CHAPTER 5

Managing External Identity Sources

The Cisco Identity Services Engine integrates with external identity sources to validate credentials in user authentication functions, and to retrieve group information and other attributes that are associated with the user for use in authorization policies. You must configure the external identity source that contains your user information in Cisco ISE. External identity sources also include certificate information for the Cisco ISE server and certificate authentication profiles.

Both internal and external identity sources can be used as the authentication source for sponsor authentication and also for authentication of remote guest users.

Table 5-1 lists the identity sources and the protocols that they support.

Table 5-1 Protocol Versus Database Support

Protocol (Authentication Type)	Internal Database	Active Directory	LDAP[1]	RADIUS Token Server or RSA
EAP-GTC[2], PAP[3] (plain text password)	Yes	Yes	Yes	Yes
MS-CHAP[4] password hash: MSCHAPv1/v2[5] EAP-MSCHAPv2[6] LEAP[7]	Yes	Yes	No	No
EAP-MD5[8] CHAP[9]	Yes	No	No	No
EAP-TLS[10] PEAP-TLS[11] (certificate retrieval) **Note** For TLS authentications (EAP-TLS and PEAP-TLS), identity sources are not required, but are optional and can be added for authorization policy conditions.	No	Yes	Yes	No

1. LDAP = Lightweight Directory Access Protocol.
2. EAP-GTC = Extensible Authentication Protocol-Generic Token Card
3. PAP = Password Authentication Protocol
4. MS-CHAP = Microsoft Challenge Handshake Authentication Protocol

5. MS-CHAPv1/v2 = Microsoft Challenge Handshake Authentication Protocol Version 1/Version 2
6. EAP-MSCHAPv2 = Extensible Authentication Protocol-Microsoft Challenge Handshake Authentication Protocol Version 2
7. LEAP = Lightweight Extensible Authentication Protocol
8. EAP-MD5 = Extensible Authentication Protocol-Message Digest 5
9. CHAP = Challenge-Handshake Authentication Protocol
10. EAP-TLS = Extensible Authentication Protocol-Transport Layer Security
11. PEAP-TLS = Protected Extensible Authentication Protocol-Transport Layer Security

This chapter describes how you can configure the following identity sources and certificate authentication profiles in Cisco ISE and contains the following topics:

Certificate Authentication Profiles

Certificate authentication profiles are used in authentication policies for certificate-based authentications in place of identity sources to verify the authenticity of the user. The certificate authentication profiles allow you to specify the following items:

- The certificate field that should be used as the principal username
- Whether a binary comparison of the certificate should be performed

The Certificate Authentication Profiles page lists the certificate authentication profiles that you have added.

For more information:

Adding or Editing a Certificate Authentication Profile, page 5-2

Adding or Editing a Certificate Authentication Profile

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 one of the following roles assigned: Super Admin or System Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To add or edit a certificate authentication profile, complete the following steps:

Step 1 Choose **Administration > Identity Management > External Identity Sources**.

Step 2 From the External Identity Sources navigation pane on the left, click **Certificate Authentication Profile**.

The Certificate Authentication Profile page appears.

Step 3 Do one of the following:

- To add a new certificate authentication profile, click **Add**.
- To edit an existing certificate authentication profile, choose the profile that you want to edit, and click **Edit**.
- To create a duplicate of an existing certificate authentication profile, choose the profile that you want to duplicate, and click **Duplicate**.

Step 4 Enter the following details:

- Name—(Required) Enter the name of the certificate authentication profile.
- Description—Enter a description of the certificate authentication profile.
- Principal Username X509 Attribute—The available list of principal username attributes for X.509 certificate includes the following selections:
  - Common Name
  - Subject Alternative Name
  - Subject Serial Number
  - Subject
  - Subject Alternative Name—Other Name
  - Subject Alternative Name—Email
  - Subject Alternative Name—DNS

Note When performing authentication via Anyconnect 3.1, you must specify the Subject Alternative Name for Microsoft certificates when using the EAP-FAST protocol with client certificate authentication. You need to specify the Common Name whenever you use certificates issued by other Certificate Authorities.

- Perform Binary Certificate Comparison with Certificate Retrieved from LDAP or Active Directory—Check this check box if you want to validate certificate information for authentication against a selected LDAP or Active Directory identity source.

  If you check this check box, you must choose the LDAP or Active Directory identity source from the available list.
- LDAP/Active Directory Instance Name—Choose the LDAP or Active Directory identity source against which you want to validate the certificate information for authentication.

Step 5 Click **Submit** to add the certificate authentication profile or save the changes.

Next Steps:

1. See Chapter 16, "Managing Authentication Policies" for information on how to create authentication policies.
2. See Chapter 17, "Managing Authorization Policies and Profiles" for information on how to create authorization profiles and policies.

Microsoft Active Directory

Cisco ISE uses Active Directory as an external identity source to access resources such as users, machines, groups, and attributes. You can configure Cisco ISE to authenticate users and machines. This section contains the following topics:

Note Cisco ISE does not support Microsoft Active Directory Servers that reside behind a network address translator and have a Network Address Translation (NAT) address.

Key Features of the Integration of Cisco ISE and Active Directory

Supported Authentication Protocols

- Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) and Protected Extensible Authentication Protocol (PEAP)—Cisco ISE supports user and machine authentication and change password against Active Directory using EAP-FAST and PEAP with an inner method of Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAPv2) and Extensible Authentication Protocol-Generic Token Card (EAP-GTC).
- Password Authentication Protocol (PAP)—Cisco ISE supports authenticating against Active Directory using PAP and also allows you to change Active Directory user passwords.
- Microsoft Challenge Handshake Authentication Protocol version 1 (MS-CHAPv1)—Cisco ISE supports user and machine authentication against Active Directory using MS-CHAPv1.
- MS-CHAPv2—Cisco ISE supports user and machine authentication against Active Directory using EAP-MSCHAPv2.
- EAP-GTC—Cisco ISE supports user and machine authentication against Active Directory using EAP-GTC.
- Extensible Authentication Protocol-Transport Layer Security (EAP-TLS)—Cisco ISE uses the certificate retrieval option to support user and machine authentication against Active Directory using EAP-TLS.
- Protected Extensible Authentication Protocol-Transport Layer Security (PEAP-TLS)—Cisco ISE supports user and machine authentication against Active Directory using PEAP-TLS.
- LEAP—Cisco ISE supports user authentication against Active Directory using LEAP.

Refer to the *Release Notes for Cisco Identity Services Engine, Release 1.1.x* for a list of Windows Server Operating Systems that support Active Directory services.

Directory Service

Active Directory is a directory service that allows for central administration and management of user accounts, clients, and servers. Active Directory can interoperate with other directory services such as Lightweight Directory Access Protocol (LDAP) and is mostly used in distributed networking environments.

User Authentication

User authentication provides network access to only those users who are listed in Active Directory.

Machine Authentication

Machine authentication provides access to network services to only those devices that are listed in Active Directory.

Attribute Retrieval for Authorization

You can configure Cisco ISE to retrieve user or machine Active Directory attributes to be used in authorization rules. The attributes are mapped to the Cisco ISE policy results and determine the authorization level for the user or machine. Cisco ISE retrieves user and machine Active Directory attributes after a successful user or machine authentication and can also retrieve the attributes for an authorization that is independent of authentication.

Group Retrieval for Authorization

Cisco ISE can retrieve user or machine groups from Active Directory after a successful authentication. Cisco ISE can also retrieve the user or machine group that is independent of authentication for authorization. You can use the Active Directory group data for authorization and introduce special conditions to match them against the retrieved groups.

Certificate Retrieval for EAP-TLS Authentication

Cisco ISE supports certificate retrieval for user or machine authentication that uses the EAP-TLS protocol. The user or machine record on Active Directory includes a certificate attribute of the binary data type. This certificate attribute can contain one or more certificates. Cisco ISE identifies this attribute as userCertificate and does not allow you to configure any other name for this attribute. Cisco ISE retrieves this certificate and uses it to verify the identity of the user or machine. The certificate authentication profile determines the field to be used for retrieving the certificates. For example, Subject Alternative Name (SAN), Common Name, or Social Security Number (SSN). After Cisco ISE retrieves the certificate, it performs a binary comparison of this certificate with the client certificate. When multiple certificates are received, Cisco ISE compares the certificates to check for one that matches. When a match is found, Cisco ISE grants the user or machine access to the network.

For EAP-TLS to perform machine authentication, it is required to use binary certificate comparison: **Administration > External Identity Sources > Certificate authenticatoin profiles > Pick a profile >** “Perform Binary Certificate Comparison with Certificate retrieved from LDAP or Active Directory” needs to be checked. Also, a certificate needs to be present in that AD or LDAP.

User Access Restriction

While authenticating or querying a user, Cisco ISE checks for the following:

- Is the user account disabled?
- Is the user locked out?
- Has the user account expired?
- Is the query run outside of the specified login hours?

If the user has one of these limitations, the *Active Directory Identifier*::IdentityAccessRestricted attribute on the Active Directory dictionary is set to indicate that the user has restricted access. You can use this attribute in all policy rules.

Active Directory identifier is the name that you enter for the Active Directory identity source.

Support for Multidomain Forests

Cisco ISE supports multidomain forests. Cisco ISE connects to a single domain, but can access resources from the other domains in the Active Directory forest if trust relationships are established between the domain to which Cisco ISE is connected and the other domains.

For more information:

- Dictionaries and Dictionary Attributes, page 7-1
- Integrating Cisco ISE with Active Directory, page 5-6

Integrating Cisco ISE with Active Directory

Prerequisites:

Before you connect your Cisco ISE server with the Active Directory domain, you must check the following:

- Ensure that Cisco ISE hostnames are only 15 characters or less in length. Active Directory does not validate hostnames larger than 15 characters, which can cause a problem if you have multiple Cisco ISE hosts in your deployment whose hostnames are identical through the first 15 characters and only distinguished from one another by trailing digits or other identifiers.
- Ensure that your Cisco ISE server and Active Directory are time synchronized. Time in the Cisco ISE is set according to the Network Time Protocol (NTP) server. We recommend that you use the NTP to synchronize time between the Cisco ISE and Active Directory. For more information on NTP server settings, see the "System Time and NTP Server Settings" section on page 8-18.

  Refer to the *Cisco Identity Services Engine CLI Reference Guide, Release 1.1.x* for information on how to configure the NTP server settings from the CLI.
- If there is a firewall between Cisco ISE and Active Directory, certain ports need to be opened to allow Cisco ISE to communicate with Active Directory. Ensure that the following default ports are open:

Protocol	Port Number
LDAP	389 (UDP)
SMB[1]	445 (TCP)
KDC[2]	88 (TCP)

Protocol	Port Number
Global Catalog	3268 (TCP), 3269
KPASS	464 (TCP)
NTP	123 (UDP)
LDAP	389 (TCP)
LDAPS[3]	636 (TCP)

1. SMB = Server Message Block
2. KDC = key distribution center
3. LDAPS = Lightweight Directory Access Protocol over TLS/SSL

- If your Active Directory source has a multidomain forest, ensure that trust relationships exist between the domain to which Cisco ISE is connected and the other domains with resources to which you need access. For more information on establishing trust relationships, refer to the *Microsoft Active Directory documentation*.
- The DNS server that is configured in Cisco ISE using the **ip name-server** command should be able to resolve the domain names in your Active Directory identity source. Typically, the DNS server that is part of the Active Directory deployment is configured in Cisco ISE. If you have to configure multiple DNS servers you can use the **application configure ise** command to do so. Refer to the *Cisco Identity Services Engine CLI Reference Guide, Release 1.1.x* for more information on usage of the command.
- There must be at least one global catalog server operational in the domain to which Cisco ISE is to be joined.
- The Active Directory username that you provide while joining to an Active Directory domain should be predefined in Active Directory and should have the permission to create and update for computer account objects and change password in the domain you are joining.

Note If your Active Directory domain has subdomains and the user belongs to one of the subdomains, then, the username should also include the subdomain name. For example, for a domain abc.com, if there are two subdomains sub1 and sub2, and the user belongs to sub1, then the username should be sub1\user1.

- Every Cisco ISE administrator account is assigned one or more administrative roles. To perform the operations that are described in the following procedures, you must have one of the following roles assigned: Super Admin or System Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges that are associated with each role.
- Ensure that your Microsoft Active Directory Server does not reside behind a network address translator and does not have a Network Address Translation (NAT) address.
- Ensure that the Microsoft Active Directory administrator account is valid, which is used for the join operation, and it is not configured with Change Password on Next Login state.

Note Sometimes, the status is indicated as “Connected” when Cisco ISE is joined and has a connection established to Active Directory. However, even when Cisco ISE is connected, there may still be issues in operation. To identify such issues, refer to the Authentication Report under **Operations > Reports**.

This section contains the following topics:

Connecting to the Active Directory Domain

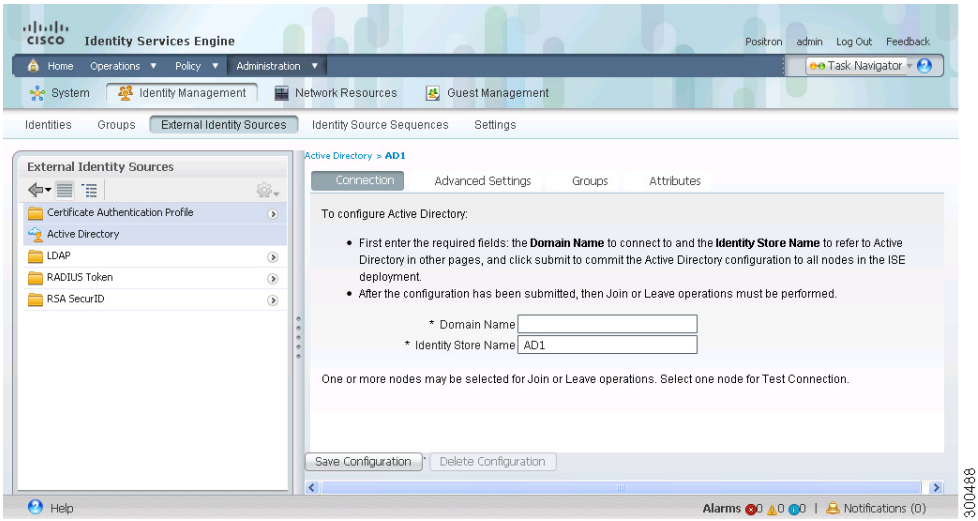
To connect to an Active Directory domain, complete the following steps:

Step 1 Choose **Administration > Identity Management > External Identity Sources**.

Step 2 From the External Identity Sources navigation pane on the left, click **Active Directory**.

The Active Directory pages appear as shown in Figure 5-1.

Figure 5-1 Active Directory Connections Page



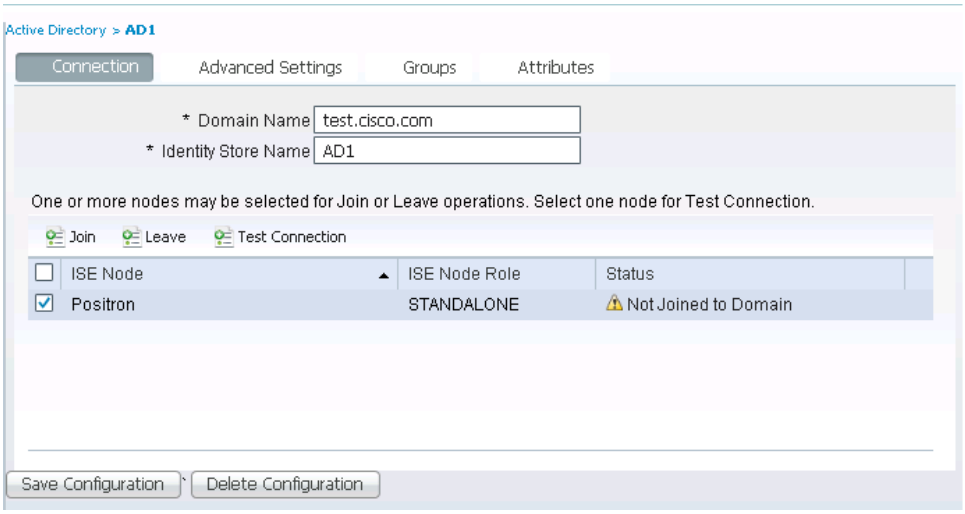
Step 3 Enter the domain name in the Domain Name text box.

