Managing Users and External Identity Sources

This chapter describes how to manage user accounts in Cisco ISE and the various identity sources that you can use to store user information for authentication and authorization purposes.

In this chapter, the term user refers to employees, contractors, and sponsor users. Guest users are covered in detail in Chapter 16, "Supporting Authorized Network Access for Guests."

This chapter contains the following sections:

Cisco ISE Users

In this chapter, the term user refers to employees and contractors who access the network regularly as well as sponsor and guest users. A sponsor user is an employee or contractor of the organization who creates and manages guest-user accounts through the sponsor portal. A guest user is an external visitor who needs access to the organization's network resources for a limited period of time.

You must create an account for any user to gain access to resources and services on the Cisco ISE network. Employees, contractors, and sponsor users are created from the Admin portal.

Related Topics

- Managing Sponsor and Guest Accounts, page 16-3
- *Cisco Identity Services Engine Sponsor Portal User Guide, Release 1.2*

User Identity

User identity is like a container that holds information about a user and forms their network access credentials. Each user's identity is defined by data and includes: a username, e-mail address, password, account description, associated administrative group, user group, and role.

User Groups

User groups are a collection of individual users who share a common set of privileges that allow them to access a specific set of Cisco ISE services and functions.

User Identity Groups

A user's group identity is composed of elements that identify and describe a specific group of users that belong to the same group. A group name is a description of the functional role that the members of this group have. A group is a listing of the users that belong to this group.

Default User Identity Groups

Cisco ISE comes with the following predefined user identity groups:

- Employee—Employees of your organization belong to this group.
- SponsorAllAccount—Sponsor users who can suspend or reinstate all guest accounts in the Cisco ISE network.
- SponsorGroupAccounts—Sponsor users who can suspend guest accounts created by sponsor users from the same sponsor user group.
- SponsorOwnAccounts—Sponsor users who can only suspend the guest accounts that they have created.
- Guest—A visitor who needs temporary access to resources in the network.
- ActivatedGuest—A guest user whose account is enabled and active.

User Role

A user role is a set of permissions that determine what tasks a user can perform and what services they can access on the Cisco ISE network. A user role is associated with a user group. For example, a network access user.

User Account Custom Attributes and Password Policies

Cisco ISE allows you to restrict a user's network access based on user attributes. Cisco ISE comes with a set of predefined user attributes and also allows you to create custom attributes. Both types of attributes can be used in conditions that define the authentication policy. You can also define a password policy for user accounts so that passwords meet specified criteria.

This section contains the following topics:

Custom User Attributes

On the User Custom Attributes Setting page, you can use the Custom Attributes pane to define additional user-account attributes. Cisco ISE provides a list of predefined attributes that are not configurable. However, you can define custom attributes by configuring the following:

- Attribute name
- Data type

User Password Policy Settings

You can define the criteria that user-account passwords must meet in the User Password Policy page. Choose **Administration > Identity Management > Settings > User Password Policy**.

Table A-34 describes the setting fields in the User Password Policy page.

Note

- Password lifetime feature is there to ensure that users and sponsors change their password regularly.
- This feature does not affect local "admin" users.
- If using "disable account" we strongly recommend using "reminder" functionality to avoid users getting locked.
- User expiry thread works at midnight and will disable all accounts that exceed the password lifetime.

Adding Users

Cisco ISE allows you to view, create, modify, duplicate, delete, change the status, import, export, or search for attributes of Cisco ISE users.

If you are using a Cisco ISE internal database, you must create an account for any new user who needs access to resources or services on a Cisco ISE network.

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

Step 2 Click **Add (+)** to create a new user.

Step 3 Enter values for the fields.

Do not include spaces in the username.

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

Related Topics

- Cisco ISE Users, page 14-1
- User Identity Groups, page 14-2
- User Account Custom Attributes and Password Policies, page 14-2
- Exporting Cisco ISE User Data, page 14-4
- Importing Cisco ISE User Data, page 14-4

Exporting Cisco ISE User Data

You might have to export user data from the Cisco ISE internal database. Cisco ISE allows you to export user data in the form of a password-protected csv file.

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

Step 2 Check the check box that corresponds to the user(s) whose data you want to export.

Step 3 Click **Export Selected**.

Step 4 Enter a key for encrypting the password in the Key field.

Step 5 Click **Start Export** to create a users.csv file.

Step 6 Click **OK** to export the users.csv file.

Related Topics

- Cisco ISE Users, page 14-1
- User Identity Groups, page 14-2
- User Account Custom Attributes and Password Policies, page 14-2
- Adding Users, page 14-3
- Importing Cisco ISE User Data, page 14-4

Importing Cisco ISE User Data

Cisco ISE allows you to import user data in the form of a csv file into its internal database. Instead of entering user accounts manually into Cisco ISE, you can import them.

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

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

Tip (Optional) If you do not have a comma-delimited text file, click **Generate a Template** to create this type of file.

Step 3 In the File text box, enter the filename containing the users to import, or click **Browse** and navigate to the location where the file resides.

Step 4 Check the **Create new user(s) and update existing user(s) with new data** check boxes if you want to both create new users and update existing users.

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

Related Topics

- Cisco ISE Users, page 14-1
- User Identity Groups, page 14-2
- User Account Custom Attributes and Password Policies, page 14-2
- Adding Users, page 14-3
- Exporting Cisco ISE User Data, page 14-4

Creating a User Identity Group

You must create a user identity group before you can assign a user to it.

Step 1 Choose **Administration > Identity Management > Groups > Identity Groups > User Identity Groups > Add**.

Step 2 Enter values in the Name and Description fields. Supported characters for the Name field are space # $ & ‘ ( ) * + - . / @ _ .

Step 3 Click **Submit**.

