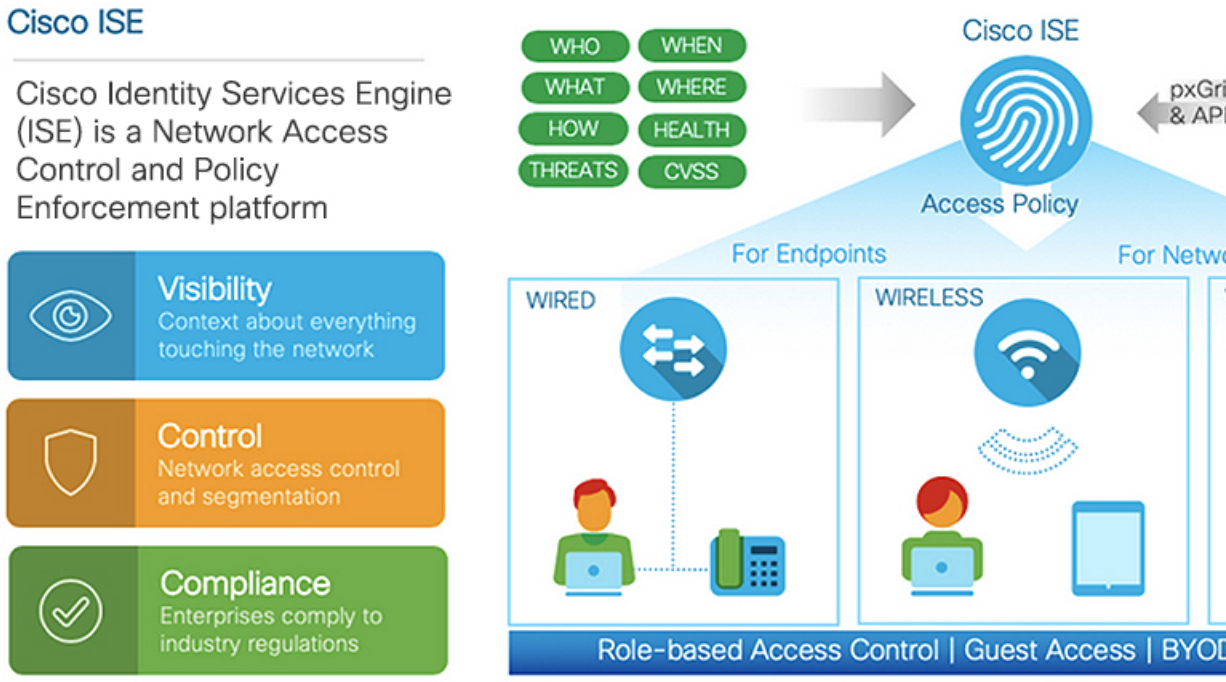
Cisco ISE 2.7 Admin Guide: Overview

Cisco ISE Overview



Cisco Identity Services Engine (ISE) is an identity-based network access control and policy enforcement system. It functions as a common policy engine that enables endpoint access control and network device administration for enterprises.

You can leverage Cisco ISE to ensure compliance, enhance infrastructure security, and streamline service operations.

A Cisco ISE administrator can gather real-time contextual data for a network, including users and user groups (who?), device type (what?), access time (when?), access location (where?), access type (wired, wireless, or VPN) (how?), and network threats and vulnerabilities.

As a Cisco ISE administrator, you can use this information to make network governance decisions. You can also tie identity data to various network elements to create policies that govern network access and usage.

Cisco ISE Features

Cisco ISE empowers you with the following capabilities:

- **Device Administration**: Cisco ISE uses the TACACS+ security protocol to control and audit the configuration of network devices. It facilitates granular control of who can access which network device

and change the associated network settings. Network devices can be configured to query Cisco ISE for authentication and authorization of device administrator actions. These devices also send accounting messages to Cisco ISE to log such actions.

