Manage Users and External Identity Sources

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.

From Cisco ISE Release 3.2, you can choose to add the **Date Enabled** column (**Settings** > **Columns** > **Date Enabled**) and the **Days Until Password Expires** column (**Settings** > **Columns** > **Days Until Password Expires**) to the **Network Access User** table in the **Network Access Users** window (**Administration** > **Identity Management** > **Identities** > **Users**) to help you sort through network access users by using their password expiry information. These fields are not added by default. You can add them to the table using the customization option in the window.

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

Cisco ISE allows you to restrict network access based on user attributes for both network access users and administrators. 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.

Custom User Attributes

You can configure more user-account attributes on the **User Custom Attributes** window (**Administration > Identity Management > Settings > User Custom Attributes**). You can also view the list of predefined user attributes in this window. You cannot edit the predefined user attributes.

Enter the required details in the **User Custom Attributes** pane to add a new custom attribute. The custom attributes and the default values that you add on the **User Custom Attributes** window are displayed while adding or editing a Network Access user (**Administration > Identity Management > Identities > Users > Add/Edit**) or Admin user (**Administration > System > Admin Access > Administrators > Admin Users > Add/Edit**). You can change the default values while adding or editing a Network Access or Admin user.

You can select the following data types for the custom attributes on the **User Custom Attributes** window:

- String: You can specify the maximum string length (maximum allowed length for a string attribute value).
- Integer: You can configure the minimum and maximum value (specifies the lowest and the highest acceptable integer value).
- Enum: You can specify the following values for each parameter:
  - Internal value
  - Display value

  You can also specify the default parameter. The values that you add in the Display field are displayed while adding or editing a Network Access or Admin user.
- Float
- Password: You can specify the maximum string length.
- Long: You can configure the minimum and maximum value.
- IP: You can specify a default IPv4 or IPv6 address.
- Boolean: You can set either True or False as the default value.
- Date: You can select a date from the calendar and set it as the default value. The date is displayed in yyyy-mm-dd format.

Check the **Mandatory** check box if you want to make an attribute mandatory while adding or editing a Network Access or Admin user. You can also set default values for the custom attributes.

The custom attributes can be used in the authentication policies. The data type and the allowable range that you set for the custom attributes are applied to the custom attribute values in the policy conditions.

User Authentication Settings

Not all external identity stores allow network access users to change their passwords. See the section for each identity source for more information.

Network-use password rules should be configured in **Administration** > **Identity Management** > **Settings** > **User Authentication Settings**.

The following section has additional information about some of the fields in the **Password Policy** tab.

- **Required Characters**: If you configure a user-password policy that requires upper or lowercase characters, and the user's language does not support these characters, the user cannot set a password. To support UTF-8 characters, uncheck the following check boxes:
  - **Lowercase Alphabetic Characters**
  - **Uppercase Alphabetic Characters**

- **Password Change Delta**: Specifies the minimum number of characters that must change when changing the current password to a new password. Cisco ISE does not consider changing the position of a character as a change. For Example, if the password delta is 3, and the current password is "?Aa1234?", then "?Aa1567?" ("5","6" and "7" are the three new characters) is a valid new password. "?Aa1562?" fails, because "?","2", and "?" characters are in the current password. "Aa1234??" fails, because even though the character positions changed, the same characters are in the current password.

  Password change delta also considers the previous X passwords, where X is the value of **Password must be different from the previous versions**. If your password delta is 3, and your password history is 2, then you must change the four characters that are not a part of the past two passwords.

- **Dictionary words**: Check this check box to restrict the use of any dictionary word, its characters in reverse order, or its letters replaced with other characters.

  Substitution of "$" for "s", "@" for "a", "0" for "o", "1" for "l", "!" for "i", "3" for "e", is not permitted. For example, "Pa$$w0rd".