Related Topics

- Cisco ISE Users, page 14-1
- User Identity Groups, page 14-2
- Default User Identity Groups, page 14-2
- Exporting User Identity Groups, page 14-5
- Importing User Identity Groups, page 14-6

Exporting User Identity Groups

Cisco ISE allows you to export locally configured user identity groups in the form of a csv file.

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

Step 2 Check the check box that corresponds to the user identity group that you want to export, and click **Export**.

Step 3 Click **OK**.

Related Topics

- Cisco ISE Users, page 14-1
- User Identity Groups, page 14-2
- Creating a User Identity Group, page 14-5
- Importing User Identity Groups, page 14-6

Importing User Identity Groups

Cisco ISE allows you to import user identity groups in the form of a csv file.

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

Step 2 Click **Generate a Template** to get a template to use for the import file.

Step 3 Click **Import** to import network access users from a comma-delimited text file.

Step 4 Check the **Overwrite existing data with new data** check box if you want to both add a new user identity group and update existing user identity groups.

Step 5 Click **Import**.

Step 6 Click **Save** to save your changes to the Cisco ISE database.

Related Topics

- Cisco ISE Users, page 14-1
- User Identity Groups, page 14-2
- Creating a User Identity Group, page 14-5
- Exporting User Identity Groups, page 14-5

Identity Sources

Identity sources contain user information that Cisco ISE uses to validate credentials during user authentication, and to retrieve group information and other attributes that are associated with the user for use in authorization policies. They are databases that store user information in the form of records. You can add, edit, and delete user information from identity sources.

Cisco ISE supports internal and external identity sources. Both sources can be used as an authentication source for sponsor-user and guest-user authentication.

Related Topics

- Internal Identity Sources, page 14-7
- External Identity Sources, page 14-7

Internal Identity Sources

Cisco ISE has an internal user database that you can use to store user information. Users in the internal user database are called internal users. Cisco ISE also has an internal endpoint database that stores information about all the devices and endpoints that connect to it.

External Identity Sources

Cisco ISE allows you to configure the external identity source that contains user information. Cisco ISE connects to an external identity source to obtain user information for authentication. External identity sources also include certificate information for the Cisco ISE server and certificate authentication profiles. Cisco ISE uses authentication protocols to communicate with external identity sources. Table 14-1 lists authentication protocols and the external identity sources that they support.

Table 14-1 Authentication Protocols and Supported External Identity Sources

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 can optionally be added for authorization policy conditions.	Yes	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.

Related Topics

- Certificate Authentication Profiles, page 14-8
- Active Directory as an External Identity Source, page 14-9
- LDAP, page 14-20
- RADIUS Token Identity Sources, page 14-27
- RSA Identity Sources, page 14-33
- Identity Source Sequences, page 14-38
- Identity Source Details in Reports, page 14-40

Certificate Authentication Profiles

For each profile, you must specify the certificate field that should be used as the principal username and whether you want a binary comparison of the certificates.

Related Topics:

Adding a Certificate Authentication Profile, page 14-8

Adding a Certificate Authentication Profile

You must create a certificate authentication profile if you want to use the Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) certificate-based authentication method. Instead of authenticating via the traditional username and password method, Cisco ISE compares a certificate received from a client with one in the server to verify the authenticity of a user.

Before You Begin

You must be a Super Admin or System Admin.

For Windows certificate-based authentication, you must specify the Subject Alternative Name or Subject Name.

If you are authenticating via Anyconnect 3.1, you must specify the Subject Alternative Name for Microsoft certificates when using the EAP-FAST protocol with client-certificate authentication.

If you are using certificates issued by other certificate authorities, you need to specify the Common Name.

Step 1 Choose **Administration > Identity Management > External Identity Sources > Certificate Authentication Profile > Add**.

Step 2 Enter the name and description for the certificate authentication profile.

Step 3 Choose the **Principal Username X509** attribute.

Step 4 Check box if you want to validate certificate information for authentication against a selected Lightweight Directory Access Protocol (LDAP) or Microsoft Active Directory identity source. Check the **Perform Binary Certificate Comparison with Certificate Retrieved from LDAP or Active Directory** check box.

Note If you check this check box, you must choose the LDAP or Active Directory identity source from the available list.

Step 5 Choose the LDAP or Active Directory identity source against which you want to validate the certificate information for authentication.

Step 6 Click **Submit** to add the certificate authentication profile or save the changes.

What To Do Next:

1. See Chapter 19, "Managing Authentication Policies" for information on how to create authentication policies.
2. See Chapter 20, "Managing Authorization Policies and Profiles" for information on how to create authorization profiles and policies.

Active Directory as an External Identity Source

Cisco ISE uses Microsoft Active Directory (AD) as an external identity source to access resources such as users, machines, groups, and attributes.

Cisco ISE supports Microsoft AD sites and services when integrated with AD.

User and Machine Authentication in Active Directory

User and machine authentication in Active Directory allows network access only to users and devices that are listed in Active Directory.

Active Directory Supported Authentication Protocols and Features

Active Directory supports features such as user and machine authentications, changing Active Directory user passwords, and so on with some protocols. Table 14-2 lists the authentication protocols and the respective features that are supported by Active Directory.