Step 4 Enter a friendly name in the Identity Store Name text box for your Active Directory identity source (by default, this value will be AD1).

Step 5 Click **Save Configuration**.

After you successfully submit with a domain name, the deployment join/leave table is displayed with all the Cisco ISE nodes, node roles, and their status, as shown in Figure 5-2.

Figure 5-2 Active Directory Nodes Table



Saving the configuration saves the Active Directory domain configuration globally (in the primary as well as the secondary policy service nodes), but none of the Cisco ISE nodes are joined to the domain.

Note Even though you submitted the configuration in Step 4, you have to explicitly click **Join** to connect your Cisco ISE node to the Active Directory domain. You must manually perform the join operation for each of the secondary policy service nodes in your deployment for them to be connected to the Active Directory domain.

Step 6 To verify if your Cisco ISE node can be connected to the Active Directory domain, check the check box next to the Cisco ISE node and click **Test Connection**. A dialog box appears and prompts you to enter the Active Directory username and password.

Step 7 Enter the Active Directory username and password, and click **OK**.

Note If your Active Directory domain has subdomains and the user belongs to one of the subdomains, then, the username should also include the subdomain name. For example, for a domain abc.com, if there are two subdomains sub1 and sub2, and the user belongs to sub1, then the username should be sub1\user1.

A dialog box appears with the status of the test connection operation.

Step 8 Click **OK**.

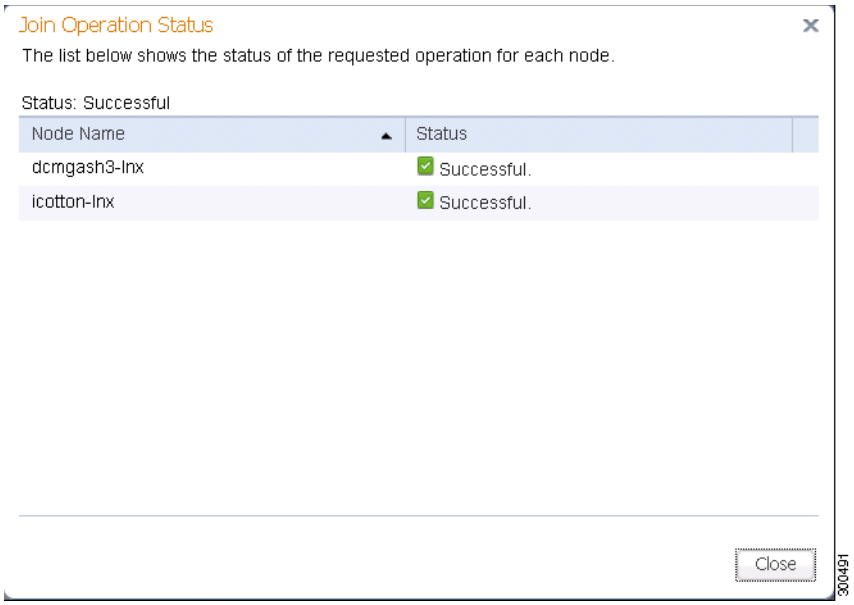
Step 9 To join the Cisco ISE node to the Active Directory domain, check the check box next to the Cisco ISE node and click **Join**.

The Join Domain dialog box appears.

Step 10 Enter your Active Directory username and password, and click **OK**.

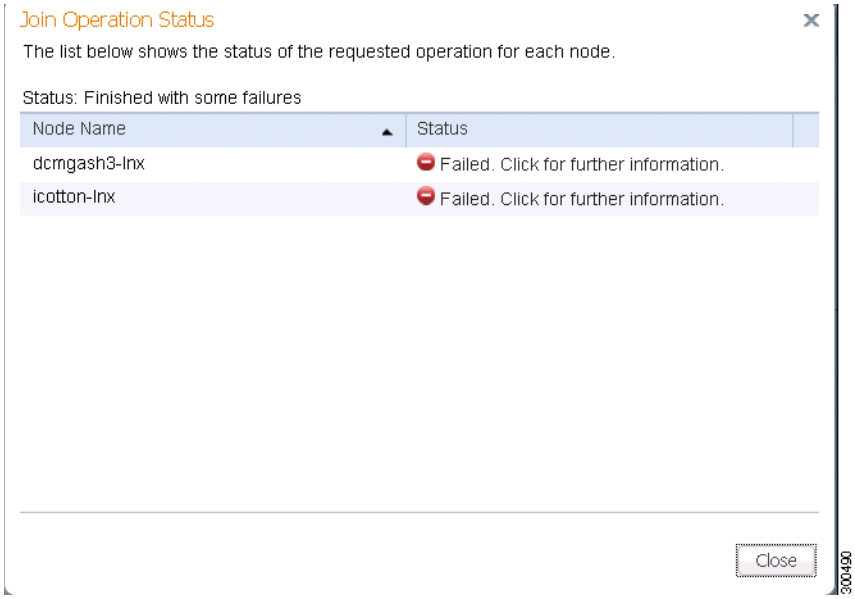
You can select more than one node to join to the Active Directory domain. After you join, a pop-up list is displayed showing the progress of the request for each node. After the operation is completed successfully, each node is marked as such. (Figure 5-3)

Figure 5-3 Success Message Displayed After Active Directory Domain Join



If the join operation is not successful, the failure message is displayed in the pop-up list as shown in Figure 5-4. You can click the failure message for each node to view detailed logs for that node (Figure 5-4).

Figure 5-4 Failure Message Displayed for Active Directory Domain Join



Step 11 Click **Close**.

Configuring Active Directory Advanced Settings

To configure Active Directory Advanced Settings, complete the following steps:

Step 1 Choose **Administration > Identity Management > External Identity Sources**.

Step 2 From the External Identity Sources navigation pane on the left, click **Active Directory**.

Step 3 Click the **Advanced Settings** tab.

Step 4 Check the **Enable Password Change** check box to allow the user to change the password.

Step 5 Check the **Enable Machine Authentication** check box to allow machine authentication.

Step 6 Check the **Enable Machine Access Restrictions (MARs)** check box to ensure that the machine authentication results are tied to the user authentication and authorization results. If you check this check box, you must enter the Aging Time in hours.

Step 7 Enter the Aging Time in hours if you have enabled MARs.

This value specifies the expiration time for machine authentication. If the time expires, the user authentication fails. For example, if you have enabled MARs and enter a value of 2 hours, the user authentication fails if the user tries to authenticate after 2 hours.

Step 8 Click **Save Configuration**.

Next Steps:

1. Configuring Active Directory Groups, page 5-11
2. Configuring Active Directory Attributes, page 5-12

Configuring Active Directory Groups

To configure Active Directory groups that will be available for use in authorization policy conditions, complete the following steps:

Step 1 Choose **Administration > Identity Management > External Identity Sources**.

Step 2 From the External Identity Sources navigation pane on the left, click **Active Directory**.

Step 3 Ensure that your Cisco ISE server is joined to the Active Directory domain. See Connecting to the Active Directory Domain, page 5-8 for information.

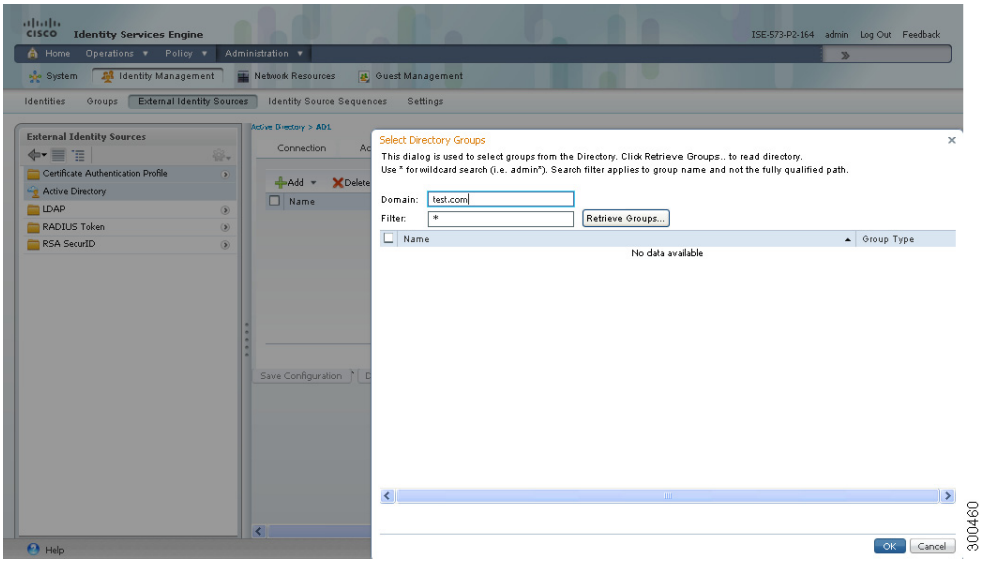
Step 4 Click the **Groups** tab.

The Groups page appears. The groups that you configure in this page will be available for use in policy conditions.

Step 5 Choose **Add > Add Group** to add a new group or choose **Add > Select Groups From Directory** to choose an existing group.

- If you choose to add groups, enter a name for a new group.
- If you want to choose groups from the directory, the Select Directory Groups page appears. You can refine your search using the filter. For example, enter **cn=users** as the filter criteria and click **Retrieve Groups** to narrow down user groups that begin with cn=users as shown in Figure 5-5. You can also enter the asterisk (*) wildcard character to filter the results.

Figure 5-5 Active Directory Groups Page



Step 6 Check the check boxes next to the groups that you want to use in policy conditions and rules, and click **OK**.

You will return to the Groups page. The groups that you have selected appear in the Groups page.

a. To remove the group that you do not want to use in your policy conditions and rules, click the radio button next to that group, and click **Delete Group**.

The following message appears:

Are you sure you want to delete?

b. Click **OK** to delete the group.

Next Step:

Configuring Active Directory Attributes, page 5-12

Configuring Active Directory Attributes

To configure Active Directory attributes that will be available for use in authorization policy conditions, complete the following steps:

Step 1 Choose **Administration > Identity Management > External Identity Sources**.

Step 2 From the External Identity Sources navigation pane on the left, click **Active Directory**.

Step 3 Ensure that your Cisco ISE server is joined to the Active Directory domain. See Connecting to the Active Directory Domain, page 5-8 for information.

Step 4 Click the **Attributes** tab to choose the attributes that you want to use in policy conditions.

Step 5 Choose **Add > Add Attribute** to add attributes that you want to use in policy conditions or choose **Add > Select Attributes From Directory** to choose a list of attributes from the directory.

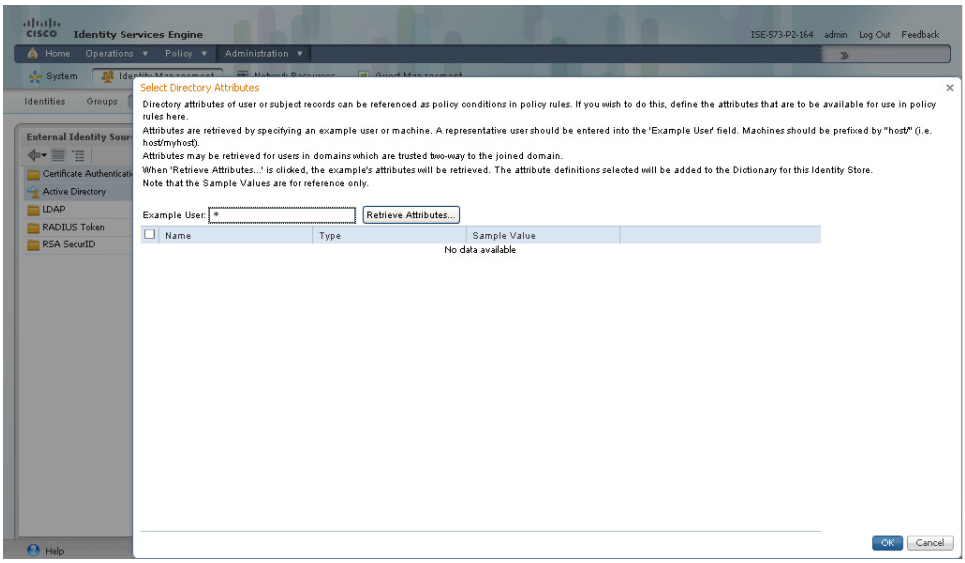
- If you choose to add an attribute, enter a name for a new attribute.

- If you want to choose attributes from directory, the Select Directory Attributes page appears. In the Select Directory Attributes page, enter the name of a user in the Example User field, and click **Retrieve Attributes** to obtain a list of attributes for the user as shown in Figure 5-6. For example, enter **admin** in the Example User field to obtain the list of attributes for administrators. You can also enter the asterisk (*) wildcard character to filter the results.

Note When you choose an example user for obtaining user attributes, ensure that you choose a user from the Active Directory domain to which the Cisco ISE is connected.

Note When you choose an example machine to obtain machine attributes, be sure to prefix the machine name with "host/." For example, you might use host/myhost.

Figure 5-6 Active Directory Attributes Page



Step 6 Check the check boxes next to the attributes from the Active Directory that you want Cisco ISE to use in policy conditions, and click **OK**.

The Attributes page appears. The attributes that you have selected will appear in this page.

To remove any attribute that you do not want to use in policy conditions, click the radio button next to the attribute, and click **Delete Attribute**.

Next Steps:

1. See Chapter 16, "Managing Authentication Policies" for information on how to create authentication policies.
2. See Chapter 17, "Managing Authorization Policies and Profiles" for information on how to create authorization profiles and policies.

Leaving the Active Directory Domain

Note Before you leave the Active Directory domain, ensure that you are not using Active Directory as an identity source in your authentication policies either directly or as part of an identity source sequence. If you leave the Active Domain, but still use Active Directory as an identity source for authentication (either directly or as part of an identity source sequence), it might cause authentications to fail.

To leave the Active Directory domain, complete the following steps:

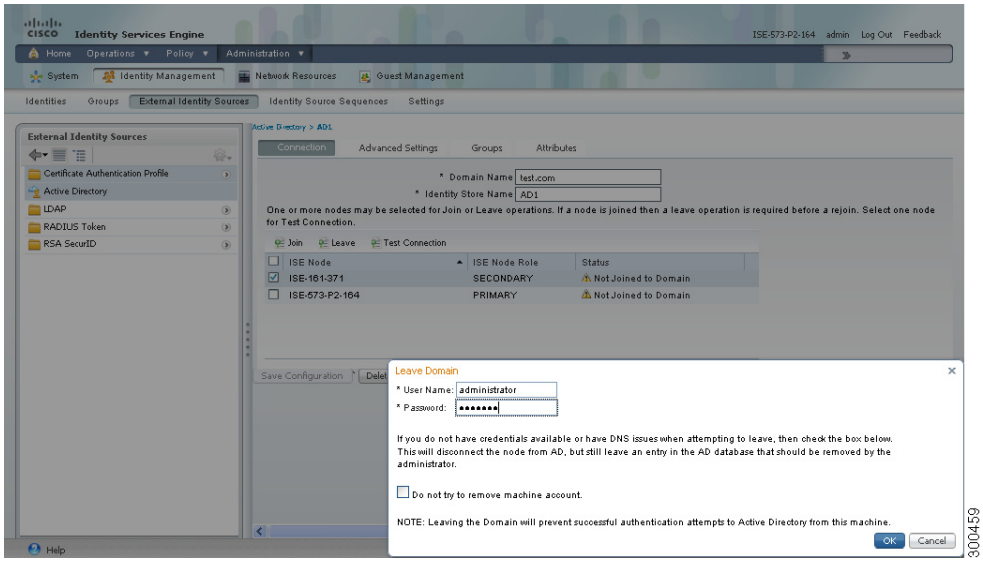
Step 1 Choose **Administration > Identity Management > External Identity Sources**.