  - **Default Dictionary**: Choose this option to use the default Linux dictionary in Cisco ISE. The default dictionary contains approximately 480,000 English words.
  - **Custom Dictionary**: Choose this option to use your customized dictionary. Click **Choose File** to select a custom dictionary file. The text file must be of newline-delimited words, .dic extension, and size less than 20 MB.

- You can use the **Password Lifetime** section to update the password reset interval and reminder. To set the lifetime of a password, check the **Change password every __ days (valid range 1 to 3650)** check box, and enter the number of days in the input field. A user account can be disabled if a user does not change the password in the specified time by selecting the **Disable User Account** option. Choose the **Require password change on next login** to prompt the user to change their password the next time they login to Cisco ISE.

  To send a reminder email for password reset, check the **Display Reminder __ Days Prior to Password Expiration** check box and enter the number of days before which a reminder email should be sent to the email address configured for the network access user. While creating a network access user, you can add the email address in the **Administration > Identity Management > Identities > Users > Add Network Access User** window to send an email notification for password reset.

Note

- The reminder email is sent from the following email address: iseadminportal@<ISE-Primary-FQDN>. You must explicitly permit access for this sender.
- By default, the reminder email has the following content: Your network access password will expire on <*password expiry date and time*>. Please contact your system administrator for assistance.

  From Cisco ISE Release 3.2, you can customize the email content after the *Please contact your system administrator for assistance* portion of the email notification.

- **Lock/Suspend Account with Incorrect Login Attempts**: Use this option to suspend or lock an account if the login attempt failed for the specified number of times. The valid range is from 3 to 20.
- **Account Disable Policy**: Configure the rules about when to disable an existing user account. See Disable User Accounts Globally for more information.

Related Topics

User Account Custom Attributes, on page 2
To Add Users, on page 5

Generate Automatic Password for Users and Administrators

You can use the **Generate Password** option on the user and administrator creation window to generate instant password adhering to Cisco ISE password policies. This helps the users or administrators to use the password generated by Cisco ISE than spending time in thinking of a safe password to be configured.

The **Generate Password** option is available in the following windows:

- **Administration > Identity Management > Identities > Users**.
- **Administration > System > Admin Access > Administrators > Admin Users**.
- **Settings > Account Settings > Change Password**.

To Add 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 the resources or services on a Cisco ISE network.

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

You can also create users by accessing the **Work Centers** > **Device Administration** > **Identities** > **Users** window.

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

Step 3 Enter values in all the fields the fields**.**

Note Do not include space, +, and * characters in the username.

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

Export 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.

Import Cisco ISE Internal Users

You can import new user data into Cisco ISE with a CSV file to create new internal accounts. A template CSV file is available for download while you import user accounts. Sponsors can import users on the Sponsor portal. See Configure Account Content for Sponsor Account Creation for information about configuring the information types that the sponsor guest accounts use.

Note If the CSV file contains custom attributes, the data type and the allowable range that you set for the custom attributes will be applied for the custom attribute values during import.

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

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

If you do not have a comma-delimited text file, click **Generate a Template** to create a CSV file with the heading rows filled in.

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 box if you want to create new users and update existing users.

Step 5 Click **Save**.

Note We recommend that you do not delete all the network access users at a time, because this may lead to CPU spike and the services to crash, especially if you are using a very large database.

Create 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**.

You can also create a user identity group by accessing the **Work Centers** > **Device Administration** > **User Identity Groups** > **Identity Groups** > **User Identity Groups** > **Add** page.

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

Step 3 Click **Submit**.

Related Topics

User Identity Groups, on page 2

Export 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**.

Import 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.

Create Authorization Policy Using External Identity Sources

Following are the steps for creating an authorization policy using external identity sources:

Step 1 Choose **Policy** > **Authorization** to create a new authorization policy rule under Standard policies.

If you enabled Policy Sets, choose **Policy** > **Policy Set**, pick the Policy Set you plan to use for this portal, expand Authorization Policy, and add a new rule.

Step 2 For **Conditions**, select an endpoint identity group that you want to use for the portal validation.