Table 14-2 Active Directory Supported Authentication Protocols

Authentication Protocols	Features
EAP-FAST and Protected Extensible Authentication Protocol (PEAP)	User and machine authentication with the ability to change passwords using EAP-FAST and PEAP with an inner method of MS-CHAPv2 and EAP-GTC
Password Authentication Protocol (PAP)	Authentication and ability to change passwords
Microsoft Challenge Handshake Authentication Protocol Version 1 (MS-CHAPv1)	User and machine authentication
Microsoft Challenge Handshake Authentication Protocol Version 2 (MS-CHAPv2)	User and machine authentication

Table 14-2 Active Directory Supported Authentication Protocols

Authentication Protocols	Features
Extensible Authentication Protocol-Generic Token Card (EAP-GTC)	User and machine authentication
Extensible Authentication Protocol-Transport Layer Security (EAP-TLS)	User and machine authentication using the certificate retrieval option
Protected Extensible Authentication Protocol-Transport Layer Security (PEAP-TLS)	User and machine authentication
Lightweight Extensible Authentication Protocol (LEAP)	User authentication

Active Directory Attribute and Group Retrieval for Use in Authorization Policies

Cisco ISE retrieves user or machine attributes from Active Directory for use in authorization policy rules. These attributes are mapped to Cisco ISE policies and determine the authorization level for a user or machine. Cisco ISE retrieves user and machine Active Directory attributes after successful authentication and can also retrieve attributes for an authorization that is independent of authentication.

Cisco ISE performs user and group membership lookups via LDAP to an Active Directory. Group membership is used to map sponsor users to the corresponding sponsor group in ISE. And if the user is not directly in an Active Directory group, but is a member of a group that is a member of the Active Directory group (nested groups), the user authorization is rejected.

User authentication on an authorization policy fails if the rule contains an Active Directory group name with special characters such as /!@\#$%^&*()_+~

Active Directory Certificate Retrieval for Certificate-Based Authentication

Cisco ISE supports certificate retrieval for user and 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 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, the user or machine is granted access to the network.

Active Directory User Authentication Process Flow

When authenticating or querying a user, Cisco ISE checks 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 in 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 Active Directory Multidomain Forests

Cisco ISE supports Active Directory with 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.

In a multidomain environment, use the full domain name as ***username@domain.com*** and not just the username. If you are using the username alone, it might lead to failure in authentication.

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.

Refer to *Release Notes for Cisco Identity Services Engine, Release 1.2* for a list of Windows Server Operating Systems that support Active Directory services.

Guidelines for Setting Up Active Directory as an External Identity Source

Read the following statements carefully to ensure that these settings are configured properly for Cisco ISE to connect to Active Directory and successfully authenticate users:

- Use the Network Time Protocol (NTP) server settings to synchronize the time between the Cisco ISE server and Active Directory.
- If you have a firewall between Cisco ISE and Active Directory, ensure that the following ports are open for communication between Cisco ISE and Active Directory.

Protocol	Port Number
LDAP	389 (UDP)
SMB[1]	445 (TCP)
KDC[2]	88 (TCP)
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 Active Directory has a multidomain forest, ensure that trust relationships exist between the domain to which Cisco ISE is connected and the other domains that have user and machine information to which you need access. For more information on establishing trust relationships, refer to *Microsoft Active Directory documentation*.
- All of the Cisco ISE nodes in the deployment need to be able to perform forward and reverse Domain Name Service (DNS) lookup to effectively interoperate with Active Directory. DNS servers that you configure in Cisco ISE using the **ip name-server** command should be able to accurately resolve the domain names in an Active Directory identity source. The DNS server that is part of an Active Directory deployment is usually configured in Cisco ISE. If you have to configure multiple DNS servers, you can use the **application configure ise** command to do so.
- You must have at least one global catalog server operational in the domain to which you are joining Cisco ISE.
- The Active Directory username that you provide when joining to an Active Directory domain should be predefined in Active Directory and must have one of the following permissions:
  - Add the workstation to the domain to which you are trying to connect.
  - On the computer where the Cisco ISE account was created, establish permissions for creating or deleting computer objects before joining Cisco ISE to the domain.
  - Permissions for searching users and groups that are required for authentication.

  After you join Cisco ISE to the Active Directory domain, you will still need these permissions to:
  - Join any secondary Cisco ISE servers to this domain
  - Back up or restore data
  - Upgrade Cisco ISE to a higher version, if the upgrade process involves a backup and restore

Related Topics

- Specifying System Time and NTP Server Settings, page 5-3
- *Cisco Identity Services Engine CLI Reference Guide, Release 1.2*

Configuring Active Directory as an External Identity Source

Before You Begin

- Ensure that Cisco ISE hostnames are 15 characters or less in length. Active Directory does not validate hostnames larger than 15 characters.
- Ensure that the 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 in Microsoft Active Directory.
- To perform the following task, you must be a Super Admin or System Admin.

Note Even when Cisco ISE is connected to Active Directory, there may still be operation issues. To identify them refer to the Authentication Report under **Operations > Reports**.

You must complete the following tasks to configure Active Directory as an external identity source.

- Connecting to the Active Directory Domain, page 14-13

- Enabling Password Changes, Machine Authentications, Machine Access Restrictions, and Domain Stripping, page 14-14
- Configuring Active Directory User Groups, page 14-15

Connecting to the Active Directory Domain

Step 1 Connect to the Active Directory domain that contains the user and machine information.

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

Step 3 Enter the domain name and friendly name.

Step 4 Click **Save Configuration**. After you save the configuration successfully, the deployment join/leave table is displayed with all the Cisco ISE nodes, node roles, and their status.

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.

Step 5 Click **Join** to connect the Cisco ISE node to the Active Directory domain. You must do this explicitly even though you saved the configuration. You must join each of the secondary policy service nodes in your deployment individually.

Step 6 Check the check box next to the Cisco ISE node and click **Test Connection** to verify if the Cisco ISE node can be connected to the Active Directory domain. You can do a basic or a detailed test. A detailed test may take longer to complete for a large Active Directory deployment.

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

Note You cannot use an alternate User Principal Name (UPN) to join Cisco ISE to the Active Directory. If the 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, in the example.com domain there are two subdomains called sub1 and sub2. If the user belongs to sub1, then the username should be sub1\user1.

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**.

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

You can select more than one node to join to the Active Directory domain.

If the join operation is not successful, a failure message appears in the pop-up. You can click the failure message for each node to view detailed logs for that node.

Step 11 Click **Close**.