Step 2 From the External Identity Sources navigation pane on the left, click **Active Directory**.

Step 3 To leave an Active Directory domain, check the check box next to the Cisco ISE node and click **Leave**.

Step 4 The Leave Domain dialog box appears as shown in Figure 5-7.

Figure 5-7 Leave Domain Dialog Box



Step 5 Enter the Active Directory username and password, and click **OK** to leave the domain and remove the configuration from the Cisco ISE database.

Step 6 If you do not have the Active Directory credentials, check the **No Credentials Available** check box, and click **OK**.

If you check the **No Credentials Available** check box, the primary Cisco ISE node will leave the Active Directory domain. The Active Directory administrator has to manually remove the entry that is made in the Active Directory database that was created during the join.

If you have entered the Active Directory credentials, the Cisco ISE will leave the Active Directory domain and delete the configuration from the Active Directory database.

Note The Active Directory credentials must have Create Computer Objects or Delete Computer Objects permission on the computer where the Cisco ISE account was created.

Deleting Active Directory Configuration

Prerequisites:

1. Before you delete the Active Directory configuration, ensure that you no longer need to connect to Active Directory and that you have left the Active Directory domain.
2. Do not delete the configuration if you want to join another Active Directory domain. You can leave the domain to which you are currently joined and join a new domain. See the Leaving the Active Directory Domain, page 5-14 for more information.

To remove the Active Directory configuration from Cisco ISE, complete the following steps:

Step 1 Choose **Administration > Identity Management > External Identity Sources**.

Step 2 From the External Identity Sources navigation pane on the left, click **Active Directory**.

The Active Directory page appears.

Note Ensure that the Local Node Status is Not Joined to a domain.

Step 3 Click **Delete Configuration**.

You have removed the configuration from the Active Directory database. If you want to use Active Directory at a later point in time, you can resubmit a valid Active Directory configuration.

Enabling Active Directory Debug Logs

Active Directory debug logs are not logged by default. You must enable this option on the Cisco ISE node that has assumed the Policy Service persona in your deployment from which you want to obtain debug information.

To enable Active Directory debug logs, complete the following steps:

Step 1 Choose **Administration > System > Logging**.

Step 2 From the Logging navigation pane on the left, click **Debug Log Configuration**.

The Node List page displays a list of nodes in your deployment.

Step 3 Click the radio button next to the Cisco ISE Policy Service node from which you want to obtain Active Directory debug information, and click **Edit**.

The Debug Level Configuration page appears.

Step 4 Click the **Active Directory** radio button, and click **Edit**.

Step 5 From the drop-down list next to Active Directory, choose DEBUG.

Step 6 Click **Save** to save the logging settings.

The log file is saved in the following location:

/opt/CSCOcpm/logs/ad_agent.log

To download the ad_agent.log file, complete the following steps:

Step 1 Choose **Operations > Troubleshoot > Download Logs**.

Step 2 From the Appliance node list navigation pane, click the node from which you want to obtain the Active Directory debug log file.

Step 3 In the right pane, click the **Debug Logs** tab.

Step 4 Scroll down this page to locate the ad_agent.log file. Click this file to download it.

Supplemental Information

This section provides pointers to help you do the following:

- Configure Group Policy in Active Directory, page 5-16
- Configure Odyssey 5.X Supplicant for EAP-TLS Machine Authentications Against Active Directory, page 5-17
- Configure AnyConnect Agent for Machine Authentication, page 5-17

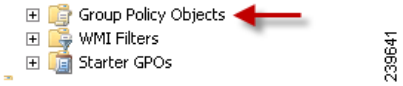
Configure Group Policy in Active Directory

This section provides pointers to set up a group policy for wired services. For more information about how to access the Group Policy management editor, refer to *Microsoft Active Directory Documentation*.

To configure group policy in Active Directory, complete the following steps:

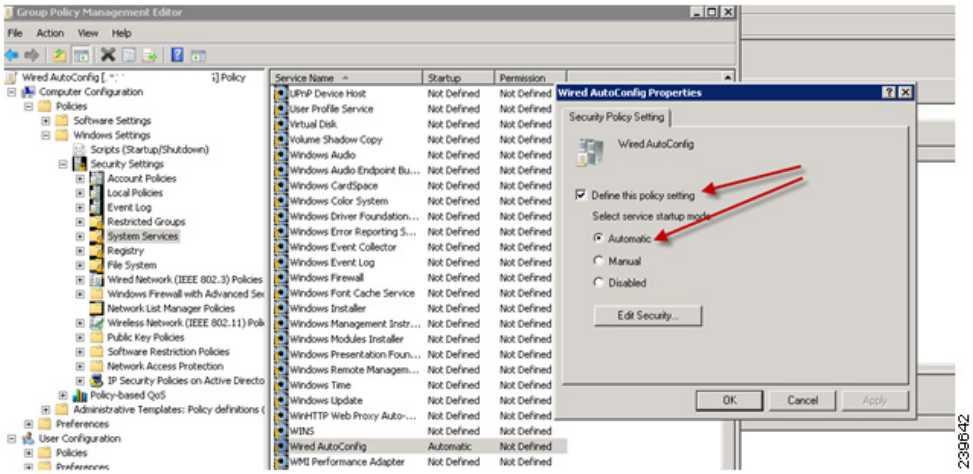
1. Open the Group Policy management editor as shown in Figure 5-8 and create a new policy object or add to an existing domain policy.

Figure 5-8 Group Policy Objects



2. Create a new policy and enter a descriptive name for it. For example, you might use Wired Autoconfiguration.
3. Check the **Define this policy setting** check box, and click the **Automatic** radio button for the service startup mode as shown in Figure 5-9.

Figure 5-9 Policy Properties



4. Apply the policy at the desired organizational unit or domain Active Directory level. The computers will receive the policy when they reboot the next time, and this service will be turned on.

Configure Odyssey 5.X Supplicant for EAP-TLS Machine Authentications Against Active Directory

If you are using the Odyssey 5.x supplicant for EAP-TLS machine authentications against Active Directory, you must configure the following in your Odyssey supplicant.

1. Start your Odyssey Access Client.
2. From the Tools menu, choose **Odyssey Access Client Administrator**.
3. Double-click the **Machine Account** icon.
4. From the Machine Account page, you must configure a profile for EAP-TLS authentications:
   a. Choose **Configuration > Profiles**.
   b. Enter a name for the EAP-TLS profile.
   c. In the Authentication tab, choose **EAP-TLS** as the authentication method.
   d. In the Certificate tab, check the **Permit login using my certificate** check box, and choose a certificate for the supplicant machine.
   e. In the User Info tab, check the **Use machine credentials** check box.

If this option is enabled, the Odyssey supplicant sends the machine name in the format host\<*machine_name*> and Active Directory identifies the request as coming from a machine and will look up computer objects to perform authentication. If this option is disabled, the Odyssey supplicant sends the machine name without the host\ prefix and Active Directory will look up user objects and the authentication will fail.

Configure AnyConnect Agent for Machine Authentication

When you configure AnyConnect Agent for machine authentication, you can do one of the following:

- Use the default machine hostname, which includes the prefix “host/.”

- Configure a new profile, in which case you must include the prefix “host/” and then the machine name.

LDAP

Lightweight Directory Access Protocol (LDAP) is a networking protocol defined by RFC 2251 for querying and modifying directory services that run on TCP/IP. LDAP is a lightweight mechanism for accessing an X.500-based directory server.

Cisco ISE integrates with an LDAP external database, which is also called an identity source, by using the LDAP protocol. See Adding and Editing LDAP Identity Sources, page 5-22 for information about configuring an LDAP identity source.

This section contains the following topics:

Key Features of Integration of Cisco ISE and LDAP

This section contains the following:

Directory Service

The directory service is a software application, or a set of applications, for storing and organizing information about the users and resources of a computer network. You can use the directory service to manage user access to these resources. The LDAP directory service is based on a client-server model. A client starts an LDAP session by connecting to an LDAP server, and sends operation requests to the server. The server then sends its responses. One or more LDAP servers contain data from the LDAP directory tree or the LDAP backend database.

The directory service manages the directory, which is the database that holds the information. Directory services use a distributed model for storing information, and that information is usually replicated between directory servers.

An LDAP directory is organized in a simple tree hierarchy and can be distributed among many servers. Each server can have a replicated version of the total directory, which is synchronized periodically.

An entry in the tree contains a set of attributes, where each attribute has a name (an attribute type or attribute description) and one or more values. The attributes are defined in a schema.

Each entry has a unique identifier: its distinguished name (DN). This name contains the relative distinguished name (RDN), which is constructed from attributes in the entry, followed by the DN of the parent entry. You can think of the DN as a full filename, and the RDN as a relative filename in a folder.

Multiple LDAP Instances

You can create more than one LDAP instance in Cisco ISE. By creating more than one LDAP instance with different IP addresses or port settings, you can configure Cisco ISE to authenticate by using different LDAP servers or different databases on the same LDAP server. Each primary server IP address and port configuration, along with the secondary server IP address and port configuration, forms an LDAP instance that corresponds to one Cisco ISE LDAP identity source instance.

Cisco ISE does not require that each LDAP instance correspond to a unique LDAP database. You can have more than one LDAP instance set to access the same database. This method is useful when your LDAP database contains more than one subtree for users or groups. Because each LDAP instance supports only one subtree directory for users and one subtree directory for groups, you must configure separate LDAP instances for each user directory subtree and group directory subtree combination for which Cisco ISE should submit authentication requests.

Failover

Cisco ISE supports failover between a primary LDAP server and a secondary LDAP server. In the context of LDAP authentication with Cisco ISE, failover applies when an authentication request fails because Cisco ISE could not connect to an LDAP server. Failover can occur when the server is down or is otherwise unreachable by Cisco ISE. To use this feature, you must define the primary and secondary LDAP servers, and you must set failover settings.

If you establish failover settings and if the first LDAP server that Cisco ISE attempts to contact cannot be reached, Cisco ISE always attempts to contact the other LDAP server. The first server that Cisco ISE attempts to contact might not always be the primary LDAP server. Instead, the first LDAP server that Cisco ISE attempts to contact depends on the previous LDAP authentication attempts and on the value that you enter in the Failback Retry Delay text box.

Note Cisco ISE always uses the primary LDAP server to obtain groups and attributes for use in authorization policies from the user interface, so the primary LDAP server must be reachable when you configure these items. Cisco ISE uses the secondary LDAP server only for authentications and authorizations at runtime, according to your failover configuration.

LDAP Connection Management

Cisco ISE supports multiple concurrent LDAP connections. Connections are opened on demand at the time of the first LDAP authentication. The maximum number of connections is configured for each LDAP server. Opening connections in advance shortens the authentication time. You can set the maximum number of connections to use for concurrent binding connections. The number of opened connections can be different for each LDAP server (primary or secondary) and is determined based on the maximum number of administration connections configured for each server.

Cisco ISE retains a list of open LDAP connections (including the binding information) for each LDAP server that is configured in Cisco ISE. During the authentication process, the connection manager attempts to find an open connection from the pool. If an open connection does not exist, a new one is opened.

If the LDAP server closed the connection, the connection manager reports an error during the first call to search the directory, and tries to renew the connection. After the authentication process is complete, the connection manager releases the connection.

User Authentication

LDAP can be used as an external database against which Cisco ISE users authenticate. Cisco ISE supports plain password authentication of users. User authentication includes the following actions:

- Searching the LDAP server for an entry that matches the username in the request
- Checking the user password with the one that is found in the LDAP server
- Retrieving the group membership information of the user for use in policies
- Retrieving values for the attributes that you have specified for use in policies and authorization profiles

To authenticate a user, Cisco ISE sends a bind request to the LDAP server. The bind request contains the DN and password of the user in clear text. A user is authenticated when the DN and password of the user match the username and password in the LDAP directory.

Note We recommend that you protect the connection to the LDAP server using Secure Sockets Layer (SSL).

- Authentication Errors—Cisco ISE logs authentication errors in the Cisco ISE log files.
- Initialization Errors—Use the LDAP server timeout settings to configure the number of seconds that Cisco ISE waits for a response from an LDAP server before determining that the connection or authentication on that server has failed. Possible reasons for an LDAP server to return an initialization error are as follows:
  - LDAP is not supported.
  - The server is down.
  - The server is out of memory.
  - The user has no privileges.
  - Administrator credentials are configured incorrectly.

Authentication Using LDAP

Cisco ISE can authenticate a subject (user or host) against an LDAP identity source by performing a bind operation on the directory server to find and authenticate the subject. After a successful authentication, Cisco ISE can retrieve groups and attributes that belong to the subject whenever they are required. You can configure the attributes to be retrieved in the Cisco ISE user interface by choosing **Administration > Identity Management > External Identity Sources > LDAP**. These groups and attributes can be used by Cisco ISE to authorize the subject.

To authenticate a user or query the LDAP identity source, Cisco ISE connects to the LDAP server and maintains a connection pool. See the "LDAP Connection Management" section on page 5-19.

Binding Errors

Possible reasons for an LDAP server to return binding (authentication) errors include the following:

- Parameter errors—Invalid parameters were entered
- User account is restricted (disabled, locked out, expired, password expired, and so on)

The following errors are logged as external resource errors, indicating a possible problem with the LDAP server:

- A connection error occurred
- The timeout expired
- The server is down
- The server is out of memory

The following error is logged as an Unknown User error:

- A user does not exist in the database

The following error is logged as an Invalid Password error, where the user exists, but the password sent is invalid:

- An invalid password was entered

User Lookup

Cisco ISE supports the user lookup feature with the LDAP server. This feature allows you to search for a user in the LDAP database and retrieve information without authentication. The user lookup process includes the following actions:

- Searching the LDAP server for an entry that matches the username in the request
- Retrieving the group membership information of the user for use in policies
- Retrieving values for the attributes that you have specified for use in policies and authorization profiles

MAC Address Lookup

Cisco ISE supports the MAC address lookup feature. This feature allows you to search for a MAC address in the LDAP database and retrieve information without authentication. The MAC address lookup process includes the following actions:

- Searching the LDAP server for an entry that matches the MAC address of the device
- Retrieving the group information for the device for use in policies
- Retrieving values for the attributes that you have specified for use in policies

Group Membership Information Retrieval

For user authentication, user lookup, and MAC address lookup, Cisco ISE must retrieve the group membership information from LDAP databases. LDAP servers represent the association between a subject (a user or a host) and a group in one of the following two ways:

- Groups Refer to Subjects—The group objects contain an attribute that specifies the subject. Identifiers for subjects can be sourced in the group as the following:
  - Distinguished names
  - Plain usernames

- Subjects Refer to Groups—The subject objects contain an attribute that specifies the group to which they belong.

LDAP identity sources contain the following parameters for group membership information retrieval:

- Reference Direction—This parameter specifies the method to use when determining group membership (either groups to subjects or subjects to groups).
- Group Map Attribute—This parameter indicates which attribute contains the group membership information.
- Group Object Class—This parameter determines that certain objects are recognized as groups.
- Group Search Subtree—This parameter indicates the search base for group searches.
- Member Type Option—This parameter specifies how members are sourced in the group member attribute (either as DNs or plain usernames).

Attributes Retrieval

For user authentication, user lookup, and MAC address lookup, Cisco ISE must retrieve the subject attributes from LDAP databases. For each instance of an LDAP identity source, an identity source dictionary is created. These dictionaries support attributes of the following data types:

- String
- Unsigned integer 32
- IPv4 address

For unsigned integers and IPv4 attributes, Cisco ISE converts the strings that it has retrieved to the corresponding data types. If conversion fails or if no values are retrieved for the attributes, Cisco ISE logs a debug message, but does not fail the authentication or the lookup process.