When the external identity source (for example, RSA SecurID) is used with the internal user group, you should create the condition using the following syntax:

```
InternalUser:IdentityGroup EQUALS User Identity Groups:Group_Name
```

Prefix the group name with "User Identity Groups:" without the quotes.

Step 3 For **Permissions**, select the portal authorization profile that you created.

Configure Maximum Concurrent Sessions

For optimal performance, you can limit the number of concurrent user sessions. You can set the limits at the user level or at the group level. Depending upon the maximum user session configurations, the session count is applied to the user.

You can configure the maximum number of concurrent sessions for each user per ISE node. Sessions above this limit are rejected.

Step 1 Choose **Administration > System > Settings > Max Sessions > User**.

Step 2 Do one of the following:

- Enter the maximum number of concurrent sessions that are allowed for each user in the **Maximum Sessions per User** field.
- Check the **Unlimited Sessions** check box if you want the users to have unlimited sessions. This option is selected by default.

Step 3 Click **Save**.

If the maximum number of sessions is configured at both the user and group level, the smaller value will have precedence. For example, if the maximum session value for a user is set as 10 and the maximum session value of the group to which the user belongs is set as 5, the user can have a maximum of 5 sessions only.

Note The maximum concurrent session count is managed by the PSN in which it is configured. This count is not synchronized among the PSNs. If the authentication is done in Cisco ISE, where the maximum concurrent sessions per user or group is configured, and authorization is done in a different proxy server, then the maximum concurrent session limit is applicable only in the Cisco ISE and is not applied to the proxy server.

Maximum concurrent session count is implemented in the runtime process and the data is stored only in the memory. If the PSN is restarted, the maximum concurrent session counters are reset.

Maximum concurrent session count is case insensitive with respect to usernames irrespective of the Network Access Device used (when the same PSN node is used)

Maximum Concurrent Sessions for a Group

You can configure the maximum number of concurrent sessions for the identity groups.

Sometimes all the sessions can be used by a few users in the group. Requests from other users to create a new session are rejected because the number of sessions has already reached the maximum configured value. Cisco ISE allows you to configure a maximum session limit for each user in the group; each user belonging to a specific identity group cannot open sessions more than the session limit, irrespective of the number of sessions other users from the same group have opened. When calculating the session limit for a particular user, the lowest configuration value takes the precedence—whether the global session limit per user, the session limit per identity group that the user belongs to, or the session limit per user in the group.

To configure maximum number of concurrent sessions for an identity group:

Step 1 Choose **Administration > System > Settings > Max Sessions > Group**.

All the configured identity groups are listed.

Step 2 Click the Edit icon next to the group that you want to edit and enter the values for the following:

- Maximum number of concurrent sessions permitted for that group. If the maximum number of sessions for a group is set as 100, the total count of all sessions established by all members of that group cannot exceed 100.

  Note Group-level session limits are applied based on the group hierarchy.

- Maximum number of concurrent sessions permitted for each user in that group. This option overrides the maximum number of sessions for a group.

If you want to set the maximum number of concurrent sessions for a group or maximum concurrent sessions for the users in a group as Unlimited, leave the **Max Sessions for Group/Max Sessions for User in Group** field blank, click the Tick icon, and then click Save. By default, both these values are set as Unlimited.

Step 3 Click **Save**.

Configure Counter Time Limit

You can configure the timeout value for concurrent user sessions.

Step 1 Choose **Administration > System > Settings > Max Sessions > Counter Time Limit**.

Step 2 Select one of the following options:

- **Unlimited**: Check this check box if you do not want to set any timeout or time limit for the sessions.
- **Delete sessions after**: You can enter the timeout value for concurrent sessions in minutes, hours, or days. When a session exceeds the time limit, Cisco ISE deletes the session from the counter and updates the session count, thereby allowing new sessions. Users will not be logged out if their sessions exceed the time limit.

Step 3 Click **Save**.