What To Do Next

Enabling Password Changes, Machine Authentications, Machine Access Restrictions, and Domain Stripping, page 14-14

Enabling Password Changes, Machine Authentications, Machine Access Restrictions, and Domain Stripping

Before you begin

- You must join Cisco ISE to the Active Directory domain
- Configure the advanced settings.

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

Step 2 Click the **Advanced Settings** tab.

Step 3 Check the **Enable Password Change** check box to allow users to change the user password in Active Directory.

Step 4 Check the **Enable Machine Authentication** check box to allow machine authentication.

Step 5 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.

Step 6 Enter the Aging Time if you have enabled MARs.

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

Step 7 Enter the prefixes and/or suffixes to be removed from the usernames during authentication by enabling the Identity Prefix Strip and/or Identity Suffix Strip. At the time of authentication to Active Directory Connector, Cisco ISE checks for matching prefixes and/or suffixes in the usernames. The matching characters are removed from the prefix and suffix of the username and the remaining part is passed to Active Directory.

You need to install Cisco ISE, Release 1.2.0.899 cumulative patch 4 or above to get these options.

While entering the list of prefixes or suffixes, follow the below guidelines:

- Enter multiple prefixes or suffixes separated only by commas. If you are using any other special character as a separator, it is considered as part of the prefix or suffix.
- Do not enter spaces as separators. You can use spaces only when they are part of the prefixes or suffixes.
- When prefixes are enabled, the characters that follow the last character of the matching prefix are considered as the username and processed for authentication. For example, if the prefix is **domain**, then the request **domain\jsmith** becomes **jsmith**.

  Some more examples with prefix list: dom1\,dom2$,dom3

  - **dom1\smith** becomes **smith**
  - **dom2$bdoe** becomes **bdoe**
  - **dom3ron** becomes **ron**
- When suffixes are enabled, the characters that precede the first character of the matching suffix are processed for authentication. For example, if the suffix is **@domain.com**, then the request **mary@domain.com** becomes **mary**.
- The Prefix and Suffix lists are enabled independently.

Note The “Network Access:UserName" attribute retains the fully qualified username. Hence even if the domain information is removed from the username, it is possible to define Authorization policy conditions based on the fully qualified username provided at the time of the RADIUS request.

Step 8 Click **Save Configuration**.

What To Do Next

Configuring Active Directory User Groups, page 14-15

Configuring Active Directory User Groups

You must configure Active Directory User Groups for them to be available for use in authorization policies.

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

Step 2 Click the **Groups** tab.

If you want to add groups from the directory, you can search for them using a filter. For example, enter **cn=users** as the filter criteria and click **Retrieve Groups** to view user groups that begin with cn=users. You can also enter the asterisk (*) wildcard character to filter the results

Step 3 Choose **Add > Add Group** to add a new group or choose **Add > Select Groups From Directory** to an existing group.

Step 4 Enter a name for a new group if you choose to add a group.

Step 5 Check the check boxes next to the groups that you want to be available for use in authorization policies and click **OK**.

Step 6 Click **Save Configuration**.

What To Do Next

Configuring Active Directory User Attributes, page 14-15

Configuring Active Directory User Attributes

You must configure Active Directory user attributes to be able to use them in authorization policy conditions.

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

Step 2 Click the **Attributes** tab.

If you choose to add attributes from directory, enter the name of a user in the Example User field, and click **Retrieve Attributes** to obtain a list of attributes for users. For example, enter **admin** to obtain a list of administrator attributes. You can also enter the asterisk (*) wildcard character to filter the results.

Step 3 Choose **Add > Add Attribute** to add a new attribute or choose **Add > Select Attributes From Directory** to choose a list of attributes from the directory.

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

Step 4 Enter a name for a new attribute if you choose to add an attribute.

Step 5 Check the check boxes next to the attributes from Active Directory that you want to select, and click **OK**.

Step 6 Click **Save Configuration**.

What To Do Next

1. See Chapter 19, "Managing Authentication Policies" for information on how to create authentication policies.
2. See Chapter 20, "Managing Authorization Policies and Profiles" for information on how to create authorization profiles and policies.

Leaving the Active Directory Domain

If you no longer need to authenticate users or machines from Active Directory, you can leave the Active Directory domain.

When you reset the Cisco ISE application configuration from the command-line interface, it performs a leave operation disconnecting the ISE node from the Active Directory domain, if it is already joined. However, the Cisco ISE node account is not removed from the Active Directory domain. We recommend that you perform a leave operation from the Admin portal with the Active Directory credentials and it removes the node account from the Active Directory domain.

Before You Begin

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 Directory 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.

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

Step 2 Check the check box next to the Cisco ISE node and click **Leave**.

Step 3 Enter the Active Directory username and password, and click **OK** to leave the domain and remove the configuration from the Cisco ISE database.

Step 4 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 leaves 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 enter the Active Directory credentials, the Cisco ISE node leaves the Active Directory domain and deletes the configuration from the Active Directory database.

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

Related Topics

Deleting Active Directory Configurations, page 14-17

Deleting Active Directory Configurations

You should delete Active Directory configurations if you are not going to use Active Directory as an external identity source. 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.

Before You Begin

Ensure that you have left the Active Directory domain.

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

Step 2 Check and ensure that the Local Node status is listed as Not Joined.

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.

Related Topics

Leaving the Active Directory Domain, page 14-16

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.

Step 1 Choose **Administration > System > Logging > Debug Log Configuration**.

Step 2 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**.

Step 3 Click the **Active Directory** radio button, and click **Edit**.

Step 4 Choose DEBUG from the drop-down list next to Active Directory.

Step 5 Click **Save**.

Obtaining Active Directory Log File for Troubleshooting

If you have issues with Active Directory configuration, you can download and view the Active Directory debug logs to troubleshoot your problems.