You can optionally configure default values for the attributes that Cisco ISE can use when the conversion fails or when Cisco ISE does not retrieve any values for the attributes.

Certificate Retrieval

If you have configured certificate retrieval as part of user lookup, then Cisco ISE must retrieve the value of the certificate attribute from LDAP. To retrieve the value of the certificate attribute from LDAP, you must have previously configured the certificate attribute in the list of attributes to be accessed while configuring an LDAP identity source.

For information on how to add LDAP identity sources, see Adding and Editing LDAP Identity Sources, page 5-22.

Adding and Editing LDAP Identity Sources

Prerequisites:

- Every Cisco ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedures, you must have one of the following roles assigned: Super Admin or System Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.
- Cisco ISE always uses the primary LDAP server to obtain groups and attributes for use in authorization policies from the user interface, so the primary LDAP server must be reachable when you configure these items.

To create an LDAP identity source, complete the following steps:

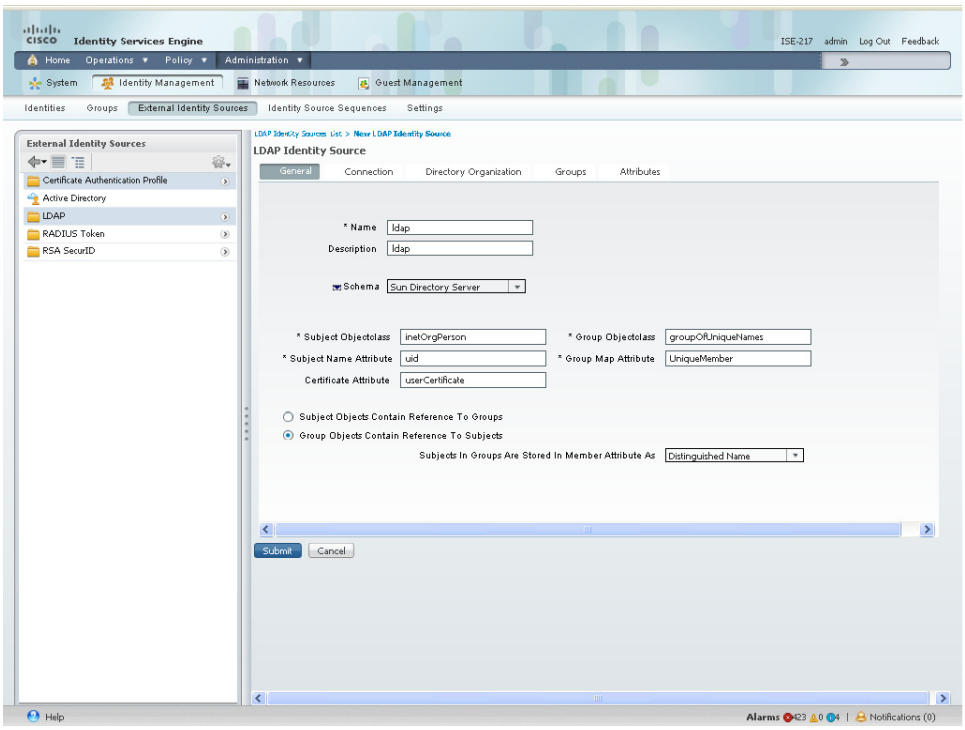
Step 1 Choose **Administration > Identity Management > External Identity Sources**.

Step 2 From the External Identity Sources navigation pane on the left, click **LDAP**.

Step 3 Click **Add** to add an LDAP identity source or check the check box next to an LDAP identity source, and click **Edit** or **Duplicate** to edit or duplicate an existing LDAP identity source.

Step 4 A page similar to the one shown in Figure 5-10 appears.

Figure 5-10 LDAP General Tab



Step 5 Enter the values as described in Table 5-2.

Step 6 Click **Submit** to create an LDAP instance.

LDAP General Information

Table 5-2 lists the fields in the LDAP general tab and their descriptions.

Table 5-2 LDAP General Tab

Option	Description
Name	(Required) 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	This description is optional, is of type string, and has a maximum length of 1024 characters.
Schema	If you choose any one of the following built-in schema types, the schema details will be prepopulated and are hidden: • Active Directory • Sun Directory Server • Novell eDirectory **Note** You can edit the details from the predefined schema, but Cisco ISE detects the change and relabels the Schema as Custom. You can click the arrow next to Schema to view the schema details.
The following fields contain the schema details and will appear only if you choose the Custom schema.	
Subject Objectclass	(Required) This value is 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	(Required) This field is the name of the attribute containing the username from request. The value is of type string and the maximum length is 256 characters.
Certificate Attribute	Enter the attribute that contains the certificate definitions. These definitions can optionally be used to validate certificates that are presented by clients when they are defined as part of a certificate authentication profile. In such cases, a binary comparison is performed between the client certificate and the certificate retrieved from the LDAP identity source.
Group Objectclass	(Required) This value is 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	(Required) This field 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 radio button if the subject objects contain an attribute that specifies the group to which they belong.
Group Objects Contain Reference To Subjects	Click this radio button 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	This option is available only when you enable the Group Objects Contain Reference To Subjects radio button. This option specifies how members are sourced in the group member attribute and defaults to the DN.

You can edit an LDAP instance to accomplish the following tasks:

- Configure LDAP Connection Settings, page 5-25
- Configure Directory Organization Values, page 5-27
- Add LDAP Groups, page 5-30
- Select LDAP Attributes, page 5-31

Configure LDAP Connection Settings

To connect to the LDAP server, complete the following steps:

Step 1 Choose **Administration > Identity Management > External Identity Sources**.

Step 2 From the External Identity Sources navigation pane on the left, click **LDAP**.

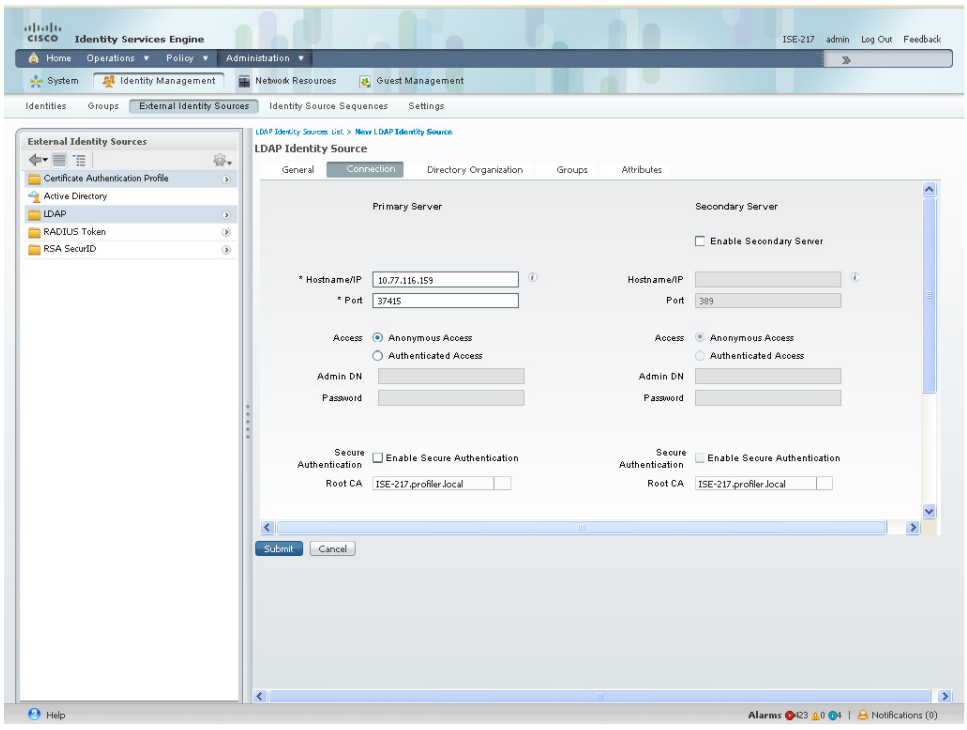
The LDAP page appears.

Step 3 Check the check box next to the LDAP instance that you want to edit, and then click **Edit**.

Step 4 Click the **Connection** tab to configure the primary and secondary servers.

A page similar to the one shown in Figure 5-11 appears.

Figure 5-11 LDAP Connection Tab



Step 5 Enter the values as described in Table 5-3.

Step 6 Click **Submit** to save the connection parameters.

LDAP Connection Settings

Table 5-3 lists the fields in the LDAP connection tab and their descriptions.

Table 5-3 LDAP Connection Tab

Option	Description
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	(Required) 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	(Required) 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.
Access	(Required) 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 permits searching of all required users under the User Directory Subtree and permits searching 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.
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.
Root CA	Choose a trusted root certificate authority from the drop-down list to enable secure authentication with a certificate. See the "Certificate Authority Certificates" section on page 13-16 and "Adding a Certificate Authority Certificate" section on page 13-18 for information on CA certificates.
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 300. The default is 10.

Table 5-3 LDAP Connection Tab (continued)

Option	Description
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.
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.

Configure Directory Organization Values

To configure directory organization values, complete the following steps:

Note For LDAP identity source, the following three searches are applicable:

- Search for all groups in group subtree for administration
- Search for user in subject subtree to locate user
- Search for groups in which the user is a member

Step 1 Choose **Administration > Identity Management > External Identity Sources**.

Step 2 From the External Identity Sources navigation pane on the left, click **LDAP**.

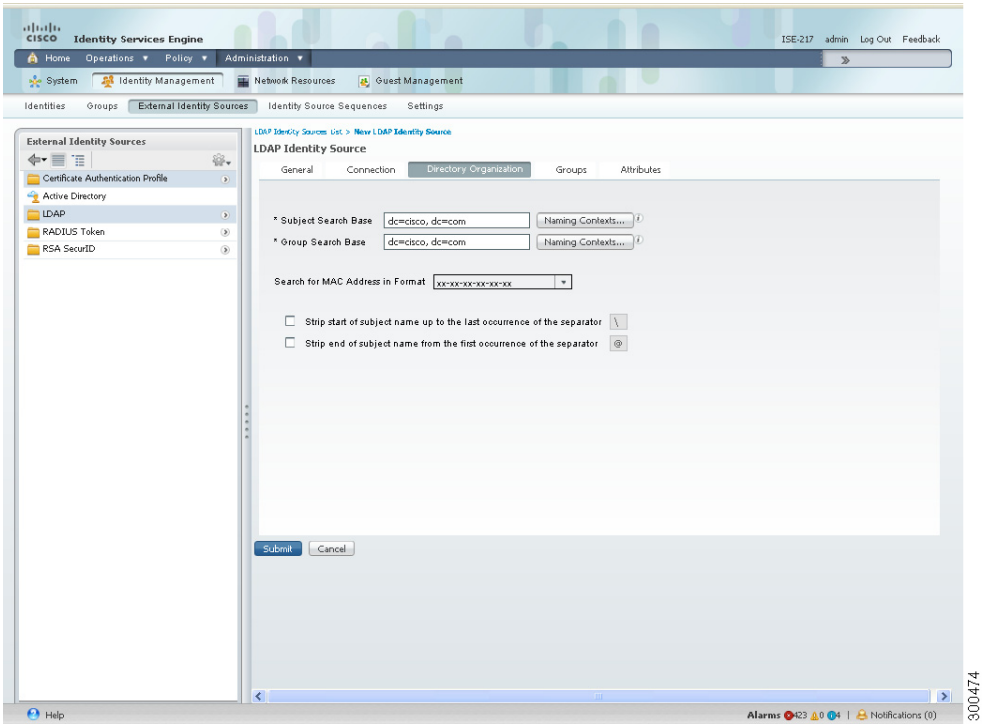
The LDAP page appears.

Step 3 Check the check box next to the LDAP instance that you want to edit, then click **Edit**.

Step 4 Click the **Directory Organization** tab.

A screen similar to the one shown in Figure 5-12 appears.

Figure 5-12 LDAP Directory Organization Tab



Step 5 Enter the values as described in Table 5-4.

Step 6 Click **Submit** to save the configuration.

LDAP Directory Organization Settings

Table 5-4 lists the fields in the LDAP directory organization tab and their descriptions.

Table 5-4 LDAP Directory Organization Tab

Option	Description
Subject Search Base	(Required) 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.

Table 5-4 LDAP Directory Organization Tab (continued)

Option	Description
Group Search Base	(Required) 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.
Search for MAC Address in Format	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, it 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, in the username, Cisco ISE finds the delimiter character that is specified in this field, 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. If you provide any of these characters, stripping fails.

Table 5-4 LDAP Directory Organization Tab (continued)

Option	Description
Strip End of Subject Name from the First Occurrence of the Separator	Enter the appropriate text to remove domain suffixes from usernames. If, in the username, Cisco ISE finds the delimiter character that is specified in this field, 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 the at symbol (@) and the username is *user1@domain*, then Cisco ISE submits *user1* to an 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. If you provide any of these characters, stripping fails.

Add LDAP Groups

To add LDAP groups, complete the following steps:

Step 1 Choose **Administration > Identity Management > External Identity Sources**.

Step 2 From the External Identity Sources navigation pane on the left, click **LDAP**.

The LDAP page appears.

Step 3 Check the check box next to the LDAP instance that you want to edit, then click **Edit**.

Step 4 Click the **Groups** tab.

The Groups page appears.

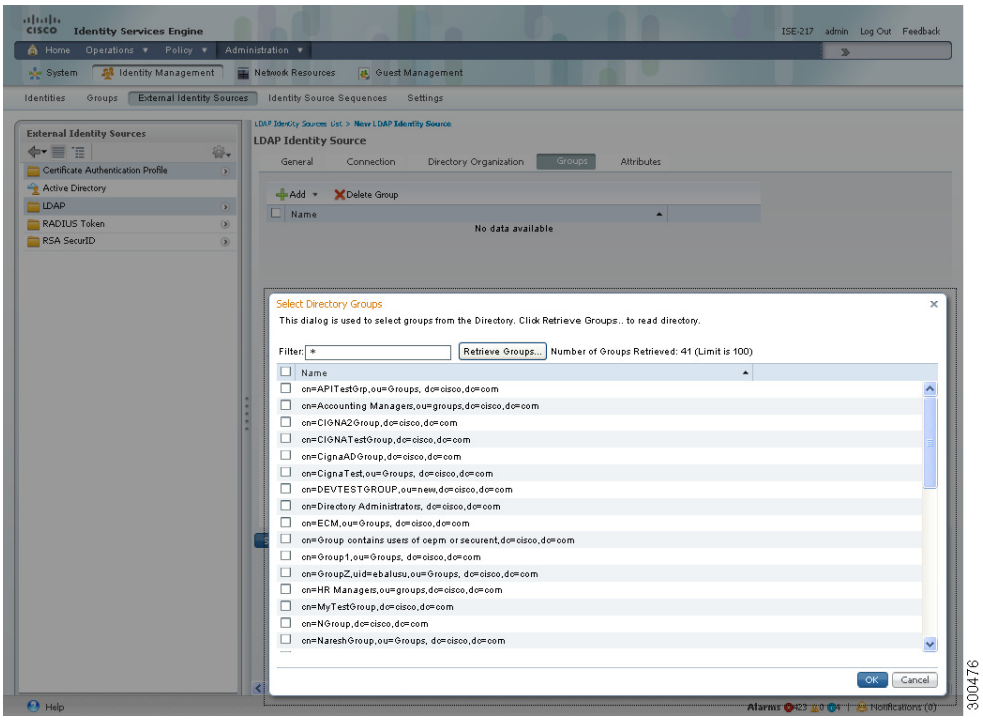
Step 5 Choose **Add > Add Group** to add a new group or choose **Add > Select Groups From Directory** to select the groups from the LDAP directory.

Step 6 If you choose to add a group, enter a name for the new group.

Step 7 If you are selecting from the directory, enter the filter criteria, and click **Retrieve Groups**. Your search criteria can contain the asterisk (*) wildcard character.

A screen similar to the one shown in Figure 5-13 appears.