You can reset the session count from the RADIUS Live Logs window. Click the Actions icon displayed on the Identity, Identity Group, or Server column to reset the session count. When you reset a session, the session is deleted from the counter (thereby allowing new sessions). Users will not be disconnected if their sessions are deleted from the counter.

Disable Individual User Accounts

Cisco ISE allows you to disable the user account for each individual user if the disable account date exceeds the date specified by the admin user.

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

Step 2 Click **Add** to create a new user or check the check box next to an existing user and click **Edit** to edit the existing user details.

Step 3 Check the **Disable account if the date exceeds** check box and select the date.

This option allows you to disable the user account when the configured date exceeds at user level. You can configure different expiry dates for different users as required. This option overrules the global configuration for each individual user. The configured date can either be the current system date or a future date.

Note You are not allowed to enter a date earlier than the current system date.

Step 4 Click **Submit** to configure the account disable policy for an individual user.

Disable User Accounts Globally

You can disable user accounts on a certain date, several days after account creation or last access date, and after several days of account inactivity.

Step 1 Choose **Administration > Identity Management > Settings > User Authentication Settings > Account Disable Policy**.

Step 2 Perform one of the following actions:

- Check the **Disable account if date exceeds** check box and select the appropriate date in yyyy-mm-dd format. This option allows you to disable the user account after the configured date. The **Disable account if date exceeds** setting at user level takes precedence over this global configuration.

- Check the **Disable account after n days of account creation or last enable** check box and enter the number of days. This option disables the user account when the account creation date or last access date exceeds the specified number of days. Administrators can manually enable the disabled user accounts, which reset the number of days count.
- Check the **Disable account after n days of inactivity** check box and enter the number of days. This option disables the user account when the account is inactive for the specified number of days.

Step 3 Click **Submit** to configure the global account disable policy.

Internal and External Identity Sources

Identity sources are databases that store user information. Cisco ISE uses user information from the identity source to validate user credentials during authentication. User information includes group information and other attributes that are associated with the user. You can add, edit, and delete user information from identity sources.

Cisco ISE supports internal and external identity sources. You can use both sources to authenticate sponsor and guest users.

Internal Identity Sources

Cisco ISE has an internal user database whree you can 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.

The following table lists authentication protocols and the external identity sources that they support.

Table 1: Authentication Protocols and Supported External Identity Sources

Protocol (Authentication Type)	Internal Database	Active Directory	LDAP	RADIUS Token Server or RSA	ODBC
EAP-GTC, PAP (plain text password)	Yes	Yes	Yes	Yes	Yes

Protocol (Authentication Type)	Internal Database	Active Directory	LDAP	RADIUS Token Server or RSA	ODBC
MS-CHAP password hash: MSCHAPv1/v2 EAP-MSCHAPv2 (as inner method of PEAP, EAP-FAST, or EAP-TTLS) LEAP	Yes	Yes	No	No	Yes
EAP-MD5 CHAP	Yes	No	No	No	Yes
EAP-TLS PEAP-TLS (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.	No	Yes	Yes	No	No

Credentials are stored differently, depending on the external data source connection type, and the features used.

- When joining an Active Directory Domain (but not for Passive ID), the credentials that are used to join are not saved. Cisco ISE creates an AD computer account, if it does not exist, and uses that account to authenticate users.
- For LDAP and Passive ID, the credentials that are used to connect to the external data source are also used to authenticate users.

Create an External Identity Source

Cisco ISE can connect with external identity sources such as Active Directory, LDAP, RADIUS Token, and RSA SecurID servers to obtain user information for authentication and authorization. External identity sources also include certificate authentication profiles that you need for certificate-based authentications.

Note To work with passive identity services, which enable you to receive and share authenticated user identities, see Additional Passive Identity Service Providers, on page 61.