Before You Begin

You must enable the Active Directory debug log configuration.

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

Step 2 Click the node from which you want to obtain the Active Directory debug log file.

Step 3 Click the **Debug Logs** tab.

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

Related Topics

Enabling Active Directory Debug Logs, page 14-17

Supplemental Information for Setting Up Cisco ISE with Active Directory

This section provides pointers to help you set up Cisco ISE with Active Directory:

- Configuring Group Policies in Active Directory, page 14-18
- Configuring Odyssey 5.X Supplicant for EAP-TLS Machine Authentications Against Active Directory, page 14-19
- AnyConnect Agent for Machine Authentication, page 14-20

Configuring Group Policies in Active Directory

For more information about how to access the Group Policy management editor, refer to *Microsoft Active Directory Documentation*.

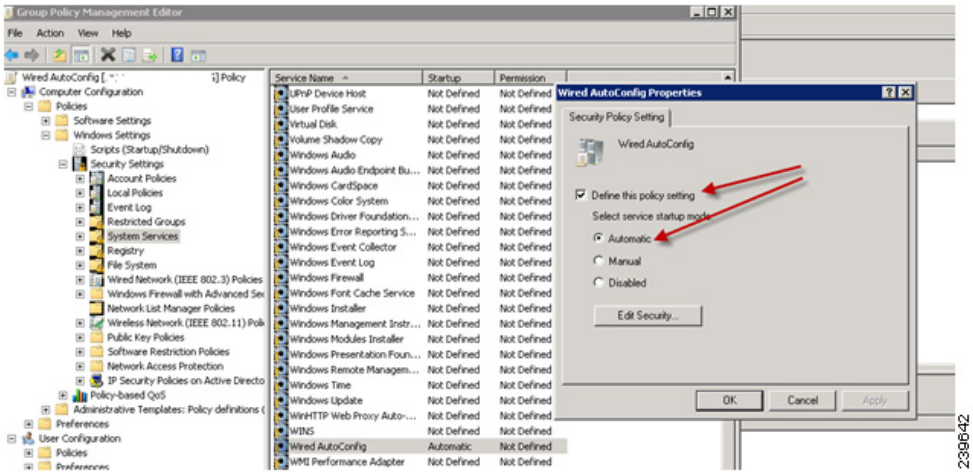
Step 1 Open the Group Policy management editor as shown in Figure 14-1 and create a new policy object or add to an existing domain policy.

Figure 14-1 Group Policy Objects

Step 2 Create a new policy and enter a descriptive name for it. For example, you might use Wired Autoconfiguration.

Step 3 Check the **Define this policy setting** check box, and click the **Automatic** radio button for the service startup mode as shown in Figure 14-2.

Figure 14-2 Policy Properties



Step 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.

Configuring 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 the supplicant.

Step 1 Start Odyssey Access Client.

Step 2 Choose **Odyssey Access Client Administrator** from the Tools menu.

Step 3 Double-click the **Machine Account** icon.

Step 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.** On the Authentication tab, choose **EAP-TLS** as the authentication method.
- **d.** On the Certificate tab, check the **Permit login using my certificate** check box, and choose a certificate for the supplicant machine.
- **e.** On 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 fails.

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.

Related Topics

Adding LDAP Identity Sources, page 14-25

LDAP Directory Service

LDAP directory service is based on a client-server model. A client starts an LDAP session by connecting to an LDAP server and sending 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 a directory, which is a database that holds 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.

Related Topics

Adding LDAP Identity Sources, page 14-25

Multiple LDAP Instances

By creating more than one LDAP instance with different IP addresses or port settings, you can configure Cisco ISE to authenticate 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 and group directory subtree combination for which Cisco ISE submits authentication requests.

Related Topics

Adding LDAP Identity Sources, page 14-25

LDAP Failover

Cisco ISE supports failover between a primary LDAP server and a secondary LDAP server. A failover occurs when an authentication request fails because Cisco ISE could not connect to an LDAP server because it is down or is otherwise unreachable.

If you establish failover settings and the first LDAP server that Cisco ISE attempts to contact cannot be reached, Cisco ISE always attempts to contact a second LDAP server. If you want Cisco ISE to use the first LDAP server again, you must enter a value 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 Admin portal, so the primary LDAP server must be accessible when you configure these items. Cisco ISE uses the secondary LDAP server only for authentications and authorizations at run time, according to the failover configuration.

Related Topics

Adding LDAP Identity Sources, page 14-25

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 open 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.

Related Topics

Adding LDAP Identity Sources, page 14-25

LDAP User Authentication

LDAP can be used as an external database for Cisco ISE user authentication. Cisco ISE supports plain password authentication. User authentication includes:

- 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 a group's membership information for use in policies
- Retrieving values for specified attributes 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.

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

Related Topics

Adding LDAP Identity Sources, page 14-25

LDAP Group and Attribute Retrieval for Use in Authorization Policies

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 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 Admin portal 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.

Related Topics

- Adding LDAP Identity Sources, page 14-25
- LDAP Connection Management, page 14-21

LDAP Group Membership Information Retrieval

For user authentication, user lookup, and MAC address lookup, Cisco ISE must retrieve 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 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 the attribute that contains 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 stored in the group member attribute (either as DNs or plain usernames).

Related Topics

Adding LDAP Identity Sources, page 14-25

LDAP 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 the authentication or lookup process does not fail.

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.

Related Topics

Adding LDAP Identity Sources, page 14-25

LDAP 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.

Related Topics

Adding LDAP Identity Sources, page 14-25.

Errors Returned by the LDAP Server

The following errors can occur during the authentication process:

- Authentication Errors—Cisco ISE logs authentication errors in the Cisco ISE log files.

