Administrative Access to Cisco ISE Using an External Identity Store

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

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

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

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

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

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

- External Authentication and Authorization, on page 2
- Configure Admin Access Using an External Identity Store for Authentication with Internal Authorization, on page 4
- External Identity Sources, on page 5

External Authentication and Authorization

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

To configure external authentication, you must:

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

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.

Configure a Password-Based Authentication Using an External Identity Store

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

Step 1

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

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

Step 4 Click **Save**.

Create an External Administrator Group

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

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

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

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

Step 2 Click **Add**.

Step 3 Enter a name and optional description.

Step 4 Click **External**.

If you have connected and joined to an Active Directory domain, your Active Directory instance name appears in the **Name** field.

Step 5 From the **External Groups** drop-down list box, choose the Active Directory group that you want to map for this external administrator group.

Click the "+" sign to map additional Active Directory groups to this external administrator group.

Step 6 Click **Save**.

Create an Internal Read-Only Admin

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

Step 2 Click **Add** and select **Create An Admin User**.

Step 3 Check the **Read Only** check box to create a Read-Only administrator.

Map External Groups to the Read-Only Admin Group

Step 1 Choose **Administration** > **Identity Management** > **External Identity Sources** to configure the external authentication source.

Step 2 Click the required external identity source, such as Active Directory or LDAP, and then retrieve the groups from the selected identity source.

Step 3 Choose **Administration** > **System** > **Admin Access** > **Authentication** to map the authentication method for the admin access with the identity source.

Step 4 Choose **Administration** > **System** > **Admin Access** > **Administrators** > **Admin Groups** and select **Read Only Admin** group.

Step 5 Check the **External** check box and select the required external groups for whom you intend to provide read-only privileges.

Step 6 Click **Save**.

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

Configure Menu Access and Data Access Permissions for External Administrator Group

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

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

Step 2 Click one of the following:

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

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

Step 4 Click **Save**.

Create an RBAC Policy for External Administrator Authentication

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

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

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

Step 2 Specify the rule name, external administrator group, and permissions.

Remember that the appropriate external administrator group must be assigned to the correct administrator user IDs. Ensure that the administrator is associated with the correct external administrator group.

Step 3 Click **Save**.

If you log in as an administrator, and the Cisco ISE RBAC policy is not able to authenticate your administrator identity, Cisco ISE displays an “unauthenticated” message, and you cannot access the Admin portal.

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

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

addition, there are two important factors to remember that are different from external authentication and authorization:

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

Step 1

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

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

Step 3 Click **Save**.

External Authentication Process Flow

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

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

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

External Identity Sources

These windows enable you to configure and manage external identity sources that contain user data that Cisco ISE uses for authentication and authorization.

LDAP Identity Source Settings

LDAP General Settings

The following table describes the fields in the **General** tab.

Table 1: LDAP General Settings

Field Name	Usage Guidelines
Name	Enter a name for the LDAP instance. This value is used in searches to obtain the subject DN and attributes. The value is of type string and the maximum length is 64 characters.
Description	Enter a description for the LDAP instance. This value is of type string, and has a maximum length of 1024 characters.
Schema	You can choose any one of the following built-in schema types or create a custom schema: • Active Directory • Sun Directory Server • Novell eDirectory You can click the arrow next to Schema to view the schema details. If you edit the attributes of the predefined schema, Cisco ISE automatically creates a Custom schema.
Note The following fields can be edited only when you choose the Custom schema.	
Subject Objectclass	Enter a value to be used in searches to obtain the subject DN and attributes. The value is of type string and the maximum length is 256 characters.
Subject Name Attribute	Enter the name of the attribute containing the username in the request. The value is of type string and the maximum length is 256 characters. **Note** The subject name attributes that are configured should be an indexed one in the external ID store.
Group Name Attribute	• CN: To retrieve the LDAP Identity Store Groups based on Common Name. • DN: To retrieve the LDAP Identity Store Groups based on Distinguished Name.
Certificate Attribute	Enter the attribute that contains the certificate definitions. For certificate-based authentication, these definitions are used to validate certificates that are presented by clients.
Group Objectclass	Enter a value to be used in searches to specify the objects that are recognized as groups. The value is of type string and the maximum length is 256 characters.
Group Map Attribute	Specifies the attribute that contains the mapping information. This attribute can be a user or group attribute based on the reference direction that is chosen.
Subject Objects Contain Reference To Groups	Click this option if the subject objects contain an attribute that specifies the group to which they belong.

Field Name	Usage Guidelines
Group Objects Contain Reference To Subjects	Click this option if the group objects contain an attribute that specifies the subject. This value is the default value.
Subjects in Groups Are Stored in Member Attribute As	(Only available when you enable the **Group Objects Contain Reference To Subjects** option) Specifies how members are sourced in the group member attribute and defaults to the DN.
User Info Attributes	By default, predefined attributes are used to collect user information (such as, first name, last name, email, telephone, locality, and so on) for the following built-in schema types: • Active Directory • Sun Directory Server • Novell eDirectory If you edit the attributes of the predefined schema, Cisco ISE automatically creates a Custom schema. You can also select the Custom option from the Schema drop-down list to edit the user information attributes based on your requirements.