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

Step 2 Choose one of these options:

- **Certificate Authentication Profile** for certificate-based authentications.
- **Active Directory** to connect to an Active Directory as an external identity source. See Active Directory as an External Identity Source, on page 15 for more details.
- **LDAP** to add an LDAP identity source. See LDAP, on page 101 for more details.
- **RADIUS Token** to add a RADIUS Token server. See RADIUS Token Identity Sources, on page 115 for more details.
- **RSA SecurID** to add an RSA SecurID server. See RSA Identity Sources, on page 120 for more details.
- **SAML Id Providers** to add an identity provider (IdP), such as Oracle Access Manager. See SAMLv2 Identity Provider as an External Identity Source, on page 124 for more details.

Authenticate Internal Users Against External Identity Store Password

Cisco ISE allows you to authenticate internal users against external identity store passwords. Cisco ISE provides an option to select the password identity store for internal users from the **Administration > Identity Management > Identities > Users** window. Administrators can select the identity store from the list of Cisco ISE External Identity Sources while adding or editing users in the **Users** window. The default password identity store for an internal user is the internal identity store. Cisco Secure ACS users will retain the same password identity store during and after migration from Cisco Secure ACS to Cisco ISE.

Cisco ISE supports the following external identity stores for password types:

- Active Directory
- LDAP
- ODBC
- RADIUS Token server
- RSA SecurID server

Note As per the current design, if authentication is done against an external ID store, then the internal user identity group name cannot be configured in authorization policy. In order to use internal user identity group for authorization, authentication policy must be configured to authenticate against Internal Users ID store and password type, which can be either internal or external, must be selected in user configuration.

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.

Add 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.

Step 1

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

Step 3 Select an identity store from the drop-down list.

Basic certificate checking does not require an identity source. If you want binary comparison checking for the certificates, you must select an identity source. If you select Active Directory as an identity source, subject and common name and subject alternative name (all values) can be used to look up a user.

Step 4 Select the use of identity from **Certificate Attribute** or **Any Subject or Alternative Name Attributes in the Certificate**. This will be used in logs and for lookups.

If you choose **Any Subject or Alternative Name Attributes in the Certificate**, Active Directory UPN will be used as the username for logs and all subject names and alternative names in a certificate will be tried to look up a user. This option is available only if you choose Active Directory as the identity source.

Step 5 Choose when you want to **Match Client Certificate Against Certificate In Identity Store**. For this you must select an identity source (LDAP or Active Directory.) If you select Active Directory, you can choose to match certificates only to resolve identity ambiguity.

- **Never**: This option never performs a binary comparison.
- **Only to resolve identity ambiguity**: This option performs the binary comparison of client certificate to certificate on account in Active Directory only if ambiguity is encountered. For example, several Active Directory accounts matching to identity names from certificate are found.
- **Always perform binary comparison**: This option always performs the binary comparison of client certificate to certificate on account in identity store (Active Directory or LDAP).

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

Active Directory as an External Identity Source

Cisco ISE uses Microsoft Active Directory as an external identity source to access resources such as users, machines, groups, and attributes. User and machine authentication in Active Directory allows network access only to users and devices that are listed in Active Directory.

ISE Community Resource

ISE Administrative Portal Access with AD Credentials Configuration Example

Active Directory-Supported Authentication Protocols and Features

Active Directory supports features such as user and machine authentications, changing Active Directory user passwords with some protocols. The following table lists the authentication protocols and the respective features that are supported by Active Directory.