- **Guest and Secure Wireless**: Cisco ISE enables you to provide secure network access to visitors, contractors, consultants, and customers. You can use web-based and mobile portals to on-board guests to your company's network and internal resources. You can define access privileges for different types of guests, and assign sponsors to create and manage guest accounts.
- **Bring Your Own Device (BYOD)**: Cisco ISE allows your employees and guests to securely use their personal devices on your enterprise network. The end users of the BYOD feature can use configured pathways to add their devices, and be provisioned predefined authentication and level of network access.
- **Asset Visibility**: Cisco ISE gives you visibility and control over who and what is on your network consistently, across wireless, wired, and VPN connections. Cisco ISE uses probes and device sensors to listen to the way devices connect to the network. The Cisco ISE profile database, which is extensive, then classifies the device. This gives the visibility and context you need to grant the right level of network access.
- **Secure Wired Access**: Cisco ISE uses a wide range of authentication protocols to provide network devices and endpoints with a secure wired network access. These include, but are not limited to, 802.1X, RADIUS, MAB, web-based, EasyConnect, and external agent-enabled authentication methods.
- **Segmentation**: Cisco ISE uses contextual data about network devices and endpoints to facilitate network segmentation. Security group tags, access control lists, network access protocols, and policy sets defining authorization, access, and authentication, are some ways in which Cisco ISE enables secure network segmentation.
- **Posture or Compliance**: Cisco ISE allows you to check for compliance, also known as posture, of endpoints before allowing them to connect to your network. You can ensure that endpoints receive the appropriate posture agents for posturing services.
- **Threat Containment**: If Cisco ISE detects threat or vulnerability attributes from an endpoint, adaptive network control policies are sent to dynamically change its access levels of the endpoint. After the threat or vulnerability is evaluated and addressed, the endpoint is given back its original access policy.
- **Security Ecosystem Integrations**: The pxGrid feature allows Cisco ISE to securely share context-sensitive information, policy and configuration data, and so on, with connected network devices, third-party vendors, or Cisco partner systems.

Cisco ISE Administrators

Administrators can use the admin portal to:

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

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

The username and password that you configure during setup is intended only for administrative access to the CLI. This role is considered to be the CLI admin user, also known as CLI administrator. By default, the username for a CLI admin user is admin, and the password is defined during setup. There is no default password. This CLI admin user is the default admin user, and this user account cannot be deleted. However, it can be edited by other administrators, including options to enable, disable, or change password for this account.

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

Administrators are users who have local privileges to configure and operate the Cisco ISE system.

Administrators are assigned to one or more admin groups.

Related Topics

Cisco ISE Administrator Groups, on page 5

Force CLI Administrator to Use External Identity Store

Authentication with an external identity source is more secure. RBAC for CLI Administrators is supported when using an external identity store.

Prerequisites

You must have defined the Admin user, and added them to an Administrator group. The Admin must be a Super Admin.

Define the User's Attributes in the AD User Directory

On the Windows server running Active Directory, modify the attributes for each user that you plan to configure as a CLI Administrator.

1. Open the Server Manager Window, and navigate to **Server Manager > Roles > Active Directory Domain Services > Active Directory Users and Computers > [ad.adserver] <ad_server>.local**.
2. Enable **Advanced Features** under the **View** menu so you can edit a user's attributes.
3. Navigate to the Active Directory group that contains the Admin user and find that user.
4. Double-click the user to open the **Properties** window and select the **Attribute Editor**.
5. Click any attribute and start typing "gid" to locate the attribute `gidNumber`. If you don't find the gidNumber attribute, click the **Filter** button and un-check **Show only attributes that have values**.
6. Double-click the attribute name to edit each attribute. For each user:
   - Assign `uidNumber` greater than 60000, and make sure that the number is unique.
   - Assign `gidNumber` as 110 or 111.
   - GidNumber 110 denotes an admin user whereas 111 denotes a read-only user.
   - Do not change the uidNumber after assignment.
   - If you modify the gidNumber, wait at least five minutes before making an SSH connection.