Figure 5-13 LDAP Select Groups Page



Step 8 Check the check boxes next to the groups that you want to select, then click **OK**.

The groups that you have selected will appear in the Groups page.

Step 9 Click **Submit** to save the group selection.

Select LDAP Attributes

To choose LDAP attributes, complete the following steps:

Step 1 Choose **Administration > Identity Management > External Identity Sources**.

Step 2 From the External Identity Sources navigation pane on the left, click **LDAP**.

The LDAP page appears.

Step 3 Check the check box next to the LDAP instance that you want to edit, then click **Edit**.

Step 4 Click the **Attributes** tab.

The Attributes page appears.

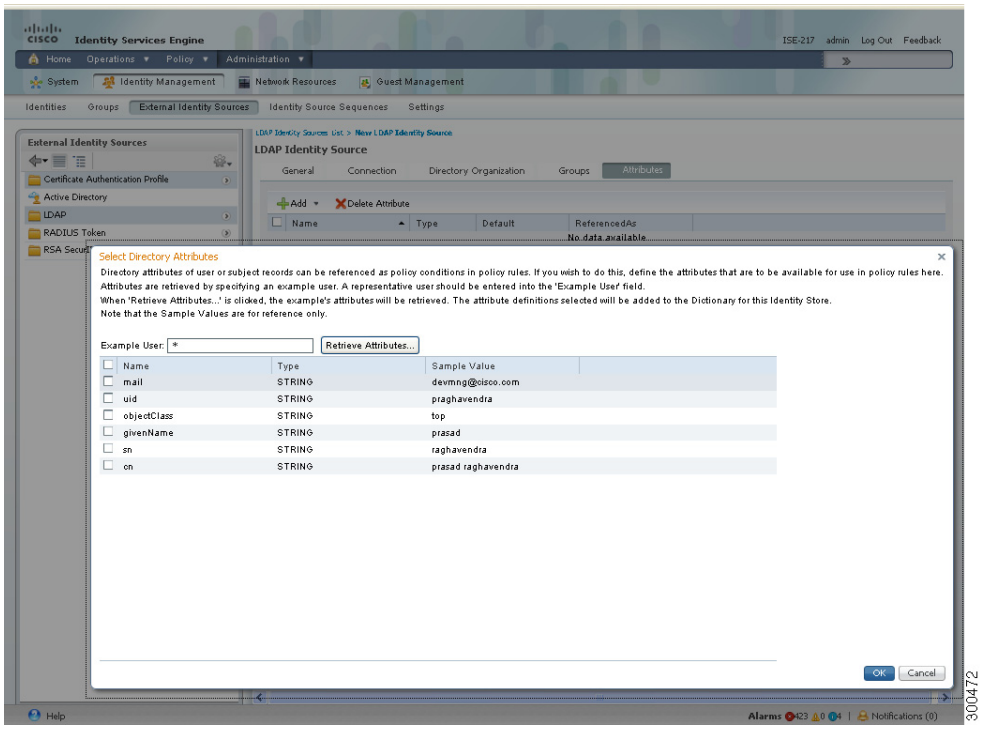
Step 5 Choose **Add > Add Attribute** to add a new attribute or choose **Add > Select Attributes From Directory** to select attributes from the LDAP server.

Step 6 If you choose to add an attribute, enter a name for the new attribute.

Step 7 If you choose the Select from Directory option, the Select Directory Attributes page appears. Enter an example user and click **Retrieve Attributes** to retrieve the user's attributes. You can use the asterisk (*) wildcard character.

Step 8 A screen similar to the one shown in Figure 5-14 appears.

Figure 5-14 Select Directory Attributes Page



Step 9 Check the check boxes next to the attributes that you want to select, then click **OK**.

The attributes that you have selected appear in the Attributes page.

Step 10 Click **Submit** to save the attribute selections.

Next Steps:

1. See Chapter 16, "Managing Authentication Policies" for information on how to create authentication policies.
2. See Chapter 17, "Managing Authorization Policies and Profiles" for information on how to create authorization profiles and policies.

RADIUS Token Identity Sources

A server that supports the RADIUS protocol and provides authentication, authorization, and accounting (AAA) services to users and devices is called the RADIUS server. The RADIUS identity source is simply an external identity source that contains a collection of subjects and their credentials and uses the

RADIUS protocol for communication. For example, the Safeword token server is an identity source that can contain several users and their credentials as one-time passwords that provides an interface that you can query using the RADIUS protocol.

Cisco ISE supports any RADIUS RFC 2865-compliant server as an external identity source. Cisco ISE supports multiple RADIUS token server identities, for example, the RSA SecurID server and the SafeWord server. RADIUS identity sources can work with any RADIUS token server that is used to authenticate the user. RADIUS identity sources use the User Datagram Protocol (UDP) port for authentication sessions. The same UDP port is used for all RADIUS communication.

For Cisco ISE to successfully send RADIUS messages to a RADIUS-enabled server, you must ensure that the gateway devices between the RADIUS-enabled server and Cisco ISE allow communication over the UDP port. You can configure the UDP port through the Cisco ISE user interface.

This section contains the following topics:

Key Features of the Integration of Cisco ISE and RADIUS Identity Source

Supported Authentication Protocols

Cisco ISE supports the following authentication protocols for RADIUS identity sources:

- RADIUS PAP
- PEAP with inner EAP-GTC
- EAP-FAST with inner EAP-GTC

Constraints

RADIUS token servers use the UDP port for authentication sessions. This port is used for all RADIUS communication. For Cisco ISE to send RADIUS one-time password (OTP) messages to a RADIUS-enabled token server, you must ensure that the gateway devices between Cisco ISE and the RADIUS-enabled token server allow communication over the UDP port.

RADIUS Shared Secret

You must provide a shared secret while configuring RADIUS identity sources in Cisco ISE. This shared secret should be the same as the shared secret that is configured on the RADIUS token server.

Failover

Cisco ISE allows you to configure multiple RADIUS identity sources. Each RADIUS identity source can have primary and secondary RADIUS servers. When Cisco ISE is unable to connect to the primary server, it uses the secondary server.

Password Prompt

RADIUS identity sources allow you to configure the password prompt. You can configure the password prompt through the Cisco ISE user interface.

User Authentication

Cisco ISE obtains the user credentials (username and passcode) and passes them to the RADIUS token server. Cisco ISE also relays the results of the RADIUS token server authentication processing to the user.

User Attribute Cache

RADIUS token servers, by default, do not support user lookups. However, the user lookup functionality is essential for the following Cisco ISE features:

- PEAP session resume—This feature allows the PEAP session to resume after successful authentication during EAP session establishment.
- EAP/FAST fast reconnect—This feature allows fast reconnection after successful authentication during EAP session establishment.

Cisco ISE caches the results of successful authentications to process user lookup requests for these features. For every successful authentication, the name of the authenticated user and the retrieved attributes are cached. Failed authentications are not written to the cache.

The cache is available in the memory at runtime and is not replicated between Cisco ISE nodes in a distributed deployment. You can configure the Time to Live (TTL) limit for the cache through the Cisco ISE user interface. You must enable the identity caching option and set the aging time in minutes. The cache is available in the memory for the specified amount of time.

RADIUS Identity Source in Identity Sequence

You can add the RADIUS identity source for authentication sequence in an identity source sequence. However, you cannot add the RADIUS identity source for attribute retrieval sequence because you cannot query the RADIUS identity source without authentication. Cisco ISE cannot distinguish among different error cases while authenticating with a RADIUS server. RADIUS servers return an Access-Reject message for all error cases. For example, when a user is not found in the RADIUS server, instead of returning a User Unknown status, the RADIUS server returns an Access-Reject message. You can, however, enable the Treat Rejects as Authentication Failed or User Not Found option, which is available in the RADIUS identity source pages of the Cisco ISE user interface.

Authentication Failure Messages

When a user is not found in the RADIUS server, the RADIUS server returns an Access-Reject message. Cisco ISE provides the option to configure this message through the Cisco ISE user interface as either Authentication Failed or User Not Found. However, this option returns a User Not Found message not only for cases where the user is not known, but for all failure cases.

Table 5-5 lists the different failure cases that are possible with RADIUS identity servers.

Table 5-5 Error Handling

Cause of Authentication Failure	Failure Cases
Authentication Failed	• User is unknown. • User attempts to log in with an incorrect passcode. • User login hours expired.

Table 5-5 Error Handling (continued)

Cause of Authentication Failure	Failure Cases
Process Failed	• RADIUS server is configured incorrectly in Cisco ISE. • RADIUS server is unavailable. • RADIUS packet is detected as malformed. • Problem during sending or receiving a packet from the RADIUS server. • Timeout.
Unknown User	Authentication failed and the Fail on Reject option is set to false.

Username Special Format with SafeWord Server

The SafeWord token server supports authentication with the following username format:

Username—Username, OTP

As soon as Cisco ISE receives the authentication request, it parses the username and converts it to the following username:

Username—Username

The SafeWord token servers support both of these formats. Cisco ISE works with various token servers. While configuring a SafeWord server, you must check the SafeWord Server check box in the Cisco ISE user interface for Cisco ISE to parse the username and convert it to the specified format. This conversion is done in the RADIUS token server identity source before the request is sent to the RADIUS token server.

Authentication Request and Response

When Cisco ISE forwards an authentication request to a RADIUS-enabled token server, the RADIUS authentication request contains the following attributes:

- User-Name (RADIUS attribute 1)
- User-Password (RADIUS attribute 2)
- NAS-IP-Address (RADIUS attribute 4)

Cisco ISE expects to receive any one of the following responses:

- Access-Accept—No attributes are required, however, the response can contain a variety of attributes based on the RADIUS token server configuration.
- Access-Reject—No attributes are required.
- Access-Challenge—The attributes that are required per RADIUS RFC are the following:
  - State (RADIUS attribute 24)
  - Reply-Message (RADIUS attribute 18)
  - One or more of the following attributes: Vendor-Specific, Idle-Timeout (RADIUS attribute 28), Session-Timeout (RADIUS attribute 27), Proxy-State (RADIUS attribute 33)

No other attributes are allowed in Access-Challenge.

For information on how to add RADIUS token servers, see the "Adding or Editing a RADIUS Token Server" section on page 5-36.

For information on how to delete RADIUS token servers, see the "Deleting a RADIUS Token Server" section on page 5-39.

Adding or Editing a RADIUS Token Server

Prerequisite:

Every Cisco ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedures, you must have one of the following roles assigned: Super Admin or System Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To create or edit a RADIUS identity source, complete the following steps:

Step 1 Choose **Administration > Identity Management > External Identity Sources**.

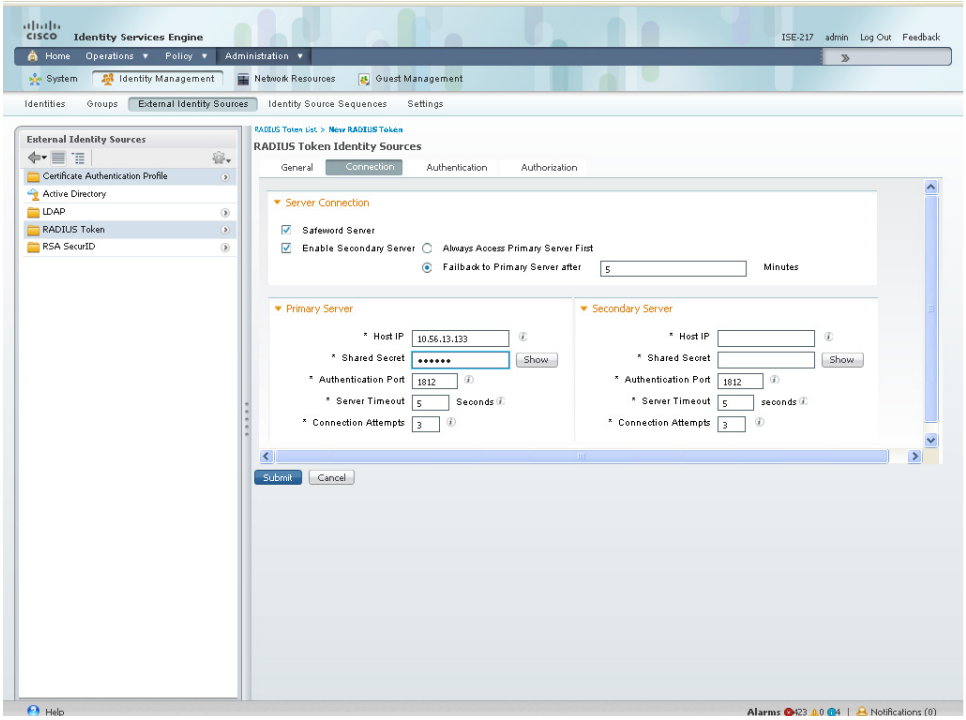
Step 2 From the External Identity Sources navigation pane on the left, click **RADIUS Token**.

The RADIUS Token Identity Sources page appears.

Step 3 Click **Add** to add a new RADIUS identity source or check the check box next to the RADIUS token server that you want to edit, then click **Edit** or **Duplicate** to create a duplicate RADIUS token server definition.

A screen similar to the one shown in Figure 5-15 appears.

Figure 5-15 RADIUS Token Server Prompts Tab



Step 4 On the General and Connection tabs, enter the values as described in Table 5-6.

Step 5 Click the **Authentication** tab.

This tab allows you to control the responses to an Access-Reject message from the RADIUS token server. This response could either mean that the credentials are invalid or that the user is not known. Cisco ISE accepts either one of the following responses: Failed authentication or User not found. This tab also allows you to enable identity caching and to set the aging time for the cache. You can also configure a prompt to request the password.

Step 6 Select the following:

- Click the **Treat Rejects as 'authentication failed'** radio button if you want the Access-Reject response from the RADIUS token server to be treated as a failed authentication.
- Click the **Treat Rejects as 'user not found'** radio button if you want the Access-Reject response from the RADIUS token server to be treated as an unknown user failure.
- Enter a prompt for requesting the password.

Step 7 Click the **Authorization** tab.

This tab allows you to configure a name that will appear for this single attribute that is returned by the RADIUS token server while sending an Access-Accept response to Cisco ISE. This attribute can be used in authorization policy conditions. Enter a name for this attribute in the Attribute Name ACS field. The default value is CiscoSecure-Group-Id.

Step 8 Click **Submit** to save the RADIUS Token identity source.

RADIUS Token Server Connections

Table 5-6 lists the fields in the RADIUS Token Server Connections tab and their default values.

Table 5-6 RADIUS Token Server Prompts Tab

Option	Description
Name	(Required) This field is the name of the RADIUS token server. The maximum number of characters allowed is 64.
Description	This field is an optional description. The maximum number of characters is 1024.
SafeWord Server	Check this check box if your RADIUS identity source is a SafeWord server.
Enable Secondary Server	Check this check box to enable the secondary RADIUS token server for Cisco ISE to be used as a backup in case the primary fails. If you check this check box, you must configure a secondary RADIUS token server.
Always Access Primary Server First	Click this radio button if you want Cisco ISE to always access the primary server first.
Fallback to Primary Server after	Click this radio button to specify the amount of time in minutes that Cisco ISE can authenticate using the secondary RADIUS token server if the primary server cannot be reached. After this time elapses, Cisco ISE reattempts to authenticate against the primary server.

