Add</li> <li>Edit</li> <li>Duplicate</li> <li>Delete</li> <li>Filter</li> </ul>	Admin Groups	Admin Group <ul style="list-style-type: none"> <li>Name*</li> <li>Description</li> </ul> <hr/> Member User <ul style="list-style-type: none"> <li>Status</li> <li>E-mail</li> <li>Username</li> <li>First Name</li> <li>Last Name</li> </ul> <p><b>Note</b> In the Member Users page, you can add, remove, or search for member users having a specific attribute (or attributes) using either the Quick Filter or Advanced Filter search function.</p>
<b>Admin Access: Permissions</b>			
<i>Your starting point for managing Permissions</i>	Menu Access <ul style="list-style-type: none"> <li>Add</li> <li>Edit</li> <li>Duplicate</li> <li>Delete</li> </ul> Data Access <ul style="list-style-type: none"> <li>Add</li> <li>Edit</li> <li>Duplicate</li> <li>Delete</li> </ul>	Menu Access <hr/> Data Access	Create Menu Access Permission <ul style="list-style-type: none"> <li>Name*</li> <li>Description</li> </ul> <hr/> Menu Access Privileges <ul style="list-style-type: none"> <li>Show or Hide</li> <li>Menu Access Permission for:               <ul style="list-style-type: none"> <li>Operations</li> <li>Policy</li> <li>Administration</li> </ul> </li> </ul> <hr/> Create Data Access Permission <ul style="list-style-type: none"> <li>Name*</li> <li>Description</li> </ul> <hr/> Data Access Privileges <ul style="list-style-type: none"> <li>Full Access or No Access</li> <li>Data Access Permission for:               <ul style="list-style-type: none"> <li>Admin Groups</li> <li>User Identity Groups</li> <li>Endpoint Identity Groups</li> <li>All Locations</li> <li>All Device Types</li> </ul> </li> </ul>



Table 4-12 Cisco ISE Admin Access Types and Values (continued)

Tab: Sub Tab	User Interface Page Functions	Panel	Values
<b>Admin Access: Settings</b>			
<i>Your starting point for managing Settings</i>	Access	Configure Access Restriction	<ul style="list-style-type: none"> <li>Allow all IP addresses to connect</li> <li>Allow only listed IP addresses to connect</li> </ul>
		Configure IP List for Access Restriction	<ul style="list-style-type: none"> <li>Add</li> <li>Edit</li> <li>Delete</li> </ul>
	Password Policy	Password Policy tab	Password check boxes and text fields requirements: <ul style="list-style-type: none"> <li>Minimum length*</li> <li>Non-allowed characters or reverse order</li> <li>Lowercase alphabetic characters</li> <li>Uppercase alphabetic characters</li> <li>Numeric characters</li> <li>Non-numeric characters</li> </ul> <p><b>Note</b> Cisco ISE does not support administrator passwords with UTF-8 characters.</p>
		Advanced tab	<ul style="list-style-type: none"> <li>Password history setting</li> <li>Password lifetime settings               <ul style="list-style-type: none"> <li>Disable Account</li> <li>Disable Reminder</li> </ul> </li> </ul>
Session Timeout	Session Timeout tab	<ul style="list-style-type: none"> <li>Session Idle Timeout* (in minutes)</li> </ul>	

**Note**

Configurable values marked with an asterisk (\*) are required.

**For more information:**

- For more information about managing RBAC policies—See [Configuring RBAC Policies, page 4-57](#) and [Configuring RBAC Permissions, page 4-50](#).
- For more information about managing administrators—See [Configuring Cisco ISE Administrators, page 4-34](#) and [Administrator Access Settings, page 4-61](#).
- For more information about managing administrator Groups—See [Configuring Admin Groups, page 4-37](#).
- For more information about Configuring Cisco ISE to allow for administrator authentication using credentials that are stored on an external identity source—See [Configuring Cisco ISE for Administrator Access Using an External Identity Store, page 4-44](#).

- For more information about managing user identity groups—See [Configuring User Identity Groups, page 4-41](#).
- For more information about managing endpoint identity groups—See [Filtering, Creating, Editing, and Deleting Endpoint Identity Groups, page 4-73](#) and [Filtering, Creating, Editing, and Deleting Endpoint Identity Groups, page 4-73](#).

## Configuring Cisco ISE Administrators

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

This section contains the following topics:

- [Displaying Existing Cisco ISE Administrators, page 4-34](#)
- [Creating a New Cisco ISE Administrator, page 4-34](#)
- [Modifying an Existing Cisco ISE Administrator, page 4-35](#)
- [Deleting an Existing Cisco ISE Administrator, page 4-35](#)
- [Changing the Status of an Existing Cisco ISE Administrator, page 4-36](#)
- [Duplicating an Existing Cisco ISE Administrator, page 4-36](#)
- [Searching for Specific Attributes in an Existing Cisco ISE Administrator, page 4-36](#)

### Displaying Existing Cisco ISE Administrators

Cisco ISE displays administrators in the Administrators page, listing locally defined administrators in the following location:

**Administration > System > Admin Access > Administrators > Admin Users.**

### Creating a New Cisco ISE Administrator

Use this procedure to create a new Cisco ISE administrator.

**To create a new Cisco ISE administrator, complete the following steps:**

- 
- Step 1** Choose **Administration > System > Admin Access > Administrators > Admin Users**.  
The Administrators page appears, listing all existing locally defined administrators.
- Step 2** Click **Add**, and do 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 following Administrator fields (for details, see Administrators in [Table 4-12 on page 4-31](#)).
- Admin User and Status
  - Password (if you click the **External** option, the Password and Re-Enter Password fields are not used)

- User Information
- Account Options
- Admin Groups

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

---

### Modifying an Existing Cisco ISE Administrator

Use this procedure to modify an existing Cisco ISE administrator configuration.

**To modify an existing Cisco ISE administrator, complete the following steps:**

---

- Step 1** Choose **Administration > System > Admin Access > Administrators > Admin Users**.  
The Administrators page appears.
- Step 2** Check the check box that corresponds to the administrator that you want to modify, and click **Edit**.  
The corresponding Admin User page appears.
- Step 3** Modify the values in the following Admin User fields that you want to change.
- Admin User and Status
  - Password (if you click the **External** option, the Password and Re-Enter Password fields are not used)
  - User Information
  - Account Options
  - Admin Groups
- Step 4** Click **Save** to save the modified administrator in the Cisco ISE database.
- 

### Deleting an Existing Cisco ISE Administrator

Use this procedure to delete an existing Cisco ISE administrator.

**To delete an existing Cisco ISE administrator, complete the following steps:**

---

- Step 1** Choose **Administration > System > Admin Access > Administrators > Admin Users**.  
The Administrators page appears.
- Step 2** Check the check box that corresponds to the administrator that you want to delete, click **Delete**, and do one of the following:
- Click **Remove from Administrator List**. The selected Administrator is removed from the list.
    - This action removes the selected Administrator from the list, but does not delete the user account.
  - Click **Delete Admin User**, then click **OK**.
    - This action deletes the selected administrator from the Cisco ISE database.
-

### Changing the Status of an Existing Cisco ISE Administrator

Use this procedure to change the status of an existing Cisco ISE administrator.

**To change the status of an existing Cisco ISE administrator, complete the following steps:**

- 
- Step 1** Choose **Administration > System > Admin Access > Administrators > Admin Users**.  
The Administrators page appears.
- Step 2** Check the check box that corresponds to the administrator whose status you want to change, and click **Change Status**.
- Step 3** Click **OK** in the confirmation dialog box to change the status of the selected administrator.  
The Administrators page appears with this modified status.
- 

### Duplicating an Existing Cisco ISE Administrator

Use this procedure to duplicate an existing Cisco ISE administrator.

**To duplicate an existing Cisco ISE administrator, complete the following steps:**

- 
- Step 1** Choose **Administration > System > Admin Access > Administrators > Admin Users**.  
The Administrators page appears.
- Step 2** Check the check box that corresponds to the administrator who you want to duplicate, and click **Duplicate**.  
The Administrators page appears with the duplicated status.
- Step 3** Modify the duplicated administrator as necessary.
- Step 4** Click **Submit** to save this new administrator.
- 

### Searching for Specific Attributes in an Existing Cisco ISE Administrator

Use this procedure to search for an existing Cisco ISE administrator based on specific attributes.

**To search for an existing Cisco ISE administrator using specific attributes, complete the following steps:**

- 
- Step 1** Choose **Administration > System > Admin Access > Administrators > Admin Users**.  
The Administrators page appears.
- Step 2** Click the Show drop-down list, and choose one of the following options:
- Quick Filter (see Step 3)
  - Advanced Filter (see Step 4)
- Step 3** To perform a Quick Filter, perform the following:
- a. Enter search criteria in one or more of the following attribute fields:
    - Status
-

- Name
  - Description
  - First Name
  - Last Name
  - Admin Groups
- b. To filter, click **Go** in each field.
- Cisco ISE administrator entries that match the specified attribute(s) are displayed in the Cisco ISE Administrators page.

**Step 4** To perform an Advanced Filter, create a matching rule by performing the following:

- a. Choose one of the following options from the Filter drop-down list:
  - b. Choose one of the following options from the second drop-down list:
    - **Contains**
    - **Does not contain**
    - **Does not equal**
    - **Ends with**
    - **Is empty**
    - **Is exactly (or equals)**
    - **Is greater than**
    - **Is greater than or equal to**
    - **Is less than**
    - **Is less than or equal to**
    - **Is not empty**
    - **Starts with**
  - c. In the text box, enter your desired search value.
  - d. Click **Go** to launch the filter process, or click plus (+) to add additional search criteria.
  - e. Click **Clear Filter** to reset the filter process.
- 

## Configuring Admin Groups

The Admin Groups page lets you display, create, modify, delete, duplicate, or filter Cisco ISE network admin groups and this section contains the following topics:

- [Displaying Existing Admin Groups, page 4-38](#)
- [Creating an Admin Group, page 4-38](#)
- [Modifying an Existing Admin Group, page 4-39](#)
- [Deleting an Existing Admin Group, page 4-39](#)
- [Duplicating an Existing Admin Group, page 4-40](#)
- [Searching for Specific Attributes in an Existing Admin Group, page 4-40](#)

**Prerequisite**

To configure an external administrator group type, you must have already specified one or more external identity stores according to the guidelines that are found in these sections:

- [Microsoft Active Directory, page 5-4](#)
- [LDAP, page 5-18](#)
- [RADIUS Token Identity Sources, page 5-32](#)
- [RSA Identity Sources, page 5-39](#)

**Displaying Existing Admin Groups**


To display existing admin groups, choose **Administration > System > Admin Access > Administrators > Admin Groups**.