Note The subject name attributes that are configured should be an indexed one in the external ID store.

LDAP Connection Settings

The following table describes the fields in the **Connection Settings** tab.

Table 2: LDAP Connection Settings

Field Name	Usage Guidelines
Enable Secondary Server	Check this option to enable the secondary LDAP server to be used as a backup if the primary LDAP server fails. If you check this check box, you must enter configuration parameters for the secondary LDAP server.
Primary and Secondary Servers	
Hostname/IP	Enter the IP address or DNS name of the machine that is running the LDAP software. The hostname can contain from 1 to 256 characters or a valid IP address expressed as a string. The only valid characters for hostnames are alphanumeric characters (a to z, A to Z, 0 to 9), the dot (.), and the hyphen (-).
Port	Enter the TCP/IP port number on which the LDAP server is listening. Valid values are from 1 to 65,535. The default is 389, as stated in the LDAP specification. If you do not know the port number, you can find this information from the LDAP server administrator.

Field Name	Usage Guidelines
Specify server for each ISE node	Check this check box to configure primary and secondary LDAP server hostnames/IP and their ports for each PSN. When this option is enabled, a table listing all the nodes in the deployment is displayed. You need to select the node and configure the primary and secondary LDAP server hostname/IP and their ports for the selected node.
Access	**Anonymous Access**: Click to ensure that searches on the LDAP directory occur anonymously. The server does not distinguish who the client is and will allow the client read access to any data that is configured as accessible to any unauthenticated client. In the absence of a specific policy permitting authentication information to be sent to a server, a client should use an anonymous connection. **Authenticated Access**: Click to ensure that searches on the LDAP directory occur with administrative credentials. If so, enter information for the Admin DN and Password fields.
Admin DN	Enter the DN of the administrator. The Admin DN is the LDAP account that has permission to search all required users under the User Directory Subtree and to search groups. If the administrator specified does not have permission to see the group name attribute in searches, group mapping fails for users who are authenticated by that LDAP server.
Password	Enter the LDAP administrator account password.
Secure Authentication	Click to use SSL to encrypt communication between Cisco ISE and the primary LDAP server. Verify that the Port field contains the port number used for SSL on the LDAP server. If you enable this option, you must choose a root CA.
LDAP Server Root CA	Choose a trusted root certificate authority from the drop-down list to enable secure authentication with a certificate.
Server Timeout	Enter the number of seconds that Cisco ISE waits for a response from the primary LDAP server before determining that the connection or authentication with that server has failed. Valid values are 1 to 99. The default is 10.
Max. Admin Connections	Enter the maximum number of concurrent connections (greater than 0) with LDAP administrator account permissions that can run for a specific LDAP configuration. These connections are used to search the directory for users and groups under the User Directory Subtree and the Group Directory Subtree. Valid values are 1 to 99. The default is 20.
Force reconnect every N seconds	Check this check box and enter the desired value in the **Seconds** field to force the server to renew LDAP connection at the specified time interval. The valid range is from 1 to 60 minutes.
Test Bind to Server	Click to test and ensure that the LDAP server details and credentials can successfully bind. If the test fails, edit your LDAP server details and retest.
Failover	

Field Name	Usage Guidelines
Always Access Primary Server First	Click this option if you want Cisco ISE to always access the primary LDAP server first for authentications and authorizations.
Failback to Primary Server After	If the primary LDAP server that Cisco ISE attempts to contact cannot be reached, Cisco ISE attempts to contact the secondary LDAP server. If you want Cisco ISE to use the primary LDAP server again, click this option and enter a value in the text box.

LDAP Directory Organization Settings

The following table describes the fields in the **Directory Organization** tab.

Table 3: LDAP Directory Organization Settings

Field Name	Usage Guidelines
Subject Search Base	Enter the DN for the subtree that contains all subjects. For example: o=corporation.com If the tree containing subjects is the base DN, enter: o=corporation.com or dc=corporation,dc=com as applicable to your LDAP configuration. For more information, refer to your LDAP database documentation.
Group Search Base	Enter the DN for the subtree that contains all groups. For example: ou=organizational unit, ou=next organizational unit, o=corporation.com If the tree containing groups is the base DN, type: o=corporation.com or dc=corporation,dc=com as applicable to your LDAP configuration. For more information, refer to your LDAP database documentation.