Table 5-6 RADIUS Token Server Prompts Tab (continued)

Option	Description
Primary Server	
Host IP	Enter the IP address of the primary RADIUS token server. This field can take as input a valid IP address that is expressed as a string. Valid characters that are allowed in this field are numbers and dot (.).
Shared Secret	Enter the shared secret that is configured on the primary RADIUS token server for this connection.
Authentication Port	Enter the port number on which the primary RADIUS token server is listening. Valid values are from 1 to 65,535. The default is 1812.
Server Timeout	Specify the time in seconds that Cisco ISE should wait for a response from the primary RADIUS token server before it determines that the primary server is down. Valid values are 1 to 300. The default is 5.
Connection Attempts	Specify the number of attempts that Cisco ISE should make to reconnect to the primary server before moving on to the secondary server (if defined) or dropping the request if a secondary server is not defined. Valid values are 1 to 9. The default is 3.
Secondary Server	
Host IP	Enter the IP address of the secondary RADIUS token server. This field can take as input a valid IP address that is expressed as a string. Valid characters that are allowed in this field are numbers and dot (.).
Shared Secret	Enter the shared secret configured on the secondary RADIUS token server for this connection.
Authentication Port	Enter the port number on which the secondary RADIUS token server is listening. Valid values are from 1 to 65,535. The default is 1812.
Server Timeout	Specify the time in seconds that Cisco ISE should wait for a response from the secondary RADIUS token server before it determines that the secondary server is down. Valid values are 1 to 300. The default is 5.
Connection Attempts	Specify the number of attempts that Cisco ISE should make to reconnect to the secondary server before dropping the request. Valid values are 1 to 9. The default is 3.

Next Steps:

1. See Chapter 16, “Managing Authentication Policies” for information on how to create authentication policies.
2. See Chapter 17, “Managing Authorization Policies and Profiles” for information on how to create authorization profiles and policies.

Deleting a RADIUS Token Server

Prerequisites:

- Every Cisco ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedures, you must have one of the following roles assigned: Super Admin or System Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.
- Ensure that you do not select the RADIUS token servers that are part of an identity source sequence. If you select a RADIUS token server that is part of an identity source sequence for deletion, the delete operation will fail.

To delete a RADIUS identity source, complete the following steps:

Step 1 Choose **Administration > Identity Management > External Identity Sources**.

Step 2 From the External Identity Sources navigation pane on the left, click **RADIUS Token**.

The RADIUS Token Identity Sources page appears with a list of configured RADIUS token servers.

Step 3 Check the check box next to the RADIUS token server or servers that you want to delete, then click **Delete**.

Cisco ISE prompts you with the following message:

Are you sure you want to delete?

Step 4 Click **OK** to delete the RADIUS token server or servers that you have selected.

Note If you select multiple RADIUS token servers for deleting, and one of them is used in an identity source sequence, the delete operation fails and none of the RADIUS token servers are deleted.

RSA Identity Sources

Cisco ISE supports the RSA SecurID server as an external database. RSA SecurID two-factor authentication consists of the PIN of the user and an individually registered RSA SecurID token that generates single-use token codes based on a time code algorithm. A different token code is generated at fixed intervals (usually each at 30 or 60 seconds). The RSA SecurID server validates this dynamic authentication code. Each RSA SecurID token is unique, and it is not possible to predict the value of a future token based on past tokens. Thus, when a correct token code is supplied together with a PIN, there is a high degree of certainty that the person is a valid user. Therefore, RSA SecurID servers provide a more reliable authentication mechanism than conventional reusable passwords.

Cisco ISE supports the following RSA identity sources:

- RSA ACE/Server 6.x series
- RSA Authentication Manager 7.x series

You can integrate with RSA SecurID authentication technology in any one of the following ways:

- Using the RSA SecurID agent—Users are authenticated with their username and passcode through the RSA native protocol.

- Using the RADIUS protocol—Users are authenticated with their username and passcode through the RADIUS protocol.

The RSA SecurID token server in Cisco ISE integrates with the RSA SecurID authentication technology by using the RSA SecurID Agent.

Cisco ISE Release 1.1.x supports only one RSA realm.

This section contains the following topics:

Integrating Cisco ISE with RSA SecurID Server

These are the two administrative roles involved in integrating Cisco ISE with an RSA SecurID server:

- RSA Server Administrator—Configuring and maintaining RSA systems and integration
- Cisco ISE Administrator—Configuring Cisco ISE to integrate with the RSA SecurID server and maintaining the configuration.

This section describes the processes that are involved in integrating Cisco ISE with the RSA SecurID server as an external identity source. For more information on RSA servers, please refer to the RSA documentation.

Configuring RSA in Cisco ISE

The RSA administrative system generates an sdconf.rec file, which the RSA system administrator will provide to you. This file allows you to add Cisco ISE servers as RSA SecurID agents in the realm. You have to browse and add this file to Cisco ISE. By the process of replication, the primary Cisco ISE server distributes this file to all the secondary servers.

Authenticating RSA Agents in Cisco ISE Against the RSA SecurID Server

After the sdconf.rec file is installed on all Cisco ISE servers, the RSA agent module initializes, and authentication with RSA-generated credentials proceeds on each of the Cisco ISE servers. After the agent on each of the Cisco ISE servers in a deployment has successfully authenticated, the RSA server and the agent module together download the securid file. This file resides in the Cisco ISE file system and is in a well-known place defined by the RSA agent.

Maintaining RSA Servers in Cisco ISE Deployment

After you have added the sdconf.rec file in Cisco ISE, the RSA SecurID administrator might have to update the sdconf.rec file in case of decommissioning an RSA server or adding a new RSA secondary server. The RSA SecurID administrator will provide you with an updated file. You can then reconfigure Cisco ISE with the updated file. The replication process in Cisco ISE distributes the updated file to the secondary Cisco ISE servers in the deployment. Cisco ISE first updates the file in the file system and coordinates with the RSA agent module to phase the restart process appropriately. When the sdconf.rec file is updated, the sdstatus.12 and securid files are reset (deleted).

Overriding Automatic RSA Routing

You can have more than one RSA server in a realm. The sdopts.rec file performs the role of a load balancer. Cisco ISE servers and RSA SecurID servers operate through the agent module. The agent module that resides on Cisco ISE maintains a cost-based routing table to make the best use of the RSA servers in the realm. You can, however, choose to override this routing with a manual configuration. You can override with a manual configuration for each Cisco ISE server for the realm using a text file called sdopts.rec through the Cisco ISE user interface. Refer to the RSA documentation for information on how to create this file.

Resetting an RSA Node Secret

The securid file is a secret node key file. When RSA is initially set up, it uses a secret to validate the agents. When the RSA agent that resides in Cisco ISE successfully authenticates against the RSA server for the first time, it creates a file on the client machine called securid and uses it to ensure that the data exchanged between the machines is valid. At times, you may have to delete the securid file from a specific Cisco ISE server or a group of servers in your deployment (for example, after a key reset on the RSA server). You can use the Cisco ISE user interface to delete this file from an Cisco ISE server for the realm. When the RSA agent in Cisco ISE authenticates successfully the next time, it creates a new securid file.

Note If authentications fail after upgrading to ISE 1.1.1, you must reset the RSA secret.

Resetting an RSA Automatic Availability

The sdstatus.12 file provides information about the availability of RSA servers in the realm. For example, it provides information on which servers are active and which are down. The agent module works with the RSA servers in the realm to maintain this availability status. This information is serially listed in the sdstatus.12 file, which is sourced in a well-known location in the Cisco ISE file system. Sometimes this file becomes old and the current status is not reflected in this file. You must remove this file so that the current status can be recreated. You can use the Cisco ISE user interface to delete the file from a specific Cisco ISE server for a specific realm. Cisco ISE coordinates with the RSA agent and ensures correct restart phasing.

The availability file sdstatus.12 will be deleted whenever the securid file is reset, or the sdconf.rec or sdopts.rec files are updated.

Distributed Environment Considerations

Managing RSA identity sources in a distributed Cisco ISE environment involves the following:

- Distributing the sdconf.rec and sdopts.rec files from the primary server to the secondary servers.
- Deleting the securid and sdstatus.12 files.

For more information, see the following topics:

- Importing the RSA Configuration File, page 5-42
- Configuring the Options File for a Cisco ISE Server and Resetting SecurID and sdstatus.12 Files, page 5-43
- Adding and Editing RSA Identity Sources, page 5-42

Adding and Editing RSA Identity Sources

To create or edit an RSA identity source, you must import the RSA configuration file (sdconf.rec). See the "Importing the RSA Configuration File" section on page 5-42 for more information.

Prerequisites:

1. You must obtain the sdconf.rec file from your RSA administrator.
2. Every Cisco ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedures, you must have one of the following roles assigned: Super Admin or System Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

Importing the RSA Configuration File

To configure general RSA settings, complete the following steps:

Step 1 Choose **Administration > Identity Management > External Identity Sources**.

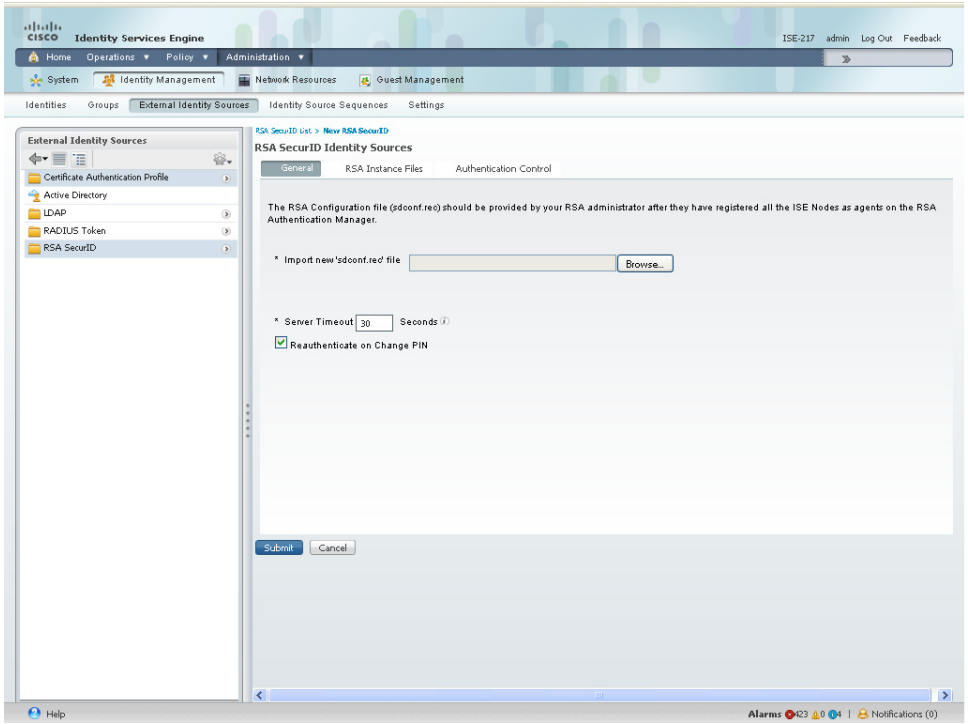
Step 2 From the External Identity Sources navigation pane on the left, click **RSA SecurID**.

The RSA SecurID Identity Sources page appears.

Step 3 Click **Add** to add an RSA identity source or check the check box next to the RSA identity source that you want to edit, and then click **Edit** or click **Duplicate** to create a duplicate entry of the RSA identity source.

The RSA General tab appears as shown in Figure 5-16.

Figure 5-16 RSA General Tab



Step 4 Click **Browse** to choose the new or updated sdconf.rec file from the system that is running your client browser.

When you create the RSA identity source for the first time, the Import new sdconf.rec file field will be a mandatory field. From then on, you can replace the existing sdconf.rec file with an updated one, but replacing the existing file is optional.

Step 5 (Required) Enter the server timeout value in seconds. Cisco ISE will wait for a response from the RSA server for the amount of time specified before it times out. This value can be any integer from 1 through 199. The default value is 30 seconds.

Step 6 Check the **Reauthenticate on Change PIN** check box to force a reauthentication when the PIN is changed.

Step 7 Click **Save** to save the configuration.

Cisco ISE also supports the following scenarios:

- Configuring the Options File for a Cisco ISE Server and Resetting SecurID and sdstatus.12 Files, page 5-43
- Configuring Authentication Control Options, page 5-46

Configuring the Options File for a Cisco ISE Server and Resetting SecurID and sdstatus.12 Files

To configure the sdopts.rec file, and to reset the securid and sdstatus.12 files, complete the following steps:

Step 1 Log into your Cisco ISE server.

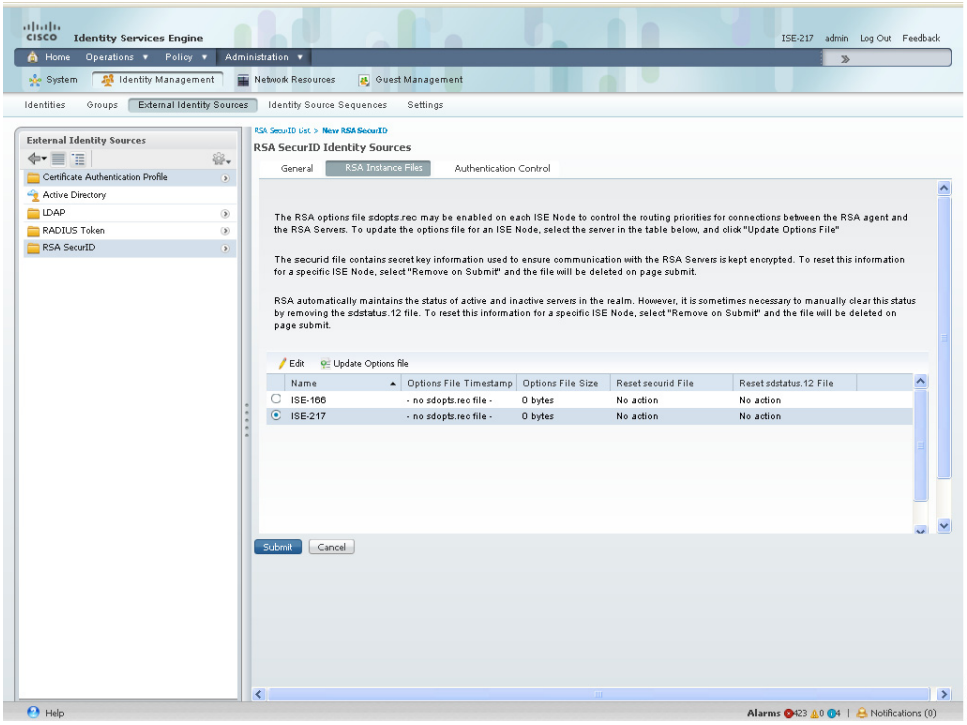
Step 2 Choose **Administration > Identity Management > External Identity Sources**.

Step 3 Click **Add** to add an RSA identity source or check the check box next to the RSA identity source that you want to edit, and then click **Edit** or click **Duplicate** to create a duplicate RSA identity source entry.

Step 4 Click the **RSA Instance Files** tab.

A screen similar to the one shown in Figure 5-17 appears.

Figure 5-17 RSA Instance Files Tab

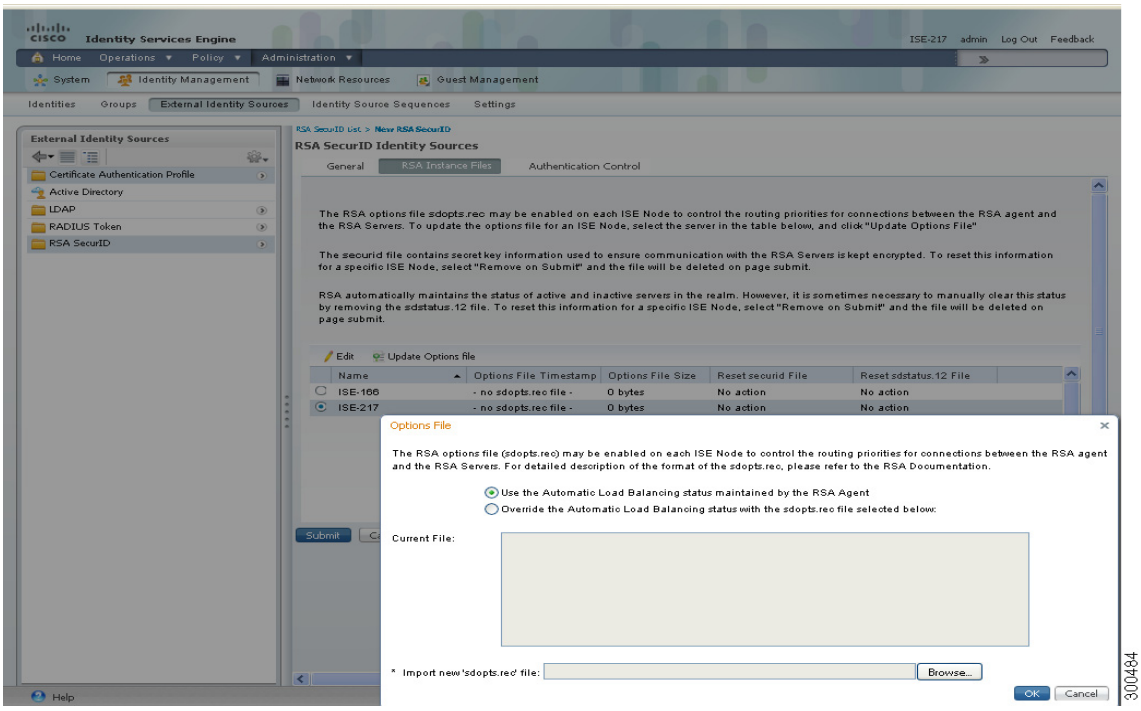


This page lists the sdopts.rec files for all the Cisco ISE servers in your deployment.