The Admin Groups page appears.

**Creating an Admin Group**

Use this procedure to create an admin group (and create or delete users within that admin group).

**To create an admin group, complete the following steps:**

- 
- Step 1** Choose **Administration > System > Admin Access > Administrators > Admin Groups**.  
The Admin Group page appears.
- Step 2** Click **Add**, and enter the values for the following Admin Group fields.
- Name
  - Description
- 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 specified 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.
- 
-  **Note** To configure an external administrator group type, you must have already specified one or more external identity stores according to the guidelines in the applicable sections of [Chapter 5, “Managing External Identity Sources.”](#)
- 
- Step 4** To add users to the Admin Group Users table, click **Add**. From the Users page, 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.
-

## Modifying an Existing Admin Group

Use this procedure to modify the configuration values for an existing locally configured admin group.

**To modify an existing admin group, complete the following steps:**

- 
- Step 1** Choose **Administration > System > Admin Access > Administrators > Admin Groups**.  
The Admin Group page appears.
- Step 2** Check the check box that corresponds to the admin group that you want to modify, and click **Edit**.  
The corresponding Admin Group page appears.
- Step 3** Modify the member users that are part of this admin group as follows:
- Click Add to add new member.
  - Check the check box corresponding to existing members, and click Remove to delete users.
  - Click Quick Filter or Advanced Filter and search on specific attributes for admin group users.
- Step 4** Click **Save** to save your modified network access user in the Cisco ISE database.
- 

## Deleting an Existing Admin Group

Use this procedure to delete an existing admin group (and by doing so, delete the users within that admin group).

**To delete an existing admin group, complete the following steps:**

- 
- Step 1** Choose **Administration > System > Admin Access > Administrators > Admin Groups**.  
The Admin Group page appears.
- Step 2** Check the check box that corresponds to the admin group that you want to delete, and click **Delete**.  
A Delete Confirmation dialog box appears.
- Step 3** Click **OK** to confirm the deletion of the selected admin group.
-

## Duplicating an Existing Admin Group

Use this procedure to duplicate an existing admin group.

**To duplicate an existing admin group, complete the following steps:**

- 
- Step 1** Choose **Administration > System > Admin Access > Administrators > Admin Groups**.  
The Admin Group page appears.
- Step 2** Check the check box that corresponds to the admin group you want to duplicate, and click **Duplicate**.  
The Admin Group window appears with the duplicated status.
- Step 3** Modify the duplicated admin group as necessary.
- Step 4** Click **Submit** to save this new admin group.
- 

## Searching for Specific Attributes in an Existing Admin Group

Use this procedure to search for an existing admin group based on specific attributes.

**To search for an existing admin group using specific attributes, complete the following steps:**

- 
- Step 1** Choose **Administration > System > Admin Access > Administrators > Admin Groups**.  
The Admin Group page appears.
- Step 2** Click the Show drop-down list, and select from one of the following options:
- **Quick Filter**
  - **Advanced Filter**
- Step 3** To perform a Quick Filter, perform the following:
- a. Enter search criteria in one or more of the following attribute fields:
    - Name
    - Description
  - b. To filter, click **Go** in each field.
- Step 4** To perform an Advanced Filter, create a matching rule by performing the following:
- a. Choose one of the following options from the **Filter** drop-down list:
    - **Description**
    - **Name**
  - b. Choose one of the following options from the second drop-down list:
    - **Contains**
    - **Does not contain**
    - **Does not equal**
    - **Ends with**
    - **Is empty**
    - **Is exactly (or equals)**



- Is greater than
  - Is greater than or equal to
  - Is less than
  - Is less than or equal to
  - Is not empty
  - Starts with
- c. In the text box, enter your desired search value.
  - d. Click **Go** to launch the filter process, or click plus (+) to add additional search criteria.
  - e. Click **Clear Filter** to reset the filter process.
- 

## Configuring User Identity Groups

The Identity Groups window lets you display, create, modify, delete, duplicate, or filter Cisco ISE user identity groups and this section contains the following topics:

- [Displaying a User Identity Group, page 4-41](#)
- [Creating a User Identity Group, page 4-41](#)
- [Modifying an Existing User Identity Group, page 4-42](#)
- [Deleting an Existing User Identity Group, page 4-42](#)
- [Importing or Exporting an Existing User Identity Group, page 4-43](#)
- [Searching for Specific Attributes in an Existing User Identity Group, page 4-43](#)

### Displaying a User Identity Group

To display a Cisco ISE user identity group, choose **Administration > Identity Management > Groups > Identity Groups > User Identity Groups**.

The User Identity Groups page appears.

### Creating a User Identity Group

Use this procedure to create a user identity group (and create or delete users within this local user identity group).

**To create a user identity group, complete the following steps:**

- 
- Step 1** Choose **Administration > Identity Management > Groups > Identity Groups > User Identity Groups**.  
The User Identity Group page appears.
  - Step 2** Click **Add**, and enter values in the following fields.
    - Name
    - Description



---

**Note** Do not include spaces when creating the name for a user identity group.

---

**Step 3** Click **Submit**.

---

### Modifying an Existing User Identity Group

Use this procedure to modify an existing user identity group (and by doing so, modify the users within this local user identity group).

**To modify an existing user identity group, complete the following steps:**

- 
- Step 1** Choose **Administration > Identity Management > Groups > Identity Groups > User Identity Groups**.
- Step 2** Check the check box corresponding to the user identity group that you want to modify, and click **Edit**.  
You can edit the name of the identity group, as well as add new or delete existing users in the user identity group. The User Identity Groups page appears that displays the identity group name and description, and the Member Users section.
- Step 3** To add users to the identity group, click **Add** in the Users page.  
The Users widget appears that contains the list of network access users.
- Step 4** Click users listed in the Users widget to add them to the user identity group.
- Step 5** To delete users from the identity group, check the check box corresponding to the user that you want to delete, and choose **Delete**.  
Delete Selected or Delete All options appear that allows you to delete selected users or all.  
A confirmation dialog box appears. Click **OK** to confirm.
- Step 6** Click **Save** to save any changes made to the user identity group in the Cisco ISE database.
- 

### Deleting an Existing User Identity Group

Use this procedure to delete an existing user identity group (and by doing so, delete the users within this local user identity group).

**To delete an existing user identity group, complete the following steps:**

- 
- Step 1** Choose **Administration > Identity Management > Groups > Identity Groups > User Identity Groups**.  
The User Identity Group page appears.
- Step 2** Check the check box next to the user identity group that you want to delete, and click **Delete**.  
A confirmation dialog box appears. Click **OK** to confirm your user identity group deletion.
-

## Importing or Exporting an Existing User Identity Group

Use this procedure to import or export locally configured user identity groups.

**To import or export existing user identity groups, complete the following steps:**

- 
- Step 1** Choose **Administration > Identity Management > Groups > Identity Groups > User Identity Groups**.
- The User Identity Group page appears.
- Step 2** Click **Import** to import network access users from a comma-delimited text file.
- The Import User Identity Groups from File page appears.
- In the File field, enter the filename that contains the user identity group that you want to import, or click **Browse** and navigate to the location where this file resides.
  - Check the **Overwrite existing data with new data** check box if you want to both add a new user identity group and update existing user identity groups.
  - If this check box option is not selected during the import process, only a new user identity group is created and existing user identity groups are not affected by any updates.
- Step 3** (Optional) If you do not have a comma-delimited text file, click **Generate a Template** to create this type of file, which includes the following fields:
- Identity Group Name
  - Identity Group Description
- Step 4** (Optional) Click **Go Back** to return to the previous page if you decide not to perform an import operation.
- Step 5** Click **Import**.
- Step 6** To export a user identity group, you must first check the check box that corresponds to the user identity group that you want to export, and click **Export**.
- The “Opening users.csv” window is displayed, and is where you can click **Save File** and click **OK** to create a users.csv file with the network access users that you selected to export.
- Step 7** Click **Save** to save your changes to the Cisco ISE database.
- 

## Searching for Specific Attributes in an Existing User Identity Group

Use this procedure to search for an existing user identity group based on specific attributes.

**To search for an existing user identity group using specific attributes, complete the following steps:**

- 
- Step 1** Choose **Administration > Identity Management > Groups > Identity Groups > User Identity Groups**.
- The User Identity Groups page appears.
- Step 2** Click the Show drop-down list, and choose one of the following options:
- Quick Filter
  - Advanced Filter
- a. To perform a Quick Filter, enter search criteria in one or more of the following attribute fields:

- **Name**
  - **Description**
  - b. To perform an Advanced Filter, create a matching rule by choosing one of the following options from the **Filter** drop-down list:
    - **Name**
    - **Description**
  - c. From the second drop-down list, choose one of the following options:
    - **Contains**
    - **Does not contain**
    - **Does not equal**
    - **Ends with**
    - **Is empty**
    - **Is exactly (or equals)**
    - **Is greater than**
    - **Is greater than or equal to**
    - **Is less than**
    - **Is less than or equal to**
    - **Is not empty**
    - **Starts with**
  - d. In the text box, enter your desired search value.
  - e. Click **Go** to launch the filter process, or click plus (+) to add additional search criteria.
  - f. Click **Clear Filter** to reset the filter process.
- 

## Configuring Cisco ISE for Administrator Access Using an External Identity Store

In Cisco ISE you can provide administrator user authentication via an external identity store like Active Directory, LDAP, or RSA SecureID. There are two models you can use to provide authentication via an external identity store:

- **External Authentication + External Authorization**—There are no credentials that are specified on the local Cisco ISE database for the administrator ID in question, and authorization is based on external identity store group membership only. This is used for Active Directory and LDAP authentication.
- **External Authentication + Internal Authorization**—There administrator’s authentication credentials come from the external identity source, and authorization and administrator role assignment takes place using the local Cisco ISE database. This 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 operation, Cisco ISE is designed to “fall back” and attempt to perform authentication from the internal identity database, if communication with the external identity store has not been established or if it fails. In addition, whenever an administrator for whom you have set up external authentication

launches a browser and initiates a login session, the administrator still has the option to request authentication via the Cisco ISE local database by choosing “Internal” from the **Identity Store** drop-down selector in the login dialog.