Join the Admin CLI User to the AD Domain

Connect to the Cisco ISE CLI, run the **identity-store** command, and assign the Admin user to the ID store. For example, to map the CLI admin user to the Active Directory defined in ISE as adpool1, **run identity-store active-directory domain-name adpool1 user admincliuser**.

When the join is complete, connect to the Cisco ISE CLI and log in as the Admin CLI user to verify your configuration.

If the domain you use in this command is the same as the one that was previously joined to the ISE node, then you must rejoin the domain in the Administrators console.

1. Navigate to **Administration > Identity Management > External Identity Sources**.
2. In the left-hand pane, select **Active Directory** and select your Active Directory name.
3. In the right-hand pane, the status for your AD connection might say **Operational**. But you will receive errors if you test the connection with **Test User** using either MS-RPC or Kerberos.
4. Verify that you can still log in to the Cisco ISE CLI as the Admin CLI user.

Create a New Administrator

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

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

Note We recommend that you configure Active Directory access in the CLI before you join it in the GUI, if the admin user's domain is the same in both the CLI and the GUI. Else, you must rejoin the domain from the GUI to avoid authentication failures to that domain.

Procedure

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

Step 2 From the drop-down, choose one of the following options:

- **Create an Admin User**

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

- **Select from Network Access Users**

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

Step 3 Enter values in the fields. The characters supported for the **Name** field are # $ ’ ( ) * + - . / @ _.

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

Related Topics

Read-Only Admin Policy, on page 21
Create an Internal Read-Only Admin
Customize Menu Access for the Read-Only Administrator, on page 21
Map External Groups to the Read-Only Admin Group

Cisco ISE Administrator Groups

Administrator groups are role-based access control (RBAC) groups in Cisco ISE. All the administrators who belong to the same group share a common identity and have the same privileges. An administrator's identity as a member of a specific administrative group can be used as a condition in authorization policies. An administrator can belong to more than one administrator group.

An administrator account with any level of access can be used to modify or delete objects for which it has permission, on any window it has access to.

The Cisco ISE security model limits administrators to creating administrative groups that contain the same set of privileges that the administrator has. The privileges given are based on the administrative role of the user, as defined in the Cisco ISE database. Thus, administrative groups form the basis for defining privileges to access the Cisco ISE systems.

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

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

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

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

Admin Group Role	Access Level	Permissions	Restrictions
Network Device Admin	Manage Cisco ISE network devices and network device repository.	• Read and write permissions on network devices • Read and write permissions on Network Device Groups and all network resources object types. • View the Cisco ISE dashboard, live logs, alarms, and reports. • Run all troubleshooting flows.	Cannot perform any policy management, identity management, or system-level configuration tasks in Cisco ISE.

Admin Group Role	Access Level	Permissions	Restrictions
Policy Admin	Create and manage policies for all Cisco ISE services across the network, which are related to authentication, authorization, posture, profiler, client provisioning, and work centers.	• Read and write permissions on all the elements that are used in policies, such as authorization profiles, NDGs, and conditions. • Read and write permissions on identities, endpoints, and identity groups (user identity groups and endpoint identity groups). • Read and write permissions on services policies and settings. • View the Cisco ISE dashboard, live logs, alarms, and reports. • Run all troubleshooting flows. • Device Administration—Access to device administration work centers. Permission for TACACS policy conditions and results. Network device permissions for TACACS proxy and proxy sequences.	Cannot perform any identity management or system-level configuration tasks in Cisco ISE. Device Administration—Access to the work center does not guarantee access to the subordinate links.

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

Admin Group Role	Access Level	Permissions	Restrictions
Read-Only Admin	Read-only access to the ISE GUI.	• View and use the functions of the dashboard, reports, and live logs or sessions, such as filtering data, querying, saving options, printing, and exporting data. • Change passwords of their own accounts. • Query ISE using global search, reports, and live logs or sessions. • Filter and save data based on the attributes. • Export data pertaining to authentication policies, profile policies, users, endpoints, network devices, network device groups, identities (including groups), and other configurations. • Customize report queries, save, print, and export them. • Generate custom report queries, save, print, or export the results. • Save UI settings for future reference. • Download logs, such as ise-psc-log from the **Operations** > **Troubleshoot** > **Download Logs** window.	