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)
- Initialization Errors—Use the LDAP server timeout settings to configure the number of seconds that Cisco ISE should wait 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:
  - LDAP is not supported.
  - The server is down.
  - The server is out of memory.
  - The user has no privileges.
  - Administrator credentials are configured incorrectly.

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

Related Topics

Adding LDAP Identity Sources, page 14-25

LDAP User Lookup

Cisco ISE supports the user lookup feature with an 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 a user's group membership information for use in policies
- Retrieving values for specified attributes for use in policies and authorization profiles

Related Topics

Adding LDAP Identity Sources, page 14-25

LDAP 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 a MAC Address group information for the device for use in policies
- Retrieving values for specified attributes for use in policies

Related Topics

Adding LDAP Identity Sources, page 14-25

Adding LDAP Identity Sources

Before You Begin

- To perform the following task, you must be a Super Admin or System Admin.
- Cisco ISE always uses the primary LDAP server to obtain groups and attributes for use in authorization policies. Therefore, your primary LDAP server must be reachable when you configure these items.

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

Step 2 Enter the values.

Step 3 Click **Submit** to create an LDAP instance.

Related Topics

LDAP Identity Source Settings, page A-29

What To Do Next

- Configuring Primary and Secondary LDAP Servers, page 14-25
- Enabling Cisco ISE to Obtain Attributes from the LDAP Server, page 14-26
- Retrieving Group Membership Details from the LDAP Server, page 14-26
- Retrieving User Attributes From the LDAP Server, page 14-27

Configuring Primary and Secondary LDAP Servers

After you create an LDAP instance, you must configure the connection settings for the primary LDAP server. Configuring a secondary LDAP server is optional.

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

Step 2 Check the check box next to the LDAP instance that you want to edit and click **Edit**.

Step 3 Click the **Connection** tab to configure the primary and secondary servers.

Step 4 Enter the values as described in LDAP Connection Settings.

Step 5 Click **Submit** to save the connection parameters.

Related Topics

- Adding LDAP Identity Sources, page 14-25
- Enabling Cisco ISE to Obtain Attributes from the LDAP Server, page 14-26
- Retrieving Group Membership Details from the LDAP Server, page 14-26
- Retrieving User Attributes From the LDAP Server, page 14-27

LDAP Connection Tab Field Settings

The following table describes the fields in **Administration > Identity Management > External Identity Sources > LDAP** Edit page.

Enabling Cisco ISE to Obtain Attributes from the LDAP Server

For Cisco ISE to obtain user and group data from an LDAP server, you must configure LDAP directory details in Cisco ISE. 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 > LDAP**.

Step 2 Check the check box next to the LDAP instance that you want to edit and click **Edit**.

Step 3 Click the **Directory Organization** tab.

Step 4 Enter the values as described in LDAP Directory Organization Settings.

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

Retrieving Group Membership Details from the LDAP Server

You can add new groups or select groups from the LDAP directory.

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

Step 2 Check the check box next to the LDAP instance that you want to edit and click **Edit**.

Step 3 Click the **Groups** tab.

Step 4 Choose **Add > Add Group** to add a new group or choose **Add > Select Groups From Directory** to select the groups from the LDAP directory.

- **a.** If you choose to add a group, enter a name for the new group.
- **b.** If you are selecting from the directory, enter the filter criteria, and click **Retrieve Groups**. Your search criteria can contain the asterisk (*) wildcard character.

Step 5 Check the check boxes next to the groups that you want to select and click **OK**.

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

Step 6 Click **Submit** to save the group selection.

Retrieving User Attributes From the LDAP Server

You can obtain user attributes from the LDAP server for use in authorization policies.

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

Step 2 Check the check box next to the LDAP instance that you want to edit and click **Edit**.

Step 3 Click the **Attributes** tab.

Step 4 Choose **Add > Add Attribute** to add a new attribute or choose **Add > Select Attributes From Directory** to select attributes from the LDAP server.

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

b. If you are selecting from the directory, enter an example user and click **Retrieve Attributes** to retrieve the user's attributes. You can use the asterisk (*) wildcard character.

Step 5 Check the check boxes next to the attributes that you want to select, then click **OK**.

Step 6 Click **Submit** to save the attribute selections.

What To Do Next:

1. See Chapter 19, "Managing Authentication Policies" for information on how to create authentication policies.
2. See Chapter 20, "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 a RADIUS server. A 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 a user. RADIUS identity sources use the User Datagram Protocol (UDP) port for authentication sessions. The same UDP port is used for all RADIUS communication.

Related Topics

- Adding a RADIUS Token Server, page 14-31
- Deleting a RADIUS Token Server, page 14-32

RADIUS Token Server Supported Authentication Protocols

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

- RADIUS PAP
- Protected Extensible Authentication Protocol (PEAP) with inner Extensible Authentication Protocol-Generic Token Card (EAP-GTC)
- EAP-FAST with inner EAP-GTC

Related Topics

- Adding a RADIUS Token Server, page 14-31
- Deleting a RADIUS Token Server, page 14-32

Ports Used By the RADIUS Token Servers for Communication

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. You can configure the UDP port through the Admin portal.

Related Topics

- Adding a RADIUS Token Server, page 14-31
- Deleting a RADIUS Token Server, page 14-32

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.

Related Topics

- Adding a RADIUS Token Server, page 14-31
- Deleting a RADIUS Token Server, page 14-32

Failover in RADIUS Token Servers

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.

Related Topics

- Adding a RADIUS Token Server, page 14-31
- Deleting a RADIUS Token Server, page 14-32

Configurable Password Prompt in RADIUS Token Servers

RADIUS identity sources allow you to configure the password prompt. You can configure the password prompt through the Admin portal.

Related Topics

- Adding a RADIUS Token Server, page 14-31
- Deleting a RADIUS Token Server, page 14-32

RADIUS Token Server 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.