Table 2: Authentication Protocols Supported by Active Directory

Authentication Protocols	Features
EAP-FAST and password based 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)	User and machine authentication
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
Extensible Authentication Protocol-Generic Token Card (EAP-GTC)	User and machine authentication
Extensible Authentication Protocol-Transport Layer Security (EAP-TLS)	• User and machine authentication • Groups and attributes retrieval • Binary certificate comparison
Extensible Authentication Protocol- Flexible Authentication via Secure Tunneling-Transport Layer Security (EAP-FAST-TLS)	• User and machine authentication • Groups and attributes retrieval • Binary certificate comparison

Authentication Protocols	Features
Protected Extensible Authentication Protocol-Transport Layer Security (PEAP-TLS)	• User and machine authentication • Groups and attributes retrieval • Binary certificate comparison
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 and groups from Active Directory for use in authorization policy rules. These attributes can be used in 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 may use groups in external identity stores to assign permissions to users or computers; for example, to map users to sponsor groups. You should note the following restrictions on group memberships in Active Directory:

- Policy rule conditions may reference any of the following: a user's or computer's primary group, the groups of which a user or computer is a direct member, or indirect (nested) groups.
- Domain local groups outside a user's or computer's account domain are not supported.

Note You can use the value of the Active Directory attribute, msRadiusFramedIPAddress, as an IP address. This IP address can be sent to a network access server (NAS) in an authorization profile. The msRADIUSFramedIPAddress attribute supports only IPv4 addresses. Upon user authentication, the msRadiusFramedIPAddress attribute value fetched for the user will be converted to IP address format.

Attributes and groups are retrieved and managed per join point. They are used in authorization policy (by selecting first the join point and then the attribute). You cannot define attributes or groups per scope for authorization, but you can use scopes for authentication policy. When you use a scope in authentication policy, it is possible that a user is authenticated via one join point, but attributes and/or groups are retrieved via another join point that has a trust path to the user's account domain. You can use authentication domains to ensure that no two join points in one scope have any overlap in authentication domains.

Note During the authorization process in a multi join point configuration, Cisco ISE will search for join points in the order in which they listed in the authorization policy, only until a particular user has been found. Once a user has been found the attributes and groups assigned to the user in the join point, will be used to evaluate the authorization policy.

Note See Microsoft-imposed limits on the maximum number of usable Active Directory groups: http://technet.microsoft.com/en-us/library/active-directory-maximum-limits-scalability(v=WS.10).aspx

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

Admin user login through Active Directory might fail if the admin username contains $ character.

Use Explicit UPN

To reduce ambiguity when matching user information against Active Directory's User-Principal-Name (UPN) attributes, you must configure Active Directory to use Explicit UPN. Using Implicit UPN can produce ambiguous results if two users have the same value for *sAMAccountName*.

To set Explicit UPN in Active Directory, open the **Advanced Tuning** page, and set the attribute *REGISTRY.Services\lsass\Parameters\Providers\ActiveDirectory\UseExplicitUPN* to 1.

Support for Boolean Attributes

Cisco ISE supports retrieving Boolean attributes from Active Directory and LDAP identity stores.

You can configure the Boolean attributes while configuring the directory attributes for Active Directory or LDAP. These attributes are retrieved upon authentication with Active Directory or LDAP.

The Boolean attributes can be used for configuring policy rule conditions.

The Boolean attribute values are fetched from Active Directory or LDAP server as String type. Cisco ISE supports the following values for the Boolean attributes:

Boolean attribute	Supported values
True	t, T, true, TRUE, True, 1
False	f, F, false, FALSE, False, 0

Note Attribute substitution is not supported for the Boolean attributes.

If you configure a Boolean attribute (for example, msTSAllowLogon) as String type, the Boolean value of the attribute in the Active Directory or LDAP server will be set for the String attribute in Cisco ISE. You can change the attribute type to Boolean or add the attribute manually as Boolean type.

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 perform binary comparison.

The certificate authentication profile determines the field where the username is taken from in order to lookup the user in Active Directory to be used for retrieving certificates, for example, Subject Alternative Name (SAN) or Common Name. 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 authentication is passed.

Active Directory User Authentication Process Flow

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

- MS-CHAP and PAP authentications check if the user is disabled, locked out, expired or out of logon hours and the authentication fails if any of these conditions are true.
- EAP-TLS authentications checks if the user is disabled or locked out and the authentication fails if any of these conditions are met.

Support for Active Directory Multidomain Forests

Cisco ISE supports Active Directory with multidomain forests. Within each forest, 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.