Field Name	Usage Guidelines
Search for MAC Address in Format	Enter a MAC Address format for Cisco ISE to use for search in the LDAP database. MAC addresses in internal identity sources are sourced in the format xx-xx-xx-xx-xx-xx. MAC addresses in LDAP databases can be sourced in different formats. However, when Cisco ISE receives a host lookup request, Cisco ISE converts the MAC address from the internal format to the format that is specified in this field. Use the drop-down list to enable searching for MAC addresses in a specific format, where <*format*> can be any one of the following: • xxxx.xxxx.xxxx • xxxxxxxxxxxx • xx-xx-xx-xx-xx-xx • xx:xx:xx:xx:xx:xx The format you choose must match the format of the MAC address sourced in the LDAP server.
Strip Start of Subject Name Up To the Last Occurrence of the Separator	Enter the appropriate text to remove domain prefixes from usernames. If Cisco ISE finds the delimiter character that is specified in this field in the username, it strips all characters from the beginning of the username through the delimiter character. If the username contains more than one of the characters that are specified in the <start_string> box, Cisco ISE strips characters through the last occurrence of the delimiter character. For example, if the delimiter character is the backslash (\) and the username is DOMAIN\user1, Cisco ISE submits user1 to an LDAP server. **Note** The <start_string> cannot contain the following special characters: the pound sign (#), the question mark (?), the quotation mark (“), the asterisk (*), the right angle bracket (>), and the left angle bracket (<). Cisco ISE does not allow these characters in usernames.
Strip End of Subject Name from the First Occurrence of the Separator	Enter the appropriate text to remove domain suffixes from usernames. If Cisco ISE finds the delimiter character that is specified in this field in the username, it strips all characters from the delimiter character through the end of the username. If the username contains more than one of the characters that are specified in this field, Cisco ISE strips characters starting with the first occurrence of the delimiter character. For example, if the delimiter character is @ and the username is *user1@domain*, then Cisco ISE submits *user1* to the LDAP server. **Note** The <*end_string*> box cannot contain the following special characters: the pound sign (#), the question mark (?), the quotation mark ("), the asterisk (*), the right angle bracket (>), and the left angle bracket (<). Cisco ISE does not allow these characters in usernames.

LDAP Group Settings

Table 4: LDAP Group Settings

Field Name	Usage Guidelines
Add	Choose **Add > Add Group** to add a new group or choose **Add > Select Groups From Directory** to select the groups from the LDAP directory. If you choose to add a group, enter a name for the new group. If you are selecting from the directory, enter the filter criteria, and click **Retrieve Groups**. Check the check boxes next to the groups that you want to select and click **OK**. The groups that you have selected will appear in the **Groups** window.

LDAP Attribute Settings

Table 5: LDAP Attribute Settings

Field Name	Usage Guidelines
Add	Choose **Add > Add Attribute** to add a new attribute or choose **Add > Select Attributes From Directory** to select attributes from the LDAP server. If you choose to add an attribute, enter a name for the new attribute. If you are selecting from the directory, enter the username and click **Retrieve Attributes** to retrieve the attributes. Check the check boxes next to the attributes that you want to select, and then click OK.

LDAP Advanced Settings

The following table describes the field in the Advanced Settings tab.

Table 6: LDAP Advanced Settings

Field Name	Usage Guidelines
Enable Password Change	Check this check box to enable the user to change the password in case of password expiry or password reset while using PAP protocol for device admin and RADIUS EAP-GTC protocol for network access. User authentication fails for the unsupported protocols. This option also enables the user to change the password on their next login.

Related Topics

LDAP Directory Service
LDAP User Authentication
LDAP User Lookup
Add LDAP Identity Sources

RADIUS Token Identity Sources Settings

Related Topics

RADIUS Token Identity Sources

Add a RADIUS Token Server

RSA SecurID Identity Source Settings

RSA Prompt Settings

The following table describes the fields in the **RSA Prompts** tab.

Table 7: RSA Prompt Settings

Field Name	Usage Guidelines
Enter Passcode Prompt	Enter a text string to obtain the passcode.
Enter Next Token Code	Enter a text string to request the next token.
Choose PIN Type	Enter a text string to request the PIN type.
Accept System PIN	Enter a text string to accept the system-generated PIN.
Enter Alphanumeric PIN	Enter a text string to request an alphanumeric PIN.
Enter Numeric PIN	Enter a text string to request a numeric PIN.
Re-enter PIN	Enter a text string to request the user to re-enter the PIN.

RSA Message Settings

The following table describes the fields in the **RSA Messages** tab.

Table 8: RSA Messages Settings

Field Name	Usage Guidelines
Display System PIN Message	Enter a text string to label the system PIN message.
Display System PIN Reminder	Enter a text string to inform the user to remember the new PIN.
Must Enter Numeric Error	Enter a message that instructs users to enter only numbers for the PIN.
Must Enter Alpha Error	Enter a message that instructs users to enter only alphanumeric characters for PINs.
PIN Accepted Message	Enter a message that the users see when their PIN is accepted by the system.

Field Name	Usage Guidelines
PIN Rejected Message	Enter a message that the users see when the system rejects their PIN.
User Pins Differ Error	Enter a message that the users see when they enter an incorrect PIN.
System PIN Accepted Message	Enter a message that the users see when the system accepts their PIN.
Bad Password Length Error	Enter a message that the users see when the PIN that they specify does not fall within the range specified in the PIN length policy.

Related Topics

RSA Identity Sources
Cisco ISE and RSA SecurID Server Integration
Add RSA Identity Sources