Related Topics

- Adding a RADIUS Token Server, page 14-31
- Deleting a RADIUS Token Server, page 14-32

User Attribute Cache in RADIUS Token Servers

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 Admin portal. 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.

Related Topics

- Adding a RADIUS Token Server, page 14-31
- Deleting a RADIUS Token Server, page 14-32

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 errors while authenticating with a RADIUS server. RADIUS servers return an Access-Reject message for all errors. 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.

Related Topics

- Adding a RADIUS Token Server, page 14-31
- Deleting a RADIUS Token Server, page 14-32

RADIUS Server Returns the Same Message for All Errors

When a user is not found in the RADIUS server, the RADIUS server returns an Access-Reject message. Cisco ISE provides an option to configure this message through the Admin portal as either an Authentication Failed or a User Not Found message. 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 14-3 lists the different failure cases that are possible with RADIUS identity servers.

Table 14-3 Error Handling

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

Related Topics

- Adding a RADIUS Token Server, page 14-31
- Deleting a RADIUS Token Server, page 14-32

Safeword Server Supports Special Username Format

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 Admin portal 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.

Related Topics

- Adding a RADIUS Token Server, page 14-31
- Deleting a RADIUS Token Server, page 14-32

Authentication Request and Response in RADIUS Token Servers

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.

Related Topics

- Adding a RADIUS Token Server, page 14-31
- Deleting a RADIUS Token Server, page 14-32

Adding a RADIUS Token Server

Before You Begin

To perform the following task, you must be a Super Admin or System Admin.

Step 1 Choose **Administration > Identity Management > External Identity Sources > RADIUS Token > Add**.

Step 2 Enter the values in the General and Connection tabs.

Step 3 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 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 4 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 5 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 6 Click **Submit** to save the RADIUS Token identity source.

What To Do Next

1. See Chapter 19, "Managing Authentication Policies" for information on how to create authentication policies.
2. See Chapter 20, "Managing Authorization Policies and Profiles" for information on how to create authorization profiles and policies.

Related Topics

RADIUS Token Identity Sources Settings, page A-32

Deleting a RADIUS Token Server

Before You Begin

- To perform the following task, you must be a Super Admin or System Admin.
- 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 fails.

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

Step 2 Check the check box next to the RADIUS token server or servers that you want to delete, then click **Delete**.

Step 3 Click **OK** to delete the RADIUS token server or servers that you have selected.

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 connects with the RSA SecurID authentication technology by using the RSA SecurID Agent.

Cisco ISE Release 1.2 supports only one RSA realm.

This section contains the following topics:

- Cisco ISE and RSA SecurID Server Integration, page 14-33
- Configuring RSA Prompts, page 14-37
- Configuring RSA Messages, page 14-38

Cisco ISE and RSA SecurID Server Integration

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

- RSA Server Administrator—Configures and maintains RSA systems and integration
- Cisco ISE Administrator—Configures Cisco ISE to connect to the RSA SecurID server and maintains the configuration

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

RSA Configuration 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.

RSA Agent Authentication 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.

RSA Identity Sources in a Distributed Cisco ISE Environment

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.

RSA Server Updates in a Cisco ISE Deployment

After you have added the sdconf.rec file in Cisco ISE, the RSA SecurID administrator might 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).

Override 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 for each Cisco ISE server for the realm using a text file called sdopts.rec through the Admin portal. Refer to the RSA documentation for information on how to create this file.

RSA Node Secret Reset

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 Admin portal to delete this file from a 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 1.2, you must reset the RSA secret.

RSA Automatic Availability Reset

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 Admin portal 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 is deleted whenever the securid file is reset, or the sdconf.rec or sdopts.rec files are updated.

Related Topics

- Importing the RSA Configuration File, page 14-35
- Configuring the Options File for a Cisco ISE Server and Resetting SecurID and sdstatus.12 Files, page 14-36
- Adding RSA Identity Sources, page 14-35

Adding RSA Identity Sources

To create an RSA identity source, you must import the RSA configuration file (sdconf.rec). See the "Importing the RSA Configuration File" section on page 14-35 for more information.

Before You Begin

- You must obtain the sdconf.rec file from your RSA administrator.
- To perform the following task, you must be a Super Admin or System Admin.

Adding an RSA identity source involves the following tasks:

- Importing the RSA Configuration File, page 14-35
- Configuring the Options File for a Cisco ISE Server and Resetting SecurID and sdstatus.12 Files, page 14-36
- Configuring Authentication Control Options for RSA Identity Source, page 14-37

Importing the RSA Configuration File

You must import the RSA configuration file to add an RSA identity source in Cisco ISE.

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

Step 2 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 3 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 to 199. The default value is 30 seconds.

Step 4 Check the **Reauthenticate on Change PIN** check box to force a reauthentication when the PIN is changed.

Step 5 Click **Save**.

Cisco ISE also supports the following scenarios:

- Configuring the Options File for a Cisco ISE Server and Resetting SecurID and sdstatus.12 Files, page 14-36
- Configuring Authentication Control Options for RSA Identity Source, page 14-37

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

Step 1 Log into the Cisco ISE server.

Step 2 Choose **Administration > Identity Management > External Identity Sources > RSA SecurID > Add**.

Step 3 Click the **RSA Instance Files** tab.

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

Step 4 Click the radio button next to the sdopts.rec file for a particular Cisco ISE server, and click **Update Options File**.

The existing file is displayed in the Current File region.

Step 5 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 6 Click **OK**.

Step 7 Click the row that corresponds to the Cisco ISE server to reset the securid and sdstatus.12 files for that server:

a. 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.

b. Click **Save** in this row to save the changes.

Step 8 Click **Save**.

Configuring Authentication Control Options for RSA Identity Source

You can specify how Cisco ISE defines authentication failures and 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 Cisco ISE should handle such failures while processing requests and 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.

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

Step 2 Click the **Authentication Control** tab.