Step 5 Click the radio button next to the sdopts.rec file for a particular Cisco ISE server, and click **Update Options File**.

A screen similar to the one shown in Figure 5-18 appears.

Figure 5-18 RSA Options File



The existing file is displayed in the Current File region (display only).

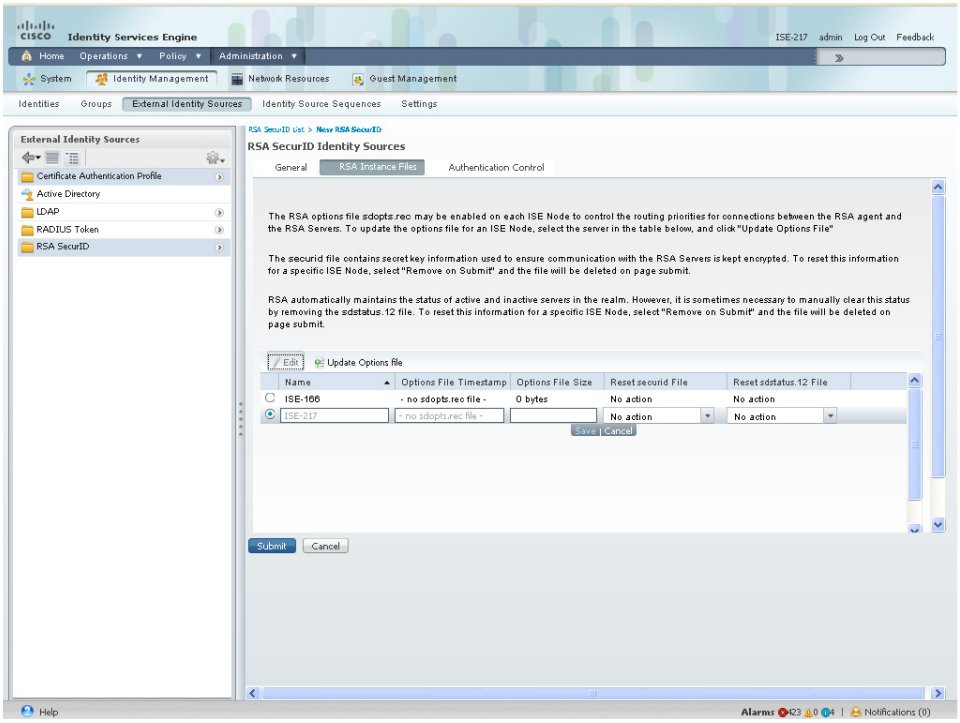
Step 6 Choose one of the following:

- Use the Automatic Load Balancing status maintained by the RSA agent—Choose this option if you want the RSA agent to automatically manage load balancing.
- Override the Automatic Load Balancing status with the sdopts.rec file selected below—Choose this option if you want to manually configure load balancing based on your specific needs. If you choose this option, you must click **Browse** and choose the new sdopts.rec file from the system that is running your client browser.

Step 7 Click **OK**.

Step 8 To reset the securid and sdstatus.12 files for an Cisco ISE server, click the row that corresponds to the Cisco ISE server. A screen similar to the one shown in Figure 5-19 appears.

Figure 5-19 Resetting securid and sdstatus.12 Files



Step 9 Click the drop-down arrow and choose **Remove on Submit** in the Reset securid File and Reset sdstatus.12 File columns.

Note The Reset sdstatus.12 File field is hidden from your view. Using the vertical and horizontal scroll bars in the innermost frame, scroll down and then to your right to view this field.

Step 10 Click **Save** in this row to save the changes.

Step 11 Click **Save** to save the configuration.

Configuring Authentication Control Options

You can use this page to specify how Cisco ISE defines authentication failures and to enable identity caching. The RSA identity source does not differentiate between “Authentication failed” and “User not found” errors and sends an Access-Reject response.

You can define how such failures should be handled by Cisco ISE for processing requests and for reporting failures. Identity caching enables Cisco ISE to process requests that fail to authenticate against the Cisco ISE server a second time. The results and the attributes retrieved from the previous authentication are available in the cache.

To configure authentication control options, complete the following steps:

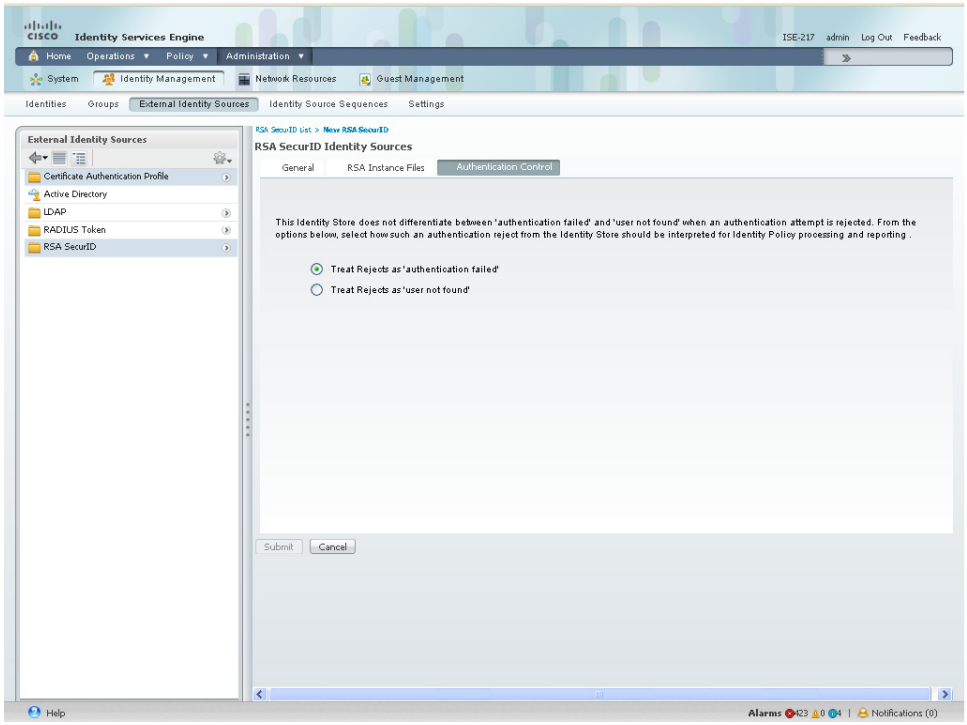
Step 1 Choose **Administration > Identity Management > External Identity Sources > RSA SecurID**.

Step 2 Click **Add** to add an RSA identity source or check the check box next to the RSA identity source that you want to edit, and then click **Edit** or click **Duplicate** to duplicate an existing RSA identity source entry.

Step 3 Click the **Authentication Control** tab.

The Authentication Control tab appears as shown in Figure 5-20.

Figure 5-20 Authentication Control Tab



Step 4 Choose one of the following:

- Treat Rejects as “authentication failed”—Choose this option if you want the rejected requests to be treated as failed authentications.
- Treat Rejects as “user not found”—Choose this option if you want the rejected requests to be treated as user not found errors.

Step 5 Click **Save** to save the configuration.

Next Steps:

1. See Chapter 16, “Managing Authentication Policies” for information on how to create authentication policies.
2. See Chapter 17, “Managing Authorization Policies and Profiles” for information on how to create authorization profiles and policies.

For more information:

- RSA Identity Sources, page 5-39
- Configuring RSA Prompts, page 5-48
- Configuring RSA Messages, page 5-49

Configuring RSA Prompts

Cisco ISE allows you to configure RSA prompts that will be presented to the user while processing requests to the RSA SecurID server.

Prerequisite:

Every Cisco ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedures, you must have one of the following roles assigned: Super Admin or System Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To configure the RSA prompts, complete the following steps:

Step 1 Choose **Administration > Identity Management > External Identity Sources**.

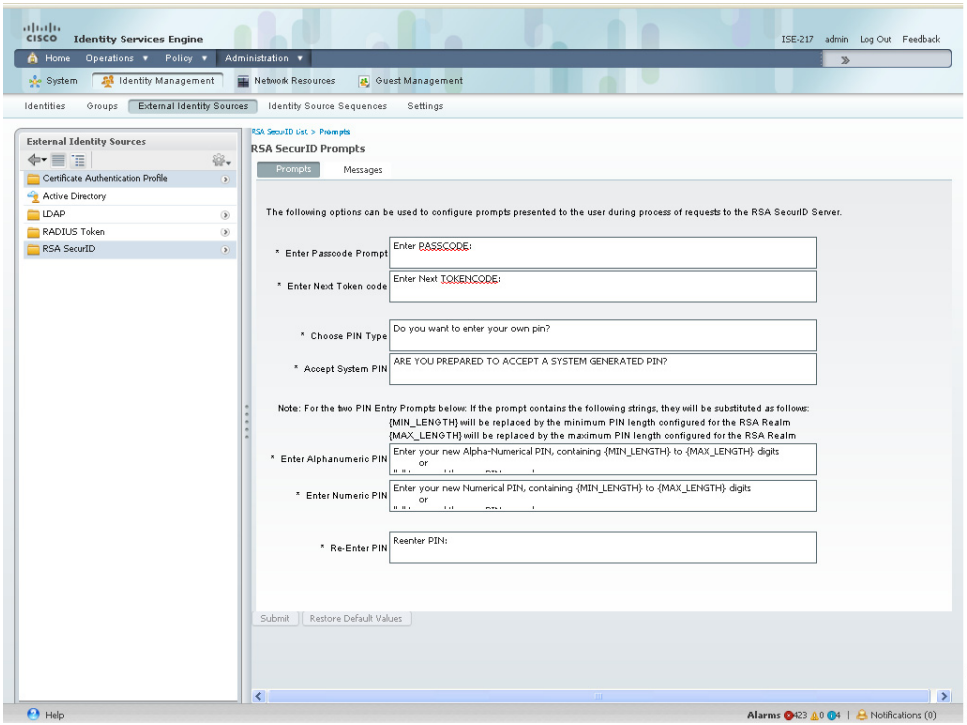
Step 2 From the External Identity Sources navigation pane on the left, click **RSA SecurID**.

The RSA SecurID Identity Sources list page appears.

Step 3 Click **Prompts**.

The RSA Prompts page appears with the default prompts as shown in Figure 5-21.

Figure 5-21 RSA Prompts Configuration Page



Step 4 Enter the information as described in Table 5-7.

Step 5 Click **Submit** to save your custom RSA Prompts or click **Reset Default Values** to apply the default RSA prompts.

RSA Prompts

Table 5-7 lists the fields in the RSA prompts tab and their default values.

Table 5-7 RSA Prompts Tab[1]

Option	Description
Enter Passcode Prompt	This field is a text string that is used to obtain the passcode. The default value is: Enter PASSCODE.
Enter Next Token Code	This field is a text string that is used to request the next token. The default value is: Enter Next TOKENCODE.
Choose PIN Type	This field is a text string that is used to request the PIN type. The default value is: Do you want to enter your own pin?
Accept System PIN	This field is a text string that is used to accept the system-generated PIN. The default value is: ARE YOU PREPARED TO ACCEPT A SYSTEM-GENERATED PIN?
Enter Alphanumeric PIN	(Optional) This field is a text string that is used to request an alphanumeric PIN. The default value is: Enter your new Alpha-Numerical PIN, containing {MIN_LENGTH} to {MAX_LENGTH} digits\n or\n"x" to cancel the new PIN procedure.
Enter Numeric PIN	(Required) This field is a text string to request a numeric PIN. The default value is: Enter your new Numerical PIN, containing {MIN_LENGTH} to {MAX_LENGTH} digits\n or\n"x" to cancel the new PIN procedure.
Re-enter PIN	(Required) This field is a text string that is used to request the user to re-enter the PIN. The default value is: Reenter PIN.

1. For the prompts, enter a string with a maximum length of 256 characters.

Next Step:

See the Configuring RSA Messages, page 5-49 for the next steps.

Configuring RSA Messages

Cisco ISE allows you to configure the messages that are presented to the user while processing requests to the RSA SecurID server.

Prerequisite:

Every Cisco ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedures, you must have one of the following roles assigned: Super Admin or System Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To configure the RSA messages, complete the following steps:

Step 1 Choose **Administration > Identity Management > External Identity Sources**.

Step 2 From the External Identity Sources navigation pane on the left, click **RSA SecurID**.

The RSA SecurID Identity Sources list page appears.

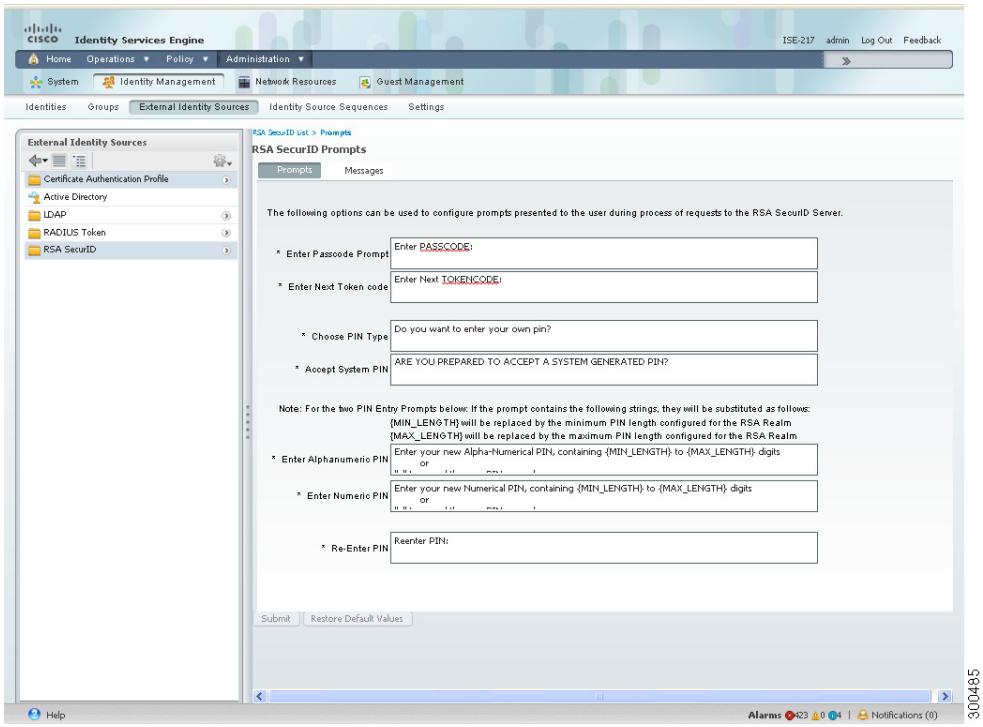
Step 3 Click **Prompts**.

The RSA Prompts page appears.

Step 4 Click the **Messages** tab.

The RSA Messages tab appears as shown in Figure 5-22.