**Note**

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

**Prerequisites**

- 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. See the following sections for guidelines:
  - [Microsoft Active Directory, page 5-4](#)
  - [LDAP, page 5-18](#)
  - [RADIUS Token Identity Sources, page 5-32](#)
  - [RSA Identity Sources, page 5-39](#)

## External Authentication + External Authorization

By default, Cisco ISE is set up to provide internal administrator authentication. Therefore, 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. For more details on setting up the password policy, see [Configuring a Password Policy for Administrator Accounts, page 4-63](#).

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. If your external network access method requires a CAC, see [Configuring Cisco ISE for Administrator CAC Authentication, page 8-4](#).

**To create an external administrator authentication password policy, complete the following steps:**

- 
- Step 1** Navigate to **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 according to the [Prerequisites](#), which are outlined on page 4-44.
  - Step 3** Configure any other specific password policy settings according to the guidelines in [Configuring a Password Policy for Administrator Accounts, page 4-63](#).
  - Step 4** Click **Save**.
- 

Next, 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. For details, see [Creating an Admin Group, page 4-38](#).

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.

**To create an internal administrator group to which you will map the external Active Directory or LDAP identity group, complete the following steps:**

- 
- Step 1** Choose **Administration > System > Admin Access > Administrators > Admin Groups > Add**.  
The Admin Groups page appears.
- Step 2** Follow the guidelines that are described in [Creating an Admin Group, page 4-38](#) to create a new external administrator group.
- Step 3** Click **Save**.
-

**To specify menu access and data access permissions for the new external administrator group, complete the following steps:**

- 
- Step 1** From the Cisco ISE Administration dashboard, choose **Administration > System > Admin Access**.
- Step 2** From the Admin Access navigation pane, click to expand **Permissions** and then click the following:
- **Menu Access**
  - **Data Access**
- The Menu Access or Data Access page appears, listing all existing default and user-defined access permissions.
- Step 3** Specify access permissions according to the guidelines in [Configuring Menu Access Permissions, page 4-50](#) and [Configuring Data Access Permissions, page 4-54](#).
- Step 4** Click **Save**.
- 

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 *internal* administrator group with menu and data access permissions to manage administrator 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. See [Duplicating RBAC Policy, page 4-60](#) for details.

---

**To create a new RBAC policy for external administrator authentication:**

- 
- Step 1** From the Cisco ISE Administration dashboard, choose **Administration > System > Admin Access > Authorization > Policy**.
- The RBAC Policies page appears. This page contains a set of ready-to-use predefined policies for default admin groups.
- Step 2** Specify the necessary external administrator authentication RBAC policy elements (group, permissions, and so on.) according to the guidelines in [Creating Custom RBAC Policy, page 4-58](#).
- Step 3** Click **Save**.
- 

**Note**

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, as described in the subsections under [Configuring Cisco ISE Administrators, page 4-34](#).

---

Figure 4-1 shows an example of the login dialog that is presented to the administrator when an external identity store has been set up in Cisco ISE to provide authentication. Upon logging in, administrators see only the menu and data access items that are specified in the RBAC policy.

**Figure 4-1 Administrator Login—External Identity Store Available**



**Note**

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 Cisco ISE administrator user interface.

## External Authentication + Internal Authorization

When configuring 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 + External 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.

**To create a new Cisco ISE administrator that authenticates via the external identity store, complete the following steps:**

- 
- Step 1** Choose **Administration > System > Admin Access > Administrators > Admin Users**.  
The Administrators page appears, listing all existing locally defined administrators.
- Step 2** Follow the guidelines at [Creating a New Cisco ISE Administrator, page 4-34](#) to ensure that the administrator username in the external RSA identity store is also present in Cisco ISE. Be sure to click the **External** option under Password.



**Note**

Remember: 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**.

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

1. The administrator sends a 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**.

Figure 4-2 shows an example of the login dialog that is presented to the administrator when RSA SecurID is the external identity store. Upon logging in, the administrator sees only the menu and data access items that are specified in the RBAC policy.

**Figure 4-2** Administrator Login—RSA SecurID External Identity Store

Identity Services Engine

Username admin

Password .....

Identity Source RSA SecurID

Login

Remember username

[Problem logging in?](#)

© 2012 Cisco Systems, Inc. Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

CISCO

284620

## Managing Admin Access (RBAC) Policies

In Cisco ISE, RBAC policies are simple access control policies that use RBAC concepts to manage admin access. These RBAC policies are formulated to grant permissions to a set of administrators that belong to one or more admin group(s) that restrict or enable access to perform various administrative functions using the user interface menus and admin group data elements.

RBAC policies determine if an admin user 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 admin user based on the admin group by using effective RBAC policies. When admin users log into the Cisco ISE user interface, they can access menus and data that are based on the policies and permissions defined for the admin groups with which they are associated.

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.

### For more information:

- To understand admin access terminologies, see [Understanding Admin Access Terminology, page 4-27](#)
- To manage admin access types and values, see [Managing Admin Access Types Using the User Interface, page 4-30](#)
- For detailed procedures for creating RBAC permissions, see [Configuring RBAC Permissions, page 4-50](#).
- For detailed procedures for creating RBAC policies, see [Configuring RBAC Policies, page 4-57](#).

## Configuring RBAC Permissions

Cisco ISE provides an out of the box set of permissions that are associated with a set of predefined admin groups. Having pre-defined 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.

The following permissions are available in Cisco ISE:

- Menu Access—See [Configuring Menu Access Permissions, page 4-50](#) for more information.
- Data Access—See [Configuring Data Access Permissions, page 4-54](#) for more information.

## Configuring Menu Access Permissions

In Cisco ISE, the menu access permissions allow you to show or hide the menu items of the Cisco ISE administrative interface to an admin group. This feature lets you create permissions for the admin group so that you can restrict or enable access to an administrator belonging to that group at the menu level.

This section contains the following topics:

- [Viewing Predefined Menu Access Permissions, page 4-51](#)
- [Creating Custom Menu Access Permissions, page 4-52](#)

- [Updating Menu Access Permissions, page 4-53](#)
- [Duplicating Menu Access Permissions, page 4-53](#)
- [Deleting Menu Access Permissions, page 4-54](#)

## Viewing Predefined Menu Access Permissions

Cisco ISE provides a set of system defined menu access permissions that are already used in the default RBAC policies.

**To view the default menu access for an admin group, complete the following steps:**

- Step 1** From the Cisco ISE Administration dashboard, choose **Administration > System > Admin Access > Authorization > Permissions**.
- Step 2** In the Admin Access navigation pane, click the arrow next to Permissions, and click **Menu Access**. The Menu Access page appears listing all existing menu access permissions, both default and user-defined.

Table 4-13 lists the default menu access permissions.

**Table 4-13** Default Menu Access Permissions

Menu Access Name	RBAC Group	Permissible Set of Menu Items <sup>1</sup>
Super Admin Menu Access	Super Admin	<ul style="list-style-type: none"> <li>• Operations &gt; All menu items</li> <li>• Policy &gt; All menu items</li> <li>• Administration &gt; All menu items</li> </ul>
Policy Admin Menu Access	Policy Admin	<ul style="list-style-type: none"> <li>• Operations &gt; All menu items</li> <li>• Policy &gt; All menu items</li> <li>• Administration &gt; <ul style="list-style-type: none"> <li>– Identity Management &gt; All menu items</li> <li>– System &gt; Settings</li> </ul> </li> </ul>
Helpdesk Admin Menu Access	Helpdesk Admin	<ul style="list-style-type: none"> <li>• Operations &gt; All menu items</li> </ul>
Identity Admin Menu Access	Identity Admin	<ul style="list-style-type: none"> <li>• Operations &gt; All menu items</li> <li>• Administration &gt; <ul style="list-style-type: none"> <li>– Identity Management &gt; All menu items</li> </ul> </li> </ul>
Network Admin Menu Access	Network Device Admin	<ul style="list-style-type: none"> <li>• Operations &gt; All menu items</li> <li>• Administration &gt; <ul style="list-style-type: none"> <li>– Network Resources &gt; All menu items</li> </ul> </li> </ul>
System Admin Menu Access	System Admin	<ul style="list-style-type: none"> <li>• Operations &gt; Authentication, Alarms, Reports, and Troubleshoot</li> <li>• Administration &gt; <ul style="list-style-type: none"> <li>– System &gt; All menu items</li> </ul> </li> </ul>

Table 4-13 Default Menu Access Permissions (continued)

Menu Access Name	RBAC Group	Permissible Set of Menu Items <sup>1</sup>
RBAC Admin Menu Access	RBAC Admin	<ul style="list-style-type: none"> <li>• Operations &gt; All menu items</li> <li>• Administration &gt; <ul style="list-style-type: none"> <li>– Admin Access &gt; All menu items</li> </ul> </li> </ul>
MnT Admin Menu Access	MnT Admin	<ul style="list-style-type: none"> <li>• Operations &gt; All menu items</li> </ul>

1. 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.

## Creating Custom Menu Access Permissions

This section describes how you create custom menu access permissions.

To add a menu access permissions for an admin group, complete the following steps:

- 
- Step 1** From the Cisco ISE Administration dashboard, choose **Administration > System > Admin Access > Authorization > Permissions**.
- Step 2** In the Admin Access navigation pane, click the arrow next to Permissions, and click **Menu Access**. The Menu Access page appears listing all existing menu access permissions, both default and user-defined.
- Step 3** Click **Add**, and enter the following field values in the Create Menu Access Permission group box:
- Name—Enter the name of the menu access permissions.
  - Description—Enter a brief description of the menu access permissions.
- The Menu Access Privileges group box contains the following two sections:
- Cisco ISE Navigation Structure —Displays a list of selectable menu items in a tree structure starting from top-level menu items, such as Operations, Policy, and Administration.
  - Permissions for Menu Access—Contains Show and Hide radio buttons.
    - Show—Shows the selected menu items to the member of the admin group upon login to the Cisco ISE user interface.
    - Hide—Hides the selected menu items. By default, all menu items are hidden.
- Step 4** To create menu access permissions for a menu item, complete the following steps:
- 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 5** Click **Save**.
-

## Updating Menu Access Permissions

You can edit only the custom menu access permissions and not the predefined menu access permissions.