Admin Group Role	Access Level	Permissions	Restrictions
			• Perform any configuration changes such as create, update, delete, import, quarantine, and Mobile Device Management (MDM) actions of objects, such as authorization policies, authentication policies, posture policies, profiler policies, endpoints, and users. • Perform system operations, such as backup and restore, registration or deregistration of nodes, synchronization of nodes, creating, editing, and deleting node groups, or upgrade and installation of patches. • Import data pertaining to policies, network devices, network device groups, identities (including groups), and other configurations. • Perform operations, such as CoA, endpoint debugging, modifying collection filters, bypassing suppression on live sessions data, modifying the PAN-HA failover settings, and editing

Admin Group Role	Access Level	Permissions	Restrictions
			the personas or services of Cisco ISE nodes. • Run commands that might have a heavy impact on performance. For example, access to the TCP Dump in the **Operations** > **Troubleshoot** > **Diagnostic Tools** > **General Tools** window is restricted. • Generate support bundles.

Admin Group Role	Access Level	Permissions	Restrictions
Super Admin	All Cisco ISE administrative functions. The default administrator account belongs to this group.	Create, read, update, delete, and eXecute (CRUDX) permissions on all Cisco ISE resources. **Note** The super admin user cannot modify the default system-generated RBAC policies and permissions. To do this, you must create new RBAC policies with the necessary permissions based on your needs, and map these policies to an admin group. Device Administration—Access to device administration work centers. Permission for TACACS policy conditions and results. Network device permissions for TACACS proxy and proxy sequences. In addition, permission to enable TACACS global protocol settings.	• Device Administration—Access to the work center does not guarantee access to the subordinate links. • Only an admin user from the default Super Admin Group can modify or delete other admin users. Even an externally mapped user who is part of an Admin Group cloned with the Menu and Data Access privileges of the Super Admin Group cannot modify or delete an admin user.

Admin Group Role	Access Level	Permissions	Restrictions
System Admin	All Cisco ISE configuration and maintenance tasks.	Full access (read and write permissions) to perform all the activities under the **Operations** tab and partial access to some menu items under the **Administration** tab: • Read permissions on administrator account settings and administrator group settings. • Read permissions on admin access and data access permissions along with the **RBAC policy** window. • Read and write permissions for all options under **Administration** > **System**. • View authentication details. • Enable or disable Endpoint Protection Services Adaptive Network Control • Create, edit, and delete alarms; generate and view reports; and use Cisco ISE to troubleshoot problems in your network. • Device Administration—Permission to enable TACACS global protocol settings.	Cannot perform any policy management or system-level configuration tasks in Cisco ISE.

Admin Group Role	Access Level	Permissions	Restrictions
Elevated System Admin (available in Cisco ISE, Release 2.6, Patch 2 and above)	All Cisco ISE configuration and maintenance tasks.	In addition to all the privileges of the System Admin, an Elevated System Admin can create Admin users.	• Cannot create or delete Super Admin users. • Cannot Manage the Super Admin groups.
External RESTful Services (ERS) Admin	Full access to all ERS API requests such as GET, POST, DELETE, PUT	• Create, read, update, and delete ERS API requests.	The role is meant only for ERS authorization supporting internal users, identity groups, endpoints, endpoint groups, and SGT
External RESTful Services (ERS) Operator	Read-only access to ERS API, only GET	• Can only read ERS API requests	The role is meant only for ERS authorization supporting internal users, identity groups, endpoints, endpoint groups, and SGT.
TACACS+ Admin	Full access	Access to: • Device Administration Work Center. • Deployment—To enable TACACS+ services. • External Identity Stores. • **Operations** > **TACACS Live Logs** window.	—

Related Topics

Cisco ISE Administrators, on page 2

Create an Admin Group

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

Before you begin

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

Procedure

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

Step 2 Click **Add**, and enter a name and description.