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

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.

Prerequisites for Integrating Active Directory and Cisco ISE

This section describes the manual steps required to configure Active Directory for integration with Cisco ISE. However, in most cases, you can enable Cisco ISE to automatically configure Active Directory. The following are the prerequisites to integrate Active Directory with Cisco ISE.

- Ensure you have Active Directory Domain Admin credentials, required to make changes to any of the AD domain configurations.
- Ensure you have the privileges of a Super Admin or System Admin in Cisco ISE.
- Use the Network Time Protocol (NTP) server settings to synchronize the time between the Cisco ISE server and Active Directory. You can configure NTP settings from Cisco ISE CLI.
- Cisco ISE can connect with multiple Active Directory domains that do not have a two-way trust or have zero trust between them. If you want to query other domains from a specific join point, ensure that trust relationships exist between the join point and the other domains that have user and machine information to which you need access. If trust relationships does not exist, you must create another join point to the untrusted domain. For more information on establishing trust relationships, refer to Microsoft Active Directory documentation.

- You must have at least one global catalog server operational and accessible by Cisco ISE, in the domain to which you are joining Cisco ISE.

Active Directory Account Permissions Required to Perform Various Operations

Join Operations	Leave Operations	Cisco ISE Machine Accounts
The join operation requires the following account permissions: • Search Active Directory (to see if a Cisco ISE machine account exists) • Create Cisco ISE machine account to domain (if the machine account does not already exist) • Set attributes on the new machine account (for example, Cisco ISE machine account password, SPN, dnsHostname)	The leave operation requires the following account permissions: • Search Active Directory (to see if a Cisco ISE machine account exists) • Remove the Cisco ISE machine account from the domain If you perform a force leave (leave without the password), it will not remove the machine account from the domain.	The ISE machine account that communicates to the Active Directory connection requires the following permissions: • Change password • Read the user and machine objects corresponding to users and machines that are authenticated • Query Active Directory to get information (for example, trusted domains, alternative UPN suffixes, and so on) • Read the tokenGroups attribute You can precreate the machine account in Active Directory. If the SAM name matches the Cisco ISE appliance hostname, it is located during the join operation and re-used. If there are multiple join operations, multiple machine accounts are maintained inside Cisco ISE, one for each join.

Note The credentials that are used for the join or leave operation are not stored in Cisco ISE. Only the newly created Cisco ISE machine account credentials are stored.

The **Network access: Restrict clients allowed to make remote calls to SAM** security policy in Microsoft Active Directory has been revised. Hence, Cisco ISE might not able to update its machine account password every 15 days. If the machine account password is not updated, Cisco ISE will no longer authenticate users through Microsoft Active Directory. You will receive the **AD: ISE password update failed** alarm on your Cisco ISE dashboard to notify you of this event.

Note This issue happens in Windows Server 2016 Active Directory or later and Windows 10 version 1607 due to the restriction in them. To overcome this restriction, when you are integrating Windows Server 2016 Active Directory or later or Windows 10 version 1607 with Cisco ISE, you much set the registry value in the following registry from non-zero to blank to give access to all: Registry:HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\restrictremotesam This allows Cisco ISE to update its machine account password.

The security policy allows users to enumerate users and groups in the local Security Accounts Manager (SAM) database and in Microsoft Active Directory. To ensure Cisco ISE can update its machine account password, check that your configurations in Microsoft Active Directory are accurate. For more information on the Windows operating systems and Windows Server versions affected, what this means for your network, and what changes may be needed, see:

https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-access-restrict-clients-allowed-to-make-remote-sam-calls

Network Ports that Must Be Open for Communication

Protocol	Port (remote-local)	Target	Authenticated	Notes
DNS (TCP/UDP)	Random number greater than or equal to 49152	DNS Servers/AD Domain Controllers	No	—
MSRPC	445	Domain Controllers	Yes	—
Kerberos (