Figure 5-22 RSA Messages Tab



Step 5 Enter the information as described in Table 5-8.

Step 6 Click **Submit** to save your custom RSA messages or click **Reset Default Values** to apply the default RSA messages.

RSA Messages

Table 5-8 lists the fields in the RSA messages tab and their default values.

Table 5-8 RSA Messages Tab

Option	Description
Display System PIN Message	Enter a text string to label the system PIN message. The default is: PIN.
Display System PIN Reminder	Enter a text string to inform the user to remember the new PIN. The default is: Please remember your new PIN, then press Return to continue.
Must Enter Numeric Error	Enter a message that instructs users to enter only numbers for the PIN. The default is: PIN must only contain numbers.
Must Enter Alpha Error	Enter a message that instructs users to enter only alphanumeric characters for PINs. The default is: PIN must only contain alphanumeric characters.
PIN Accepted Message	Enter a message that the users see when their PIN is accepted by the system. The default is: PIN accepted, wait for next card code before trying again.
PIN Rejected Message	Enter a message that the users see when the system rejects their PIN. The default is: PIN rejected.
User Pins Differ Error	Enter a message that the users see when they enter an incorrect PIN. The default is: PINs differ, not changed.
System PIN Accepted Message	Enter a message that the users see when the system accepts their PIN. The default is: Wait for next card code before trying again.
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. The default is: PIN must be between *minimum length* and *maximum length* characters.

Identity Source Sequences

Identity source sequences define the order in which Cisco ISE will look for user credentials in the different databases. Cisco ISE supports the following databases:

- Internal Users
- Internal Endpoints
- Active Directory
- LDAP
- RSA
- RADIUS Token Servers
- Certificate Authentication Profiles

If you have your user information in more than one of these databases that are connected to your Cisco ISE, you can define the order in which you want Cisco ISE to look for user information in these databases. Once a match is found, Cisco ISE does not look any further, but evaluates the credentials, and returns the result to the user. This policy is the first match policy.

This section contains the following topics:

Creating Identity Source Sequences

Prerequisites:

1. Ensure that you have configured your external identity sources in Cisco ISE. See the "Identity Source Sequences" section on page 5-51 for information on how to configure external identity sources.
2. Every Cisco ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedures, you must have one of the following roles assigned: Super Admin or System Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To define an identity source sequence, complete the following steps:

Step 1 Choose **Administration > Identity Management > Identity Source Sequences**.

The Identity Source Sequences page appears with a list of identity source sequences that you have defined.

Step 2 Click **Add** to add an identity source sequence. You can check the check box next to an identity source sequence, and click **Edit** or **Duplicate** to edit or duplicate it.

Step 3 Enter a name for the identity source sequence. You can also enter an optional description.

Step 4 In the Certificate-Based Authentication area, check the **Select Certificate Authentication Profile** check box and choose a certificate authentication profile from the drop-down list, if you wish to use a certificate authentication profile for authentication.

Step 5 In the Authentication Search List area, the Available list lists a set of databases that are connected to Cisco ISE. Choose a database that you want to include in the identity source sequence and click the  button to move it to the Selected list. You can add more databases to the Selected list if you want. You can click the  button to move all the databases from the Available list to the Selected list.

Step 6 You can rearrange the databases in the Selected list using the move up () or move down () buttons.

Step 7 In the Advanced Search List area, choose one of the following options:

- **Do not access other stores in the sequence and set the AuthenticationStatus attribute to ProcessError**—Click this radio button if you want Cisco ISE to discontinue the search, if the user is not found in the first selected identity source.
- **Treat as if the user was not found and proceed to the next store in the sequence**—Click this radio button if you want Cisco ISE to continue searching the other selected identity sources in sequence, if the user is not found in the first selected identity source.

Step 8 After you have the correct sequence of databases in the Selected list, click **Submit** to create the identity source sequence that you can then use in policies.

Note While processing a request, Cisco ISE will search these identity sources in sequence. Ensure that you have the identity sources in the Selected list box listed in the order in which you want Cisco ISE to search the identity sources.

Note For allowing guest users to authenticate through Local WebAuth, you must configure both the Guest Portal authentication source and the identity source sequence to contain the same identity stores. See "Specifying an Authentication Source" section on page 21-28 for more information on how to configure Guest Portal authentication source.

Next Steps:

See the "Configuring the Simple Authentication Policy" section on page 16-27 and the "Configuring the Rule-Based Authentication Policy" section on page 16-30 for information on how to use the identity source sequence in authentication policies.

Deleting Identity Source Sequences

Prerequisite:

1. Ensure that the identity source sequence that you are about to delete is not used in any authentication policies.
2. Every Cisco ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedures, you must have any one of the following roles assigned: Super Admin or System Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To delete an identity source sequence, complete the following steps:

Step 1 Choose **Administration > Identity Management > Identity Source Sequences**.

The Identity Source Sequences page appears with a list of identity source sequences that you have defined.

Step 2 Check the check box next to the identity source sequence or sequences that you want to delete, then click **Delete**.

Note An identity source sequence that is referenced in an authentication policy cannot be deleted. If you have selected multiple identity source sequences to be deleted and if one of the selected identity source sequence is referenced in an authentication policy, then the delete operation will fail.

The following message appears:

Are you sure you want to delete?

Step 3 Click **OK** to delete the identity source sequence or sequences.

Viewing and Monitoring the Identity Sources

Cisco ISE provides information about the identity sources through the following:

- Cisco ISE Dashboard, page 5-54
- Authentications, page 5-55
- Reports, page 5-56

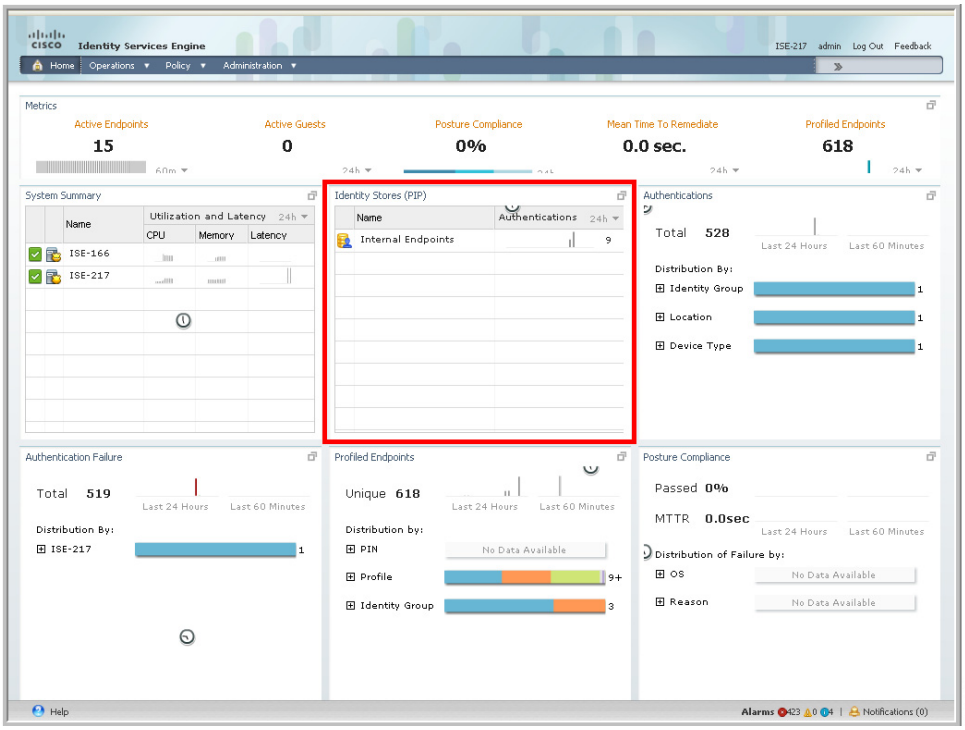
Prerequisite:

Every Cisco ISE administrator account is assigned one or more administrative roles. To view the reports in Cisco ISE, you must have one of the following roles assigned: Super Admin, Helpdesk Admin, or Monitoring Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

Cisco ISE Dashboard

Cisco ISE provides an at-a-glance view of identity source-related information in a dashlet that appears on the Cisco ISE dashboard. Figure 5-23 shows the dashboard and the Identity Stores dashlet that provides statistical data.

Figure 5-23 Cisco ISE Dashboard



Click the icon in the Identity Stores dashlet to view the details in a new page. You can drill down further for granular information.

For more information on the dashboard and how to work with it, see the "Cisco ISE Dashboard Monitoring" section on page 24-3.

Authentications

From the Authentications page, you can drill down to find more information including failure reasons.

Figure 5-24 shows the Authentications page and highlights the magnifier icon that you must click to drill down for details.

Figure 5-24 Authentications Page

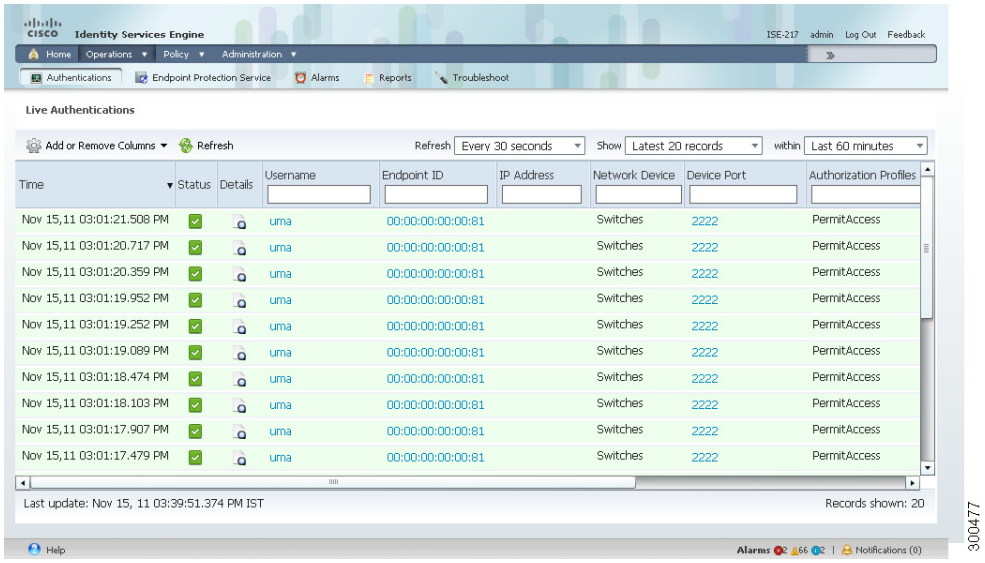
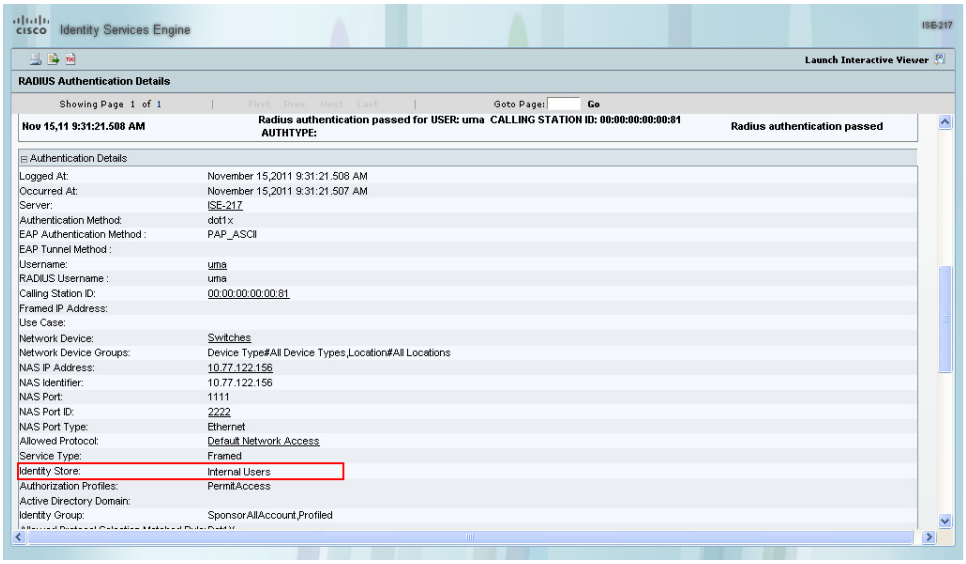


Figure 5-25 shows the drill-down view that identifies the identity source that was used for authentication.

Figure 5-25 Drill-Down View of Authentications Page



For more information on the Authentications page, see the "Monitoring Live Authentications" section on page 24-25.

Reports

Cisco ISE provides various reports that include information about identity sources. Authentication, authentication summary, and top N reports allow you to query for information based on identity sources. Table 5-9 provides a list of reports that allow you to run a query and generate a report based on identity sources.

Table 5-9 Identity Source Information in Reports

Type of Report	Report Name
AAA Protocol	Authentication Trend
	RADIUS Authentication
Allowed Protocol	Allowed Protocol Authentication Summary
	Top N Authentications By Allowed Protocol
Server Instance	Server Authentication Summary
	Top N Authentications By Server
Endpoint	Endpoint MAC Authentication Summary
	Top N Authentications By MAC Address
	Top N Authentications By Machine
Failure Reason	Failure Reason Authentication Summary
	Top N Authentications By Failure Reason
Network Device	Network Device Authentication Summary
	Top N Authentications By Network Device

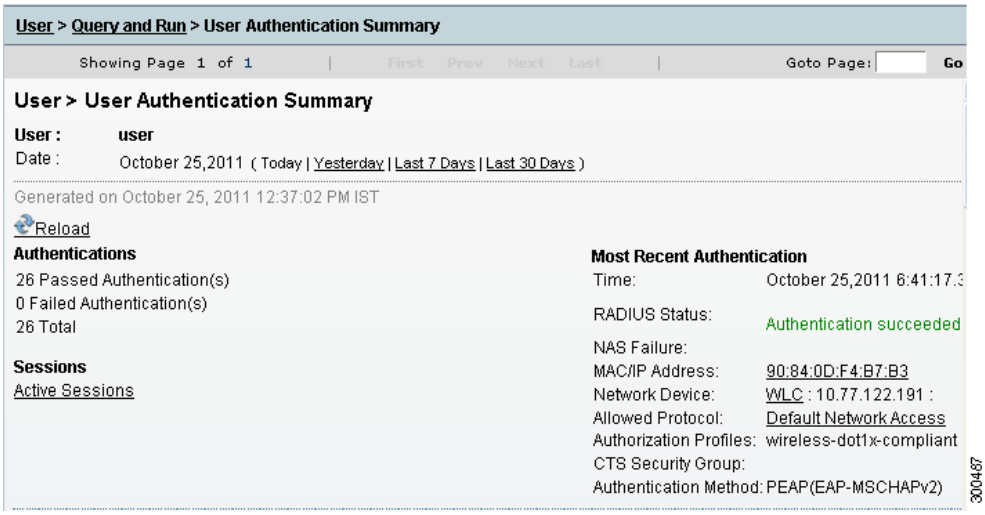
Table 5-9 Identity Source Information in Reports (continued)

Type of Report	Report Name
User	Top N Authentications By User
	User Authentication Summary

See the "Available Reports" section on page 25-41 for a description of these reports.

To run a query and generate a report, for example, the User Authentication Summary report, choose **Operations > Reports > Catalog**. Click **User** from the type of reports that are listed in the left navigation pane. Click the **User Authentication Summary** radio button and choose **Run > Query And Run**. Enter the username and any other search criteria that you want to use to run the report, and click **Run**. A report that is similar to the one that is shown in Figure 5-26 appears.

Figure 5-26 User Authentication Summary Report



You can run any of the reports listed in Table 5-9 for information on authentication, authentication summary, or top N details based on identity sources.

For information on how to run, view, navigate, customize, export, and print these reports, see the following sections:

- Running, Viewing, and Navigating Reports, page 25-3
- Accessing Catalog Reports, page 25-6
- Exporting and Printing Reports, page 25-4