The supported special characters for the **Name** field are: space, # $ & ‘ ( ) * + - . / @ _ .

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

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

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

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

Step 5 Click **Submit**.

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

Administrative Access to Cisco ISE

Cisco ISE administrators can perform various administrative tasks based on the administrative group to which they belong. These administrative tasks are critical. Grant administrative access only to users who are authorized to administer Cisco ISE in your network.

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

Administrative Access Methods

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

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

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

- **CLI password**: You must enter a CLI password during installation. If you have a problem logging in to the CLI because of an invalid password, you can reset the CLI password. Connect to the console and run the **password** CLI command to rest the password. See the *ISE CLI Reference* for more information.
- **SSH access to the CLI**: You can enable SSH access either during installation or after, using the **service sshd** command. You can also force SSH connections to use a key. Note that when you do this, SSH connections to all the network devices also use that key,see the SSH Key Validation section in Cisco ISE Admin Guide: Segmentation. You can force the SSH key to use the Diffie-Hellman Algorithm. Note that ECDSA keys are not supported for SSH keys.

Role-Based Admin Access Control in Cisco ISE

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

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

Regardless of the level of access, any administrator account can modify or delete objects for which it has permission, on any page that it can access.

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

Role-Based Permissions

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

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

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

RBAC Policies

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

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

Note If you are using customized RBAC policies for admin access, ensure that you provide all relevant menu access for a given data access. For example, to add or delete endpoints with data access of Identity or Policy Admin, you must provide menu access to **Work Center > Network Access** and **Administration > Identity Management**.

Default Menu Access Permissions

Cisco ISE provides an out of the box set of permissions that are associated with a set of predefined admin groups. Having predefined admin group permissions allow you to set permissions so that a member of any admin group can have full or limited access to the menu items within the administrative interface (known as menu access) and to delegate an admin group to use the data access elements of other admin groups (known as data access). These permissions are reusable entities that can be further used to formulate RBAC policies for various admin groups. Cisco ISE provides a set of system defined menu access permissions that are already used in the default RBAC policies. Apart from the predefined menu access permissions, Cisco ISE also allows you to create custom menu access permissions that you can use in RBAC policies. The key icon represents menu access privileges for the menus and submenus, and the key with a close icon represents no access for different RBAC groups.

Note For a Super Admin user, all the menu items are available. For other admin users, all the menu items in the **Menu Access Privileges** column are available for standalone deployment and primary node in a distributed deployment. For secondary nodes in a distributed deployment, the menu items under the **Administration** tab are not available.

Configure Menu Access Permissions

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

Procedure

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

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

a) Expand the **ISE Navigation Structure** menu to the desired level, and click the option(s) for which you want to create permissions.

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

Step 3 Click **Submit**.

Prerequisites for Granting Data Access Permissions

When an RBAC admin has Full Access permission to an object (for example, Employee in the User Identity Groups data type), the admin can view, add, update, and delete users who belong to that group. Ensure that the admin has menu access permission granted for the **Users** window (**Administration > Identity Management**

> **Identities > Users**). This is applicable for network devices and endpoints objects (based on the permissions granted to the Network Device Groups and Endpoint Identity Groups data types).