Step 3 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 4 Click **Save** to save the configuration.

What To Do Next

1. See Chapter 19, "Managing Authentication Policies" for information on how to create authentication policies.
2. See Chapter 20, "Managing Authorization Policies and Profiles" for information on how to create authorization profiles and policies.

Related Topics

- RSA Identity Sources, page 14-33
- Configuring RSA Prompts, page 14-37
- Configuring RSA Messages, page 14-38

Configuring RSA Prompts

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

Before You Begin

To perform the following task, you must be a Super Admin or System Admin.

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

Step 2 Click **Prompts**.

Step 3 Enter the information as described in RSA Prompt Settings.

Step 4 Click **Submit**.

Related Topics

- RADIUS Token Identity Sources, page 14-27
- Adding RSA Identity Sources, page 14-35
- Configuring RSA Messages, page 14-38

Configuring RSA Messages

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

Before You Begin

To perform the following task, you must be a Super Admin or System Admin.

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

Step 2 Click **Prompts**.

Step 3 Click the **Messages** tab.

Step 4 Enter the information as described in RSA Message Settings.

Step 5 Click **Submit**.

Related Topics

- RADIUS Token Identity Sources, page 14-27
- Adding RSA Identity Sources, page 14-35
- Configuring RSA Prompts, page 14-37

Identity Source Sequences

Identity source sequences define the order in which Cisco ISE looks for user credentials in the different databases. Cisco ISE supports the following identity sources:

- Internal Users
- Guest Users
- Active Directory
- LDAP
- RSA

- RADIUS Token Servers
- Certificate Authentication Profiles

If you have user information in more than one of the databases that are connected to Cisco ISE, you can define the order in which you want Cisco ISE to look for information in these identity sources. 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.

Related Topics

- Creating Identity Source Sequences, page 14-39
- Deleting Identity Source Sequences, page 14-40

Creating Identity Source Sequences

Before You Begin

Ensure that you have configured your external identity sources in Cisco ISE. See the "Identity Source Sequences" section on page 14-38 for information on how to configure external identity sources.

To perform the following task, you must be a Super Admin or System Admin.

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 the Identity Source Sequence for Sponsors" section on page 16-8 for more information on how to configure Guest Portal authentication source.

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

Step 2 Enter a name for the identity source sequence. You can also enter an optional description.

Step 3 Check the **Select Certificate Authentication Profile** check box and choose a certificate authentication profile, if you wish to use a certificate authentication profile for authentication.

Step 4 Choose the database or databases that you want to include in the identity source sequence in the Selected List box.

Step 5 Rearrange the databases in the Selected list in the order in which you want Cisco ISE to search the databases.

Step 6 Choose one of the following options in the Advanced Search List area:

- **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.

While processing a request, Cisco ISE searches 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 them.

Step 7 Click **Submit** to create the identity source sequence that you can then use in policies.

Related Topics

- Configuring a Simple Authentication Policy, page 19-21
- Configuring a Rule-Based Authentication Policy, page 19-22

Deleting Identity Source Sequences

You can delete identity source sequences that you no longer use in policies.

Before You Begin

- Ensure that the identity source sequence that you are about to delete is not used in any authentication policy.
- To perform the following task, you must be a Super Admin or System Admin.

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

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

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

Identity Source Details in Reports

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

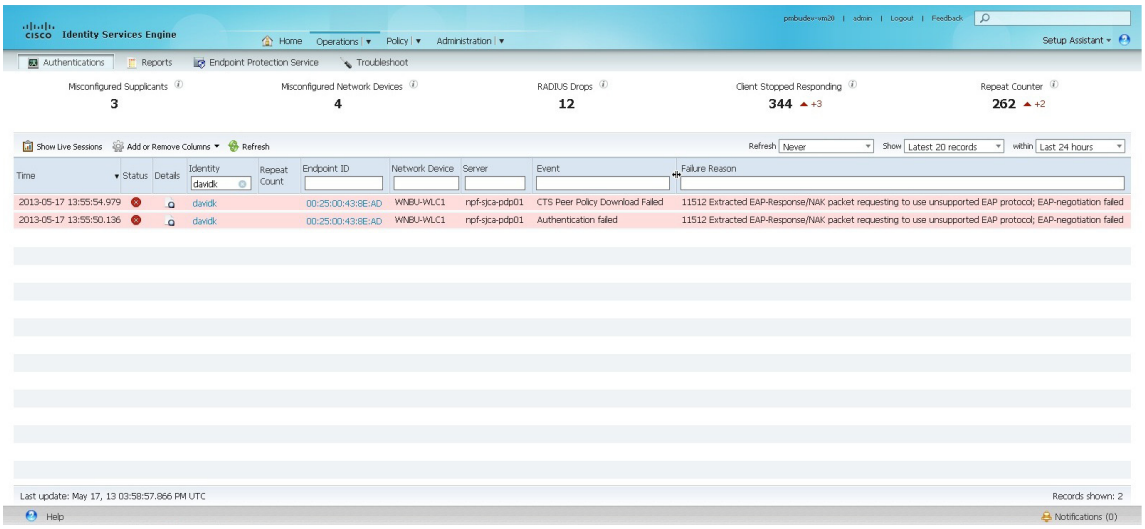
- Authentications Dashlet, page 14-40
- Identity Source Reports, page 14-41

Authentications Dashlet

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

Figure 14-3 shows the Authentications page and highlights the magnifier icon that you must click to drill down for details.

Figure 14-3 Authentications Page



For more information on the Authentications page, see the "Live Authentications" section on page 25-13.

Identity Source Reports

Cisco ISE provides various reports that include information about identity sources. See the "Available Reports" section on page 26-6 for a description of these reports.

Related Topics

- Running and Viewing Reports, page 26-2
- Exporting Reports, page 26-2