**To edit menu access permissions for an admin group, complete the following steps:**

- 
- Step 1** From the Cisco ISE Administration dashboard, choose **Administration > System > Admin Access > Authorization > Permissions**.
  - Step 2** In the Admin Access navigation pane, click the arrow next to Permissions, and click **Menu Access**.  
The Menu Access page appears listing all existing menu access permissions, both default and user-defined.
  - Step 3** Check the check box next to the menu access permissions that you want to update, and click **Edit**.  
The Edit Menu Access Permission page appears.
  - Step 4** Modify the description of the menu access permission.
    - Name
    - Description
  - Step 5** Do the following to add or remove menu items from the existing permissions:
    - To add a new menu item to the permissions, select the menu items from the Menu Access Privileges group box, and click the **Show** radio button.
    - To remove an existing menu item from the permissions, select the menu items from the Menu Access Privileges section, and click the **Hide** radio button.
  - Step 6** Click **Save** to save the menu access permissions.
- 

## Duplicating Menu Access Permissions

Duplicating menu access permissions is a process that reuses the same set of menu items that were used by the original menu access.

**To add a duplicate menu access permissions for an admin group, complete the following steps:**

- 
- Step 1** From the Cisco ISE Administration dashboard, choose **Administration > System > Admin Access > Authorization > Permissions**.
  - Step 2** In the Admin Access navigation pane, click the arrow next to Permissions, and click **Menu Access**.  
The Menu Access page appears listing all existing menu access permissions, both default and user-defined.
  - Step 3** Check the check box next to the menu access permissions that you want to duplicate, and click **Duplicate**.  
New menu access permissions are added to the list with the word “\_copy” affixed to the name of the selected permissions. For example, if you want to create a duplicate of *MnT Admin Menu Access*, the duplicate is created with the name of *MnT Admin Menu Access\_copy*.
  - Step 4** Modify the duplicate permissions as necessary.

- Step 5** Click **Save** to save the duplicate menu access permissions.
- 

## Deleting Menu Access Permissions

You can delete only the custom menu access permissions and not the predefined menu access permissions.

**To delete a menu access permissions for an admin group, complete the following steps:**

---

- Step 1** From the Cisco ISE Administration dashboard, choose **Administration > System > Admin Access > Authorization > Permissions**.
- Step 2** From the Admin Access navigation pane, click the arrow next to Permissions, and click **Menu Access**. The Menu Access page appears listing all existing menu access permissions, both default and user-defined.
- Step 3** Check the check box next to the menu access permissions that you want to delete, and click **Delete**.
- Step 4** Click **OK** in the confirmation dialog box to confirm that you want to delete the menu access permissions.
- 

## Configuring Data Access Permissions

In Cisco ISE, the data access permissions enable multiple administrators to have the data access permissions within the same user population. You can enable or restrict the use of data access permissions to one or more admin groups. This process allows autonomous delegated control to administrators of one admin group to reuse data access permissions of the chosen admin groups through selective association. Data access permissions range from full access to no access for viewing selected admin groups or the network device groups.

The section contains the following topics:

- [Viewing Predefined Data Access Permissions, page 4-54](#)
- [Creating Custom Data Access Permissions, page 4-55](#)
- [Updating Data Access Permissions, page 4-56](#)
- [Duplicating Data Access Permissions, page 4-56](#)
- [Deleting Data Access Permissions, page 4-57](#)

## Viewing Predefined Data Access Permissions

**To view data access permissions, complete the following steps:**

---

- Step 1** From the Cisco ISE Administration dashboard, choose **Administration > System > Admin Access > Authorization > Permissions**.
- Step 2** In the Admin Access navigation pane, click the arrow next to Permissions, and click **Data Access**. The Data Access page appears listing all existing data access permissions, both default and user-defined. [Table 4-14](#) lists the default data access permissions.

**Table 4-14** Default Data Access Permissions

Data Access Name	RBAC Group	Permissible Admin Groups	Permissible Network Device Groups
Super Admin Data Access	Super Admin	<ul style="list-style-type: none"> <li>Admin Groups</li> <li>User Identity Groups</li> <li>Endpoint Identity Groups</li> </ul>	<ul style="list-style-type: none"> <li>All Locations</li> <li>All Device Types</li> </ul>
Policy Admin Data Access	Policy Admin	<ul style="list-style-type: none"> <li>User Identity Groups</li> <li>Endpoint Identity Groups</li> </ul>	None
Identity Admin Data Access	Identity Admin	<ul style="list-style-type: none"> <li>User Identity Groups</li> <li>Endpoint Identity Groups</li> </ul>	None
Network Admin Data Access	Network Device Admin	None	<ul style="list-style-type: none"> <li>All Locations</li> <li>All Device Types</li> </ul>
System Admin Data Access	System Admin	<ul style="list-style-type: none"> <li>Admin Groups</li> </ul>	None
RBAC Admin Data Access	RBAC Admin	<ul style="list-style-type: none"> <li>Admin Groups</li> </ul>	None

## Creating Custom Data Access Permissions

This section describes how you can create custom data access permissions.

**To create custom data access permissions, complete the following steps:**

- 
- Step 1** From the Cisco ISE Administration dashboard, choose **Administration > System > Admin Access > Authorization > Permissions**.
- Step 2** In the Admin Access navigation pane, click the arrow next to Permissions, and click **Data Access**. The Data Access page appears listing all existing data access permissions, both default and user-defined.
- Step 3** Click **Add**, and then enter the following field values in the Create Data Access permission page:
- Name—Enter the name of the data access permissions.
  - Description—Enter a brief description of the data access permissions.
- The Data Access Privileges group box contains the following two sections:
- Hierarchy list that contains admin groups, user identity groups, and endpoint identity groups.
  - Permissions for Data Access, such as Full Access and No Access. By default, all groups are shown in No Access mode.
- Step 4** To create a data access permissions that provide full access to an admin group, do the following:
- Click to expand the admin group and select the desired admin group.
  - Click **Full Access**.
- Step 5** Click **Save**.
- This creates the required data access permissions.
-

## Updating Data Access Permissions

You can edit only the custom data access permissions and not the predefined data access permissions.

**To update a data access permissions, complete the following steps:**

- 
- Step 1** From the Cisco ISE Administration dashboard, choose **Administration > System > Admin Access > Authorization > Permissions**.
- Step 2** In the Admin Access navigation pane, click the arrow next to Permissions, and click **Data Access**.  
The Data Access page appears listing all existing data access permissions, both default and user-defined.
- Step 3** Click **Edit**, and modify the following values in the Edit Data Access Permission page:
- Name
  - Description
- Step 4** Complete the following steps to add or remove admin groups from the existing permissions:
- To add a new admin group to the permissions, select the group from the Admin Group Hierarchy, and click the **Full Access** radio button.
  - To remove an existing admin group from the permissions, select the admin group from the Admin Group, and click **No Access**.
- Step 5** Click **Save** to save the data access permissions.
- 

## Duplicating Data Access Permissions

Duplicating data access permissions is a process that reuses the same set of admin groups as the original data access is having.

**To add a duplicate data access permissions for an admin group, complete the following steps:**

- 
- Step 1** From the Cisco ISE Administration dashboard, choose **Administration > System > Admin Access > Authorization > Permissions**.
- Step 2** In the Admin Access navigation pane, click the arrow next to Permissions, and click **Data Access**.  
The Data Access page appears listing all existing data access permissions, both default and user-defined.
- Step 3** Check the check box next to the data access permissions that you want to duplicate, and click **Duplicate**.  
New data access permissions are added to the list with the word “\_copy” affixed to the name of the selected permission. For example, if you want to create a duplicate of *Policy Admin Data Access*, the duplicate will be created with the name *Policy Admin Data Access\_copy*.
- Step 4** Modify the duplicate permissions as necessary.
- Step 5** Click **Save** to save the duplicate data access permissions.
-



## Deleting Data Access Permissions

You can delete only the custom data access permissions and not the predefined data access permissions.

**To delete a data access permissions for an admin group, complete the following steps:**

- 
- Step 1** From the Cisco ISE Administration dashboard, choose **Administration > System > Admin Access > Authorization > Permissions**.
  - Step 2** In the Admin Access navigation pane, click the arrow next to Permissions, and click **Data Access**. The Data Access page appears listing all existing data access permissions, both default and user-defined.
  - Step 3** Check the check box next to the data access permissions that you want to delete, and click **Delete**.
  - Step 4** Click **OK** in the confirmation dialog box to confirm that you want to delete the data access permissions.
- 

## Configuring RBAC Policies

In Cisco ISE, an RBAC policy is represented in an *if-then* format, where *if* is the RBAC Admin Group value and *then* is the RBAC Permissions value.

From the Cisco ISE Administration dashboard, choose **Administration > System > Admin Access > Authorization > Policy**, which displays all default RBAC policies. These default policies cannot be modified or deleted. This page also provides the interfaces to create custom RBAC policies for an admin group.

The following topics provide procedures for performing these tasks:

- [Using Predefined RBAC Policies, page 4-57](#)
- [Creating Custom RBAC Policy, page 4-58](#)
- [Updating RBAC Policy, page 4-60](#)
- [Duplicating RBAC Policy, page 4-60](#)
- [Deleting RBAC Policy, page 4-61](#)

## Using Predefined RBAC Policies

Cisco ISE provides a set of system-defined RBAC policies to perform various Cisco ISE administrative functions. You can use these policies as is unless you plan for more granular access policies.

**To create a custom RBAC policy, complete the following:**

From the Cisco ISE Administration dashboard, choose **Administration > System > Admin Access > Authorization > Policy**.

The RBAC Policies page appears. This page contains a set of ready-to-use predefined policies for default admin groups.

[Table 4-15](#) lists the predefined policies, the associated admin groups, and the permissions.

Table 4-15 Predefined RBAC Policies

Policy Name	RBAC Group <sup>1</sup>	Permissions (Menu Access and/or Data Access) <sup>2</sup>
Helpdesk Admin Policy	Helpdesk Admin	<ul style="list-style-type: none"> <li>Helpdesk Admin Menu Access</li> </ul>
Identity Admin Policy	Identity Admin	<ul style="list-style-type: none"> <li>Identity Admin Menu Access</li> <li>Identity Admin Data Access</li> </ul>
MnT Admin Policy	MnT Admin	<ul style="list-style-type: none"> <li>MnT Admin Menu Access</li> </ul>
Network Device Policy	Network Device Admin	<ul style="list-style-type: none"> <li>Network Device Menu Access</li> <li>Network Device Data Access</li> </ul>
Policy Admin Policy	Policy Admin	<ul style="list-style-type: none"> <li>Policy Admin Menu Access</li> <li>Policy Admin Data Access</li> </ul>
RBAC Admin Policy	RBAC Admin	<ul style="list-style-type: none"> <li>RBAC Admin Menu Access</li> <li>RBAC Admin Data Access</li> </ul>
Super Admin Policy	Super Admin	<ul style="list-style-type: none"> <li>Super Admin Menu Access</li> <li>Super Admin Data Access</li> </ul>
System Admin Policy	System Admin	<ul style="list-style-type: none"> <li>System Admin Menu Access</li> <li>System Admin Data Access</li> </ul>

1. See [Understanding Admin Access Terminology, page 4-27](#), for more information on the default admin groups.
2. See [Table 4-13](#) for the list of predefined menu access permissions and [Table 4-14](#) for the list of predefined data access permissions.

## Creating Custom RBAC Policy

Besides the default policies, you can create custom RBAC policies specifically for your work place, and apply to personalized admin groups.

### Prerequisites:

- Ensure that you have created all admin groups for which you want to define the RBAC policies. See [Configuring Admin Groups, page 4-37](#), for more information on how to create admin groups.
- Ensure that these admin groups are mapped to the individual admin users. See [Configuring Cisco ISE Administrators, page 4-34](#), for more information on how to create admin users.
- Ensure that you have configured the RBAC permissions, such as menu access and data access permissions. See [Configuring RBAC Permissions, page 4-50](#), for more information on how to create RBAC permissions.

To create a custom RBAC policy, complete the following steps:

- 
- Step 1** From the Cisco ISE Administration dashboard, choose **Administration > System > Admin Access > Authorization > Policy**.
- The RBAC Policies page appears. This page contains a set of ready-to-use predefined policies for default admin groups.
- Step 2** Click **Actions** next to the RBAC policy rule in the RBAC Policies page.
- Here, you can insert new RBAC policies, duplicate an existing RBAC policy, and delete an existing RBAC policy in the RBAC Policies page.

Table 4-16 lists the RBAC policy object selector options.

**Table 4-16 RBAC Policy Object Selector Options**

Action Name	Result
Duplicate	Adds a copy of the selected policy in the PBAC policies page, along with the word copy in the RBAC policy name. Save the policy with an appropriate name.
Insert New Policy	Adds a new policy row.
Delete	Deletes the selected policy. This option is disabled for default policies.

**Step 3** Click the appropriate action from the drop-down menu.

RBAC policies appear in an alphabetical order according to their rule names after you save the RBAC policy in the RBAC Policies page.

**Step 4** Enter values for the following RBAC policy fields:

- Rule Name—Enter a name for the new policy.
- RBAC Group(s)—Choose a name for the RBAC group that is associated with the policy.
  - Click the plus sign (+) next to RBAC Groups to display a drop-down list of group choices. This list shows all existing RBAC groups, including the default groups and user-defined internal and external groups.
  - Click the plus sign (+) next to RBAC Groups to add multiple RBAC groups.
- Permissions—Choose the permissions, which include menu access and data access permissions.
 

To add permissions:

  - Click the plus sign (+) next to Permissions to enter the menu access permissions name.
  - Click the button next to Enter Menu Access Permission to display a drop-down list of menu access permission choices.
  - Click the necessary Menu Access Permission in the list to add it to the policy.
  - Click the plus sign (+) next to the selected Menu Access Permission name to add data access permissions.
  - Click the button next to Enter Data Access Permission to display a drop-down list of data access permission choices.
  - Click the necessary Data Access Permission in the list to add it to the policy.



**Note** You cannot select multiple menu access and data access permissions when creating an RBAC policy.

- Click **Submit**.

The RBAC policy creation is now complete.

## Updating RBAC Policy

In the Cisco ISE Administration dashboard, there is no specific button or control available to edit a policy. You can update only the custom RBAC policies and not the default RBAC policies. You can update all or any RBAC Policy fields by modifying the field values that you want to change.

**To edit a custom RBAC policy, complete the following steps:**

- 
- Step 1** From the Cisco ISE Administration dashboard, choose **Administration > System > Admin Access > Authorization > Policy**.
- The RBAC Policies page appears.
- Step 2** Modify the values of following fields, as necessary:
- Rule Name
  - RBAC Group
  - Permissions
    - Menu Access Permission
    - Data Access Permission
- Step 3** Click **Save** to save the modified RBAC Policy.
- 

## Duplicating RBAC Policy

Use this procedure to add a duplicate RBAC policy.

**To duplicate a policy, complete the following steps:**

- 
- Step 1** From the Cisco ISE Administration dashboard, choose **Administration > System > Admin Access > Authorization > Policy**.
- The RBAC Policies page appears.
- Step 2** Click **Actions** next to the RBAC policy rule in the RBAC Policies page.
- Step 3** Click **Duplicate**.
- A duplicate policy row is added in the desired location with the word “\_copy” affixed to the selected policy name.
- Step 4** Modify values of the policy fields, as necessary.
- Step 5** Click **Save** to save the duplicate policy.
-

## Deleting RBAC Policy

You can delete only the custom RBAC policies and not the default RBAC policies.

**To delete a policy, complete the following steps:**

- 
- Step 1** From the Cisco ISE Administration dashboard, choose **Administration > System > Admin Access > Authorization > Policy**.
- The RBAC Policies page appears.
- Step 2** Click **Actions** next to the RBAC policy rule in the RBAC Policies page.
- Step 3** Click **Delete**.
- Step 4** Click **Save** to delete the policy from the Cisco ISE database.
- 

# Configuring Settings for Accounts

This section describes how to configure general settings for different Cisco ISE accounts and contains the following topics:

- [Administrator Access Settings, page 4-61](#)
- [Configuring Network Access for User Accounts, page 4-66](#)

## 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.



---

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

---

This section describes how to define rules for administrator accounts:

- [Restricting Administrative Access to the Management Interfaces, page 4-62](#)
- [Configuring a Password Policy for Administrator Accounts, page 4-63](#)
- [Configuring Session Timeout for Administrators, page 4-65](#)

**For more information:**

Refer to the *Cisco Identity Services Engine Hardware Installation Guide, Release 1.1.x* for a list of ports that must be open for specific services.

The username and password that you configure using Setup is intended only for administrative access to the Cisco ISE command-line interface (CLI), and this role is considered to be the CLI-admin user. By default, the username for the CLI-admin user is “admin” and the password is user-defined during Setup (there is no default password).

As the CLI-admin user, you 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 of the CLI-admin user, we recommend that you protect the CLI-admin user credentials and create web-based admin users for configuring and managing your Cisco ISE deployment.

**For more information:**

- For information about web-based admin users, see the [“Configuring Cisco ISE Administrators” section on page 4-34](#).
- For details about the differences between the CLI-admin users and web-based admin users, refer to the [Cisco Identity Services Engine Hardware Installation Guide, Release 1.1.x](#).

## Restricting Administrative Access to the Management Interfaces

Cisco ISE allows you to restrict administrative access to the management interfaces based on the IP address of the remote client. You can choose to do one of the following:

- Allow all IP addresses to connect
- Allow only listed IP addresses to connect

If you choose the Allow only listed IP addresses to connect option, you must add a list of IP addresses.



**Note**

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

**Prerequisite:**

Every Cisco ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have any one of the following roles assigned: Super Admin or System Admin. See [Table 4-11](#) for more information on the various administrative roles and the privileges associated with each of them.

**To add a range of IP addresses to the IP List area, complete the following steps:**

- 
- Step 1** Choose **Administration > System > Admin Access > Settings > Access**.
- The Configure Access Restriction page appears.
- Step 2** Do one of the following:
- Click the **Allow all IP addresses to connect** radio button and proceed to [Step 4](#).
  - Click the **Allow only listed IP addresses to connect** radio button, and complete the following steps:
    - a. From the Configure IP List for Access Restriction area, click **Add**.  
The Add IP CIDR page appears.
    - b. Enter IP addresses in the classless interdomain routing (CIDR) format in the IP address field.  
Enter the subnet mask in the Netmask in CIDR format field.
    - c. Click **OK** to add the range of IP addresses to the IP List area.
    - d. Repeat the process to add more IP address ranges to this list.

Administrative access to Cisco ISE will now be restricted to the IP address ranges that are specified in this list after you click Submit.

**Step 3** Click **Submit** to save the changes.

---

#### Related Topics

- [Configuring Cisco ISE Administrators, page 4-34](#)
- [Configuring Admin Groups, page 4-37](#)

## Configuring a Password Policy for Administrator Accounts

You can create a password policy for administrator accounts to enhance security. The 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.

---

#### Prerequisite:

Every Cisco ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have any one of the following roles assigned: RBAC Admin, Super Admin, or System Admin. See [Table 4-11](#) for more information on the various administrative roles and the privileges that are associated with each of them.

## Specifying Password-Based or Client Certificate-Based Authentication

**To enable either password-based or client certificate-based administrator authentication:**

---

**Step 1** Navigate to **Administration > System > Admin Access > Authentication**.

**Step 2** On the Authentication Method tab, select either the **Password Based** or the **Client Certificate Based** option.

- 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. The default setting is “Internal.”

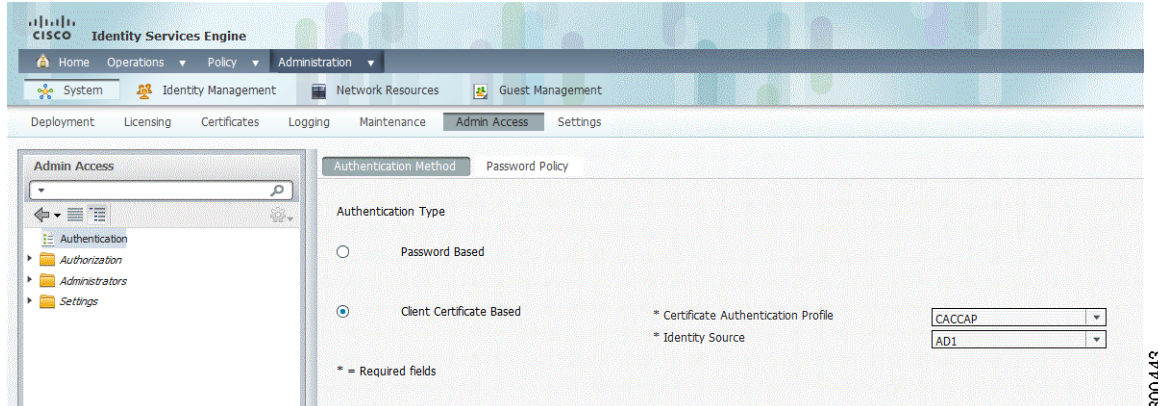


**Note** If you have configured an external identity source such as LDAP and want to use that as your authentication source to grant access to the admin user, you must select that particular identity source from the Identity Source list box.

---

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

Figure 4-3 Administrator &gt; System &gt; Admin Access &gt; Authentication &gt; Authentication Method



## Specifying the Administrator Password Policy

To create the password policy for administrators, complete the following steps:

- Step 1** Choose **Administration > System > Admin Access > Authentication**.
- Step 2** Click the **Password Policy** tab.
- Step 3** On the Password Policy tab, enter the following information:



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

- **Minimum Length—(Required)** Specifies the minimum length of the password (in characters). The default is six characters.
- **Password should not contain the admin name or its characters in reversed order**—Check this check box to restrict the use of the administrator username or its characters in reverse order.
- **Password should not contain ‘cisco’ or its characters in reversed order**—Check this check box to restrict the use of the word “cisco” or its characters in reverse order.
- **Password should not contain *variable* or its characters in reversed order**—Check this check box to restrict the use of any word that you define or these characters in reverse order.
- **Password should not contain repeated characters four or more times consecutively**—Check this check box to restrict the use of repeated characters four or more times consecutively.
- **Password must contain at least one character of each of the selected types**—Specifies that the administrator password must contain at least one character of the type that you choose from the following choices:
  - Lowercase alphabetic characters
  - Uppercase alphabetic characters
  - Numeric characters
  - Non-alphanumeric characters



- Password History—Specifies the number of previous passwords from which the new password must be different to prevent the repeated use of the same password.
- Password Lifetime—Specifies the following options to force users to change passwords after a specified time period:
  - Time (in days) before the administrator account is disabled if the password is not changed. (The allowable range is 0 to 2,147,483,647 days.)
  - Reminder (in days) before the administrator account is disabled.
- Incorrect Password Attempts—Specifies the number of times Cisco ISE records incorrect administrator passwords before locking the administrator out of Cisco ISE and disabling account credentials:
  - The number of failed attempts Cisco ISE logs before the administrator account is disabled based on incorrect password entry. (The minimum and default number of attempts is 5, and the maximum number of allowed attempts is 20.)
  - Text that is displayed notifying the user of the administrator account deactivation.



**Note** If you are using external identity stores 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. For information on administrator login via external identity stores, see [Configuring Cisco ISE for Administrator Access Using an External Identity Store, page 4-44](#).

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

#### Related Topics

- [Configuring Cisco ISE Administrators, page 4-34](#)
- [Configuring Admin Groups, page 4-37](#)
- [Configuring Cisco ISE for Administrator Access Using an External Identity Store, page 4-44](#)

## Configuring 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 administrative user interface.

#### Prerequisite:

Every Cisco ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have any one of the following roles assigned: Super Admin or System Admin. See [Table 4-11](#) for more information on the various administrative roles and the privileges associated with each of them.

**To configure session timeout, complete the following steps:**

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

- Step 2** Enter the amount of 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** to save the administrator session timeout settings.

#### Related Topics

- [Configuring Cisco ISE Administrators, page 4-34](#)
- [Configuring Admin Groups, page 4-37](#)

## Changing Administrator Name

Cisco ISE allows the name of the internal administrator account to be changed to help prevent security breaches of the system. Since ISE supports role-based access control, this is applicable not only to the default Cisco ISE Administrator but to all the internal administrators.

All administrators can change their own name in two ways:

- From the respective Edit screens, based on their privilege level
- From the *logged in user's* link that is available on the left of the **Logout** button. This link appears in the logged in user's name. For example, if you have logged in as *Smith*, the link is displayed as *Smith*. [Figure 4-4](#) shows *admin* as the logged in user.

**Figure 4-4** Logged in User Link



When administrators edit their own name, they are redirected to the login page. A Super admin can change the name of all other admin roles, including system/default administrators.

The administrator name can be changed in the following ways:

- A Super/System/RBAC admin can change the administrator name from the **Administration > System > Admin Access > Administrators > Admin Users > Edit** page or from the *logged in user's* link.
- An Identity or Policy admin can change the administrator name from the *logged in user's* link only.
- A network access user who is promoted to Identity or Policy admin can change the administrator name from the **Administration > Identity Management > Identities > Users > Edit** page or from the *logged in user's* link.

## Configuring Network Access for User Accounts

Cisco ISE allows you to restrict network access for user accounts that are based on authentication settings that you configure for attributes and passwords associated with the user accounts. When defining user accounts, you can manage network access in the following ways:

- Use pre-defined system attributes or create custom attributes
- Define authentication settings that form a password policy

There are two options for configuring network access for user accounts:

- [User Custom Attributes Policy, page 4-67](#)
- [User Password Policy, page 4-67](#)

For information about configuring network access user accounts, see [Configuring Network Access User Accounts, page 4-68](#).

## User Custom Attributes Policy

When you choose User Custom Attributes Policy, the page displays two panes with the following options that you can use to define user account attributes:

- Pre-defined Attributes
- Custom Attributes

The Cisco ISE provides the following predefined and nonconfigurable attributes that help to define a user account:

- AllowPasswordChangeAfterLogin—A string that defines a password change after logging in
- CredentialPassword—A string defining the credential password
- DatePasswordLastUpdatedOn—A string defining the last date the account password was updated
- Description—A string representing the account password
- EmailAddress—A string defining the e-mail address for the account
- EnableFlag—A string defining the account as enabled
- FirstName—A string defining the user first name
- LastName—A string defining the user last name
- NumberOfSuccessiveFailedAttempts—An integer value defining the number successful or failed login attempts
- OlderGenerationPasswordList—A string list defining previous account passwords
- SecureID—A string defining the account username
- isSystemData—An integer representing system data for the account
- isAdmin—A string defining whether the account role is an admin or user

The Cisco ISE also allows you to define custom attributes to help further define a user account by configuring the following:

- Attribute Name—Enter a name for the custom attribute you create
- Data Type—Choose one of the following from a drop-down list for the custom attribute:
  - **String**
  - **Integer**
  - **Enum**
  - **Float**
  - **Password**

## User Password Policy

When you choose User Password Policy, the Password Policy page allows you to set by entering values in text boxes or checking check boxes.

The following choices that you configure creates a password policy for managing network access per user account:

- Password Policy
  - Minimum Length—Sets the minimum length of password (in characters)
  - Username—Restricts the use of the username or its characters in reversed order
  - Cisco—Restricts the use of “cisco” or its characters in reversed order
  - Special characters—Restricts the use of special characters that you define in reverse order
  - Repeated characters—Restricts the use of characters repeated four or more times consecutively
  - Required characters—Requires that the password include at least one of each of the following types:
    - Lowercase alphabetic characters
    - Uppercase alphabetic characters
    - Numeric characters
    - Non-alphanumeric characters

Cisco ISE provides the following configurable options that you set by entering values in text boxes or checking check boxes.

The following choices that you configure creates an advanced password policy for managing network access per user account:

- **Password History**—Sets the number of previous versions from which the password must be different to prevent the repeated use of the same password.
- **Password Lifetime**—Sets the following options to force users to change passwords after a specified time period:
  - Time (in days) before the user account is disabled if the password is not changed
  - Reminder (in days) before the user account is disabled



**Note**

---

Options marked by an asterisk (\*) are required settings that must have a value configured.

---

## Configuring Network Access User Accounts

The following topics describe how to configure or manage a network access user account:

- [Configuring a User Password Policy for the Network Access User Account, page 4-68](#)
- [Filtering the Predefined Attributes, page 4-69](#)
- [Configuring Custom Attributes for the Network Access User Account, page 4-71](#)

### Configuring a User Password Policy for the Network Access User Account

Use this procedure to configure a password policy for any network access user account.

**To configure a user password policy for a network access user account, complete the following steps:**

- 
- Step 1** Choose **Administration > Identity Management > Settings > User Password Policy**.

The Password Policy page appears.

- Step 2** Configure the password policy for the user account by entering the desired values in the text boxes or checking specific check boxes.



**Note** For more information about the values and corresponding text boxes and check boxes, see [User Password Policy, page 4-67](#).

For example, to create a password policy that requires a strong password, enter the following values or check the following check boxes:

- Enter 10 or greater in the Minimum Length: text box.
- The **Password should not contain the username or its characters in reversed order** check box is checked by default. You may uncheck it if you require.
- Check the **Password should not contain “cisco” or its characters in reversed order** check box.
- Check the **Password should not contain or its characters in reversed order** check box with a specific string in the text box if you require.
- Check the **Password may not contain repeated characters four or more times consecutively** check box.
- Under Password must contain at least one character of each of the following types, check the following check boxes:
  - **Lowercase alphabetic characters**
  - **Uppercase alphabetic characters**
  - **Numeric characters**
  - **Non-alphanumeric characters**

- Step 3** Configure the advanced password settings by entering values or selecting check boxes to define the Password History and Password Lifetime.

For example, to define unique passwords, enter the following values or check the following check boxes:

- Under Password History, enter 5 or greater in the Password must be different from the previous versions text box.
- Under Password Lifetime, check the following check boxes:
  - **Disable user account after \_\_ days if password was not changed**, and enter 30 in the text box (to represent 30 days).
  - **Display reminder after \_\_ days**, and enter 15 in the text box (to represent 15 days).

- Step 4** Click **Save** to save this user password policy locally.

## Filtering the Predefined Attributes

Predefined attributes are system-configured and cannot be modified. However, you can filter the list of predefined attributes and search for specific attributes. Use this procedure to filter and search for specific attributes of interest.

To search for specific predefined attributes, complete the following steps:

---

**Step 1** Choose **Administration > Identity Management > Settings > User Custom Attributes**.

The Pre-defined Attributes page appears with a list of all predefined attributes.

**Step 2** Click the Show drop-down list and choose one of the following options:

- Quick Filter
- Advanced Filter
- a. To perform a Quick Filter, enter search criteria in one of the following attribute fields:
  - Required
  - Attribute Name
  - Data Type
  - Parameter



**Note**

---

By default, all four search fields are displayed. To customize your search to one or more fields, click Action and choose Columns. Unmark any of the selected search fields that you do not wish to use in a search.

---

- b. To perform an Advanced Filter, create a matching rule by choosing one of the following options from the Filter drop-down list:
    - **Attribute Name**
    - **Data Type**
    - **Parameters**
    - **Required**
  - c. From the second drop-down list, choose one of the following options:
    - **Contains**
    - **Does not contain**
    - **Does not equal**
    - **Ends with**
    - **Is empty**
    - **Is exactly (or equals)**
    - **Is not empty**
    - **Starts with**
  - d. In the text box, enter your desired search value.
  - e. Click **Go** to launch the filter process, or click plus (+) to add additional search criteria.
  - f. Click **Clear Filter** to reset the filter process.
-

## Configuring Custom Attributes for the Network Access User Account

The Pre-defined Attributes page allows you to configure custom attributes as part of the authentication settings for the network access user account. The network access user account already contains a set of predefined attributes. You can configure custom attributes using the following process.

**To configure custom attributes for a network access user account, complete the following steps:**

---

**Step 1** Choose **Administration > Identity Management > Settings > User Custom Attributes**.

The Pre-defined Attributes page appears

**Step 2** In the Custom Attributes group box, do the following:

- Enter the name for the custom attribute in the Attribute Name text box.
- From the Data Type drop-down list, choose the data type from these choices:
  - **String**
  - **Integer**
  - **Enum**
  - **Float**
  - **Password**
- To add parameters, click plus (+) under Parameters and add the desired attribute names and data types.

**Step 3** Click **Save** to save these user custom attributes locally.

---

## Endpoint Identity Groups

An endpoint identity group is used to group all the identified endpoints on your network according to their profiles. By default, a Cisco ISE deployment creates the following four identity groups in the system: RegisteredDevices, Blacklist, Profiled, and Unknown. In addition, the system creates two more identity groups: the Cisco-IP-Phone group and the Workstation group, which are both children of the Profiled group.

When you create a new endpoint identity group, you can also choose an endpoint identity group from the available list to be a parent identity group for that new group. You can also assign an endpoint that you create directly (statically) to any one of the identity group that exists in the system, and the profiling service cannot reassign the identity group.

When you create an endpoint profiling policy, you can map an endpoint profile where you match the endpoint profile with an existing profile and group it to a matching identity group. If you have an endpoint profile that matches with an existing profile, then the profiling service can create a matching identity group.

This identity group becomes the child of the Profiled identity group. When you create an endpoint profiling policy, you can check the Create matching identity group check box in the Endpoint Policies page to create a matching identity group. You cannot delete the matching identity group unless the mapping of the profile is removed.

When an endpoint is mapped to an existing profile, the profiling service searches the hierarchy of profiles for the closest parent profile that has a matching group of profiles and assigns the endpoint to the appropriate profile.

## Parent Group

A parent group is the default identity group that exists in the system. By default, a Cisco ISE deployment creates the following four endpoint identity groups: RegisteredDevices, Blacklist, Profiled, and Unknown. In addition, the system creates two more identity groups: the Cisco-IP-Phone group and the Workstation group, which are both children of the Profiled group.

The profiling service includes the following endpoint identity groups:

- **RegisteredDevices**—This endpoint identity group includes endpoints, which are registered devices that are added by an employee through the devices registration portal. The profiling service continues to profile these devices normally when they are assigned to this group. Endpoints are statically assigned to this group in Cisco ISE, and the profiling service cannot reassign them to any other identity group. These devices will appear like any other endpoint in the endpoints list. You can edit, delete, and blacklist these devices that you added through the device registration portal from the endpoints list in the Endpoints page in Cisco ISE. Devices that you have blacklisted in the device registration portal are assigned to the Blacklist endpoint identity group, and an authorization profile that exists in Cisco ISE redirects blacklisted devices to an URL, which displays “Unauthorized Network Access”, a default portal page to the blacklisted devices.
- **Blacklist**—This endpoint identity group includes endpoints that are statically assigned to this group in Cisco ISE and endpoints that are blacklisted in the device registration portal.
- **Profiled**—This endpoint identity group includes endpoints that match endpoint profiling policies except Cisco IP phones and workstations.
- **Unknown**—Endpoints that do not match any profile are grouped within the Unknown endpoint identity group.

In addition, the profiling service includes the following endpoint identity groups, which are associated to the Profiled identity group:

- **Cisco-IP-Phone**—An identity group that contains all the profiled Cisco IP phones on your network.



**Note** An authorization rule for all types of Cisco IP Phones is available in Cisco ISE in the following location: Policy > Authorization > Standard.

- **Workstation**—An identity group that contains all the profiled workstations on your network.

## Using Endpoint Identity Groups in Authorization Policies

The profiling service discovers endpoints and classifies them now into their corresponding endpoint profiling policies based on the attributes that are collected and existing endpoint profiling policies in Cisco ISE. The Cisco ISE application moves these discovered endpoints to the corresponding endpoint identity groups based on the endpoint profiling policies.

The endpoint identity groups can be effectively used in the authorization policies to provide appropriate network access privileges to the discovered endpoints. To use the endpoint identity groups more effectively in the authorization policies, you must ensure that the endpoint profiling policies are either standalone policies (no parent to the policies), or their parent policies of the endpoint profiling policies are disabled.



This section includes the following topic, which describe the procedures for managing endpoint identity groups:

- [Filtering, Creating, Editing, and Deleting Endpoint Identity Groups, page 4-73](#)



**Note**

For more information on endpoint profiling in Cisco ISE networks, see [Chapter 18, “Configuring Endpoint Profiling Policies”](#).

## Filtering, Creating, Editing, and Deleting Endpoint Identity Groups

The Endpoint Identity Groups page allows you to manage endpoint identity groups, and provides an option to filter the groups by their group names and description. This section describes the basic operations that allow you to group all the identified endpoints on your network and manage the identity groups.

The procedures for managing endpoint identity groups include the following tasks:

- [Filtering Endpoint Identity Groups, page 4-73](#)
- [Creating, Editing, and Deleting an Endpoint Identity Group, page 4-75](#)

### Filtering Endpoint Identity Groups

You can use the Show drop-down list or the filter icon to both invoke a quick filter and close it in the Endpoint Identity Groups page. A quick filter is a simple filter that you can use to filter identity groups in the Endpoint Identity Groups page. The quick filter filters identity groups based on field descriptions, such as the name of the identity group and the description in the Endpoint Identity Groups page.

You can use the Show drop-down list to invoke an advanced filter. An advanced filter is a complex filter that you can preset for use and retrieve later, along with the filtering results, in the Endpoint Identity Groups page. The advanced filter filters based on a specific value that is associated with the field description. You can add or remove filters, as well as combine a set of filters into a single advanced filter.

You can use the Manage Preset Filters option, which lists all the preset filters. This option allows you to manage preset filters. Once you have created and saved a preset filter, you can choose a preset filter from the list of filtered results in the Endpoint Identity Groups page. You can also edit preset filters and remove them from the preset filters list.

**To filter identity groups in the Endpoint Identity Groups page, complete the following steps:**

- 
- Step 1** Choose **Administration > Identity Management > Groups > Endpoint Identity Groups**.  
The Endpoint Identity Groups page appears, which lists all the identity groups.
- Step 2** In the Endpoint Identity Groups page, click the Show drop-down arrow to choose the filter option.  
Here, you can choose a Quick Filter, an Advanced Filter for filtering, or the Manage Preset Filters option, which allows you to manage preset filters for filtering. See [Table 4-17](#).  
For more information, see the [To filter endpoint identity groups by using the Quick Filter option, complete the following steps;](#), page 4-74 and the [To filter endpoint identity groups by using the Advanced Filter option, complete the following steps;](#), page 4-74.



**Note** To return to the endpoint identity groups list, choose **All** from the Show drop-down list to display all the endpoint identity groups without filtering.

**To filter endpoint identity groups by using the Quick Filter option, complete the following steps:**

A quick filter filters identity groups based on each field description in the Endpoint Identity Groups page. When you click inside any field, and as you enter the search criteria in the field, it refreshes the page with the result in the Endpoint Identity Groups page. If you clear the field, it displays the list of all the endpoint identity groups in the Endpoint Identity Groups page.

- Step 1** To filter, click **Go** in each field to refresh the page with the results that are displayed in the Endpoint Identity Groups page.
- Step 2** To clear the field, click **Clear** in each field.

**To filter endpoint identity groups by using the Advanced Filter option, complete the following steps:**

An advanced filter enables you to filter identity groups by using variables that are more complex. It contains one or more filters that filter identity groups based on the values that match the field descriptions. A filter on a single row filters identity groups based on each field description and the value that you define in the filter. Multiple filters can be used to match the value(s) and filter identity groups by using any one or all of the filters within a single advanced filter.

- Step 1** To choose the field description, click the drop-down arrow.
- Step 2** To choose the operator, click the drop-down arrow.
- Step 3** Enter the value for the field description that you selected.
- Step 4** Click **Add Row** (plus [+] sign) to add a filter, or click **Remove Row** (minus [-] sign) to remove a filter.
- Step 5** Choose **All** to match the value in each filter, or **Any** to match the value in any one of the filters.
- Step 6** Click **Go** to start filtering.
- Step 7** Click the **Save** icon to save the filter.

The Save Preset Filter dialog appears. Enter a file name to save the filter, and click **Save**. Do not include spaces when creating the name for a preset filter. Click **Cancel** to clear the filter without saving the current filter.



**Note** Any preset filter that you create and save is browser-based only and is only accessible using the same browser type (preset filters are not saved in the Cisco ISE database). For example, any preset filter you create and save using a Firefox version 3.6.x browser will not be accessible by a Microsoft Internet Explorer (IE8) browser (or vice versa).

- Step 8** Click **Clear Filter** after filtering.

Table 4-17 describes the fields in the Endpoint Identity Groups page that allow you to filter the endpoint identity groups.

**Table 4-17** Filtering Endpoint Identity Groups

Filtering Method	Filtering Field	Filtering Field Description
Quick Filter	Name	This field enables you to filter identity groups by the name of the endpoint identity group.
	Description	This field enables you to filter identity groups by the description of the endpoint identity group.
Advanced Filter	Choose the field description from the following: <ul style="list-style-type: none"> <li>Name</li> <li>Description</li> </ul>	Click the drop-down arrow to choose the field description.
	Operator	From the Operator field, click the drop-down arrow to choose an operator that can be used to filter identity groups.
	Value	From the Value field, choose the value for the field description that you selected against which the endpoint identity groups are filtered.

## Creating, Editing, and Deleting an Endpoint Identity Group

You can create, edit, or delete an endpoint identity group in the Endpoint Identity Groups page.

To create an endpoint identity group in the Endpoint Identity Groups page, complete the following steps:

- 
- Step 1** Choose **Administration > Identity Management > Groups > Identity Groups > Endpoint Identity Groups**.
- The Endpoint Identity Groups page appears, which lists all the identity groups.
- Step 2** In the Endpoint Identity Groups page, choose **Create**.
- Step 3** Modify the values in the New Endpoint Group page, as shown in [Table 4-18](#).
- Step 4** Perform one of the following tasks:
- Click **Submit** to create the endpoint, which appears in the Endpoint Identity Groups page.
  - Click **Cancel** to terminate the action without creating the endpoint.
- Step 5** Click the **Endpoint Group List** link to return to the Endpoint Identity Groups page.
-

Table 4-18 describes the fields in the Endpoint Identity Groups page that allow you to create an endpoint identity group:

**Table 4-18** *Creating Endpoint Identity Groups*

Field Name	Description
Name	In the Name field, enter the name of the endpoint identity group that you want to create.  <b>Note</b> Use the best practice to include no spaces when creating the name for an endpoint identity group.
Description	In the Description field, enter the description of the endpoint identity group that you want to create.
Parent Group	Cisco ISE creates the following four endpoint identity groups on your deployment: RegisteredDevices, Blacklist, Profiled, and Unknown.  In the Parent Group field, choose an endpoint identity group. Click the drop-down arrow to view the endpoint identity groups, which are created on your Cisco ISE deployment.

**To edit an endpoint identity group in the Endpoint Identity Groups page, complete the following steps:**

**Step 1** Choose **Administration > Identity Management > Groups > Identity Groups > Endpoint Identity Groups**.

The Endpoint Identity Groups page appears, which lists all the identity groups.

**Step 2** In the Endpoint Identity Groups page, choose an identity group, then choose **Edit**.



**Note** You can only edit the name and description of the identity groups that you create in the system. The name of the endpoint identity groups are not editable but their description are editable that are created by Cisco ISE in the system.

**Step 3** Perform one of the following tasks:

- a. Click **Reset** to revert to the previous data.
- b. Verify if you want to reset the data and lose any current data, or click **Cancel** to continue with the current input data.
- c. Click **Save** to save the current input data in the edit page.

**Step 4** Click the **Endpoint Group List** to return to the Endpoint Identity Groups page after editing an endpoint identity group.

**To delete an endpoint identity group in the Endpoint Identity Groups page, complete the following steps:**

**Step 1** Choose **Administration > Identity Management > Groups > Identity Groups > Endpoint Identity Groups**.

The Endpoint Identity Groups page appears, which lists all the identity groups.

**Step 2** Choose an endpoint identity group in the Endpoint Identity Groups page, then choose **Delete**.



**Note** You can only delete the identity groups that you create in the system. You cannot delete the endpoint identity groups that are created by Cisco ISE in the system.

- Step 3** Click **OK** in the confirmation dialog to delete an endpoint identity group.
- Click **Cancel** to return to the Endpoint Identity Groups page without deleting the endpoint identity group.

#### Related Topics

[Filtering, Adding and Removing Endpoints in an Endpoint Identity Group, page 4-77](#)

## Filtering, Adding and Removing Endpoints in an Endpoint Identity Group

This section describes the basic operations that allow you to manage endpoints in an endpoint identity group. The MAC address is used in all the basic operations.

You can filter, add, or remove statically added endpoints in any endpoint identity group. If an endpoint identity group assignment is not static, then endpoints are reprofiled after adding, or removing from any endpoint identity group. Endpoints that are identified dynamically by the profiler appear in appropriate endpoint identity groups. If you remove dynamically added endpoints from an endpoint identity group, Cisco ISE displays a message that you have successfully removed endpoints from the identity group but reprofiles them back in the endpoint identity group. You can only add endpoints from the Endpoints widget to a specific identity group. If you add an endpoint to the specific endpoint identity group, then the endpoint is moved from the endpoint identity group where it was dynamically grouped earlier. Upon removal from the endpoint identity group where you recently added an endpoint, the endpoint is reprofiled back to the appropriate identity group. Here, you do not delete endpoints from the endpoint identity group but only remove them from the endpoint identity group.

The Endpoint Identity Group page displays the name and description of all the endpoint identity groups. You can use the Edit menu in the Endpoint Identity Groups page to filter, add, or remove endpoints in an endpoint identity group.

The procedure for managing endpoints in the endpoint identity groups include the following tasks:

- [Filtering Endpoints in an Endpoint Identity Group, page 4-77](#)
- [Adding Endpoints in an Endpoint Identity Group, page 4-79](#)
- [Removing Endpoints in an Endpoint Identity Group, page 4-79](#)

### Filtering Endpoints in an Endpoint Identity Group

You can use the Show drop-down list or the filter icon to both invoke a quick filter and close it on the Endpoint Identity Groups page. A quick filter is a simple filter that you can use to filter endpoints in an endpoint identity group in the Endpoint Identity Groups page.

You can use the Show drop-down list to invoke an advanced filter. An advanced filter is a complex filter that you can preset for use and retrieve later, along with the filtering results, in the Endpoint Identity Groups page. You can add or remove filters, as well as combine a set of filters into a single advanced filter. Both the filters use only the MAC address for filtering endpoints in any endpoint identity group.

You can use the Manage Preset Filters option, which lists all the preset filters. This option allows you to manage preset filters. Once you have created and saved a preset filter, you can choose a preset filter from

the list of filtered results in the Endpoint Identity Groups page. You can also edit preset filters and remove them from the preset filters list.

**To filter endpoints in an identity group on the Identity Group Endpoints page, complete the following steps:**

- 
- Step 1** Choose **Administration > Identity Management > Groups > Endpoint Identity Groups**.  
The Endpoint Identity Group Page appears, which lists all the endpoint identity groups.
- Step 2** In the Endpoint Identity Group page, choose an endpoint identity group, and then **Edit**.  
Click the arrow in front of Endpoints to display or hide the Identity Group Endpoints page.
- Step 3** Click the Show drop-down list to list the filter options in the Identity Group Endpoints page.  
Here, you can choose a Quick Filter, an Advanced Filter for filtering, or the Manage Preset Filters option, which allows you to manage preset filters for filtering.
- For more information, see the [To filter endpoints in an endpoint identity group by using the Quick Filter option, complete the following steps:](#), page 4-78 and [To filter endpoints in an endpoint identity group by using the Advanced Filter option, complete the following steps:](#), page 4-78




---

**Note** To return to the identity group endpoints list, choose All from the Show drop-down list to display all the endpoints without filtering.

---

**To filter endpoints in an endpoint identity group by using the Quick Filter option, complete the following steps:**

A quick filter filters endpoints based on the MAC address in an endpoint identity group.

- 
- Step 1** Enter the MAC address in the form of nn:nn:nn:nn:nn to filter endpoints in an endpoint identity group.
- Step 2** To filter, click **Go**.  
As you enter the MAC address, the Endpoint Identity Groups page refreshes with endpoints that match the search criteria in the Endpoint Identity Groups page.  
If you choose to clear the MAC address, the Endpoint Identity Groups page displays the list of all the endpoints.
- 

**To filter endpoints in an endpoint identity group by using the Advanced Filter option, complete the following steps:**

An advanced filter allows you to filter endpoints based on the MAC address. A filter on a single row filters endpoints based on the MAC address that you define. Multiple filters can be used to match the MAC addresses and filter endpoints by using any one or all of the filters within a single advanced filter.

- 
- Step 1** To choose the field description, click the drop-down arrow.
- Step 2** To choose the operator, click the drop-down arrow.
- Step 3** Enter the value for the field description that you selected.
- Step 4** Click **Add Row** (plus [+] sign) to add a filter, or click **Remove Row** (minus [-] sign) to remove a filter.
- Step 5** Choose **All** to match the value in each filter, or **Any** to match the value in any one of the filters.
- Step 6** Click **Go** to start filtering.

- Step 7** Click the **Save** icon to save the filter.
- The Save Preset Filter dialog appears. Enter a file name to save the filter, and click **Save**. Do not include spaces when creating the name for a preset filter. Click **Cancel** to clear the filter without saving the current filter.
- Step 8** Click **Clear Filter** after filtering.
- 

## Adding Endpoints in an Endpoint Identity Group

You can add endpoints to an identity group from the Endpoints widget, or remove endpoints from the identity group. You cannot remove an endpoint from the identity group that has a matching profile with an existing profile.

**To add endpoints to an endpoint identity group, complete the following steps:**

---

- Step 1** Choose **Administration > Identity Management > Groups > Endpoint Identity Groups**.
- The Endpoint Identity Groups page appears, which lists all the identity groups.
- Step 2** In the Endpoint Identity Groups page, choose an identity group.
- Step 3** In the Endpoint Identity Groups page, choose **Edit**.
- Step 4** Click the arrow in front of Endpoints to display or hide the Identity Group Endpoints list page, which displays the list of endpoints for the selected endpoint identity group.
- Step 5** Click **Add**.
- The Endpoints widget appears.
- Step 6** Choose an endpoint In the Endpoints widget.
- The endpoint appears in the endpoint identity group.
- Step 7** Click the **Endpoint Group List** link to return to the Endpoint Identity Groups page.
- 

## Removing Endpoints in an Endpoint Identity Group

You can remove one or more endpoints in an endpoint identity group. If endpoints are filtered in the Identity Group Endpoints list page, only those filtered endpoints are removed from the endpoint identity group when you are using the Removing All option.

**To remove endpoints in an endpoint identity group, complete the following steps:**

---

- Step 1** Choose **Administration > Identity Management > Groups > Endpoint Identity Groups**.
- The Endpoint Identity Groups page appears, which lists all the identity groups.
- Step 2** In the Endpoint Identity Groups page, choose an identity group.
- Step 3** In the Endpoint Identity Groups page, choose **Edit**.
- Step 4** Click the arrow in front of Endpoints to display or hide the Identity Group Endpoints list page, which displays the list of endpoints for the selected endpoint identity group.
- Step 5** Choose an endpoint from the Identity Group Endpoints list, and choose **Remove**.

Remove Selected and Remove All options appear. You can choose to remove one or more endpoints that you select or remove all the endpoints in an endpoint identity group.



---

**Note** Here, you can remove one or more endpoints from the endpoint identity group.

---

**Step 6** Click the **Endpoint Group List** link to return to the Endpoint Identity Groups page.

---