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

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

Default Data Access Permissions

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

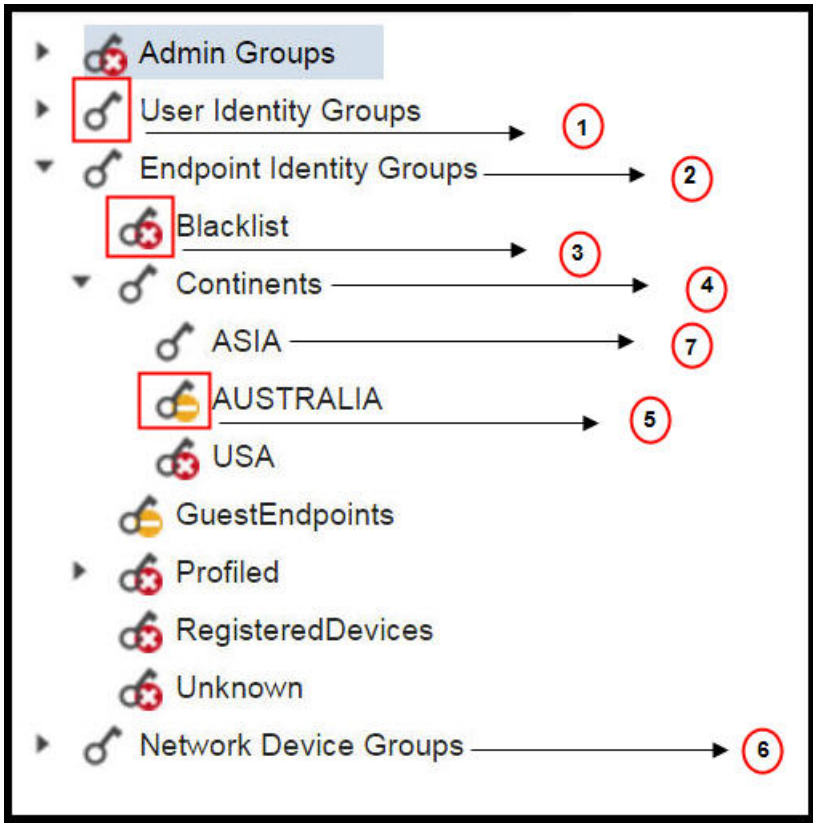
There are three data access permissions, namely, Full Access, No Access, and Read Only access that can be granted to admin groups.

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

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

If you have read-Ooly permission for a data type (for example, Endpoint Identity Groups), you will not be able to perform CRUD operations on that data type. If you have read-only permission for an object (for example, GuestEndpoints), you cannot perform edit or delete operations on that object.

Figure 1: The following image describes how Data Access Privileges apply at the second-level or third-level menu that contains additional submenus or options for different RBAC groups.



Label	Description
1	Denotes full access for the User Identity Groups data type.
2	Denotes that Endpoint Identity Groups derive the maximum permission (full access) that is granted to its child (Asia).
3	Denotes no access for the object (Blacklist).
4	Denotes that the parent (Continents) derives the maximum access permission granted to its child (Asia).
5	Denotes Read Only access for the object (Australia).
6	Denotes that when Full Access is granted to the parent (Network Device Groups), it results in the children automatically inheriting permissions.

Label	Description
7	Denotes that when Full Access is granted to the parent (Asia), it results in the objects inheriting the Full Access permission, unless permissions are explicitly granted to the objects.

Configure Data Access Permissions

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

Procedure

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

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

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

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

b) Click **Full Access**, **Read Only Access,** or **No Access**.

Step 4 Click **Save**.

Read-Only Admin Policy

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

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

Customize Menu Access for the Read-Only Administrator

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

Procedure

Step 1 Log in to the Admin Portal as a Super Admin.

Step 2 Navigate to the **Administration > System > Admin Access > Authorization > Permissions > Menu Access** page.

Step 3 Click **Add** and enter a **Name** (for example, MyMenu) and **Description**.

Step 4 In the **Menu Access Privileges** section, you can select the **Show/Hide** option to choose the required options (for example, Home and Administration tabs) that should be displayed for the Read-Only Administrator.

Step 5 Click **Submit**.
The custom menu access permission is displayed in the **Permissions** drop-down correspoinding to the Read-Only Admin Policy displayed in the Administration > System > Admin Access > Authorization > Policy page.

Step 6 Navigate to the **Administration > System > Admin Access > Authorization > RBAC Policy** page.

Step 7 Click the **Permissions** drop-down corresponding to the **Read-Only Admin Policy**.

Step 8 Select a default (MnT Admin Menu Access) or custom menu access permission (MyMenu) that you have created in the **Administration > System > Admin Access > Authorization > Permissions > Menu Access** page.

Step 9 Click **Save**.

You will encounter an error if you choose Data Access permissions for the Read-Only Admin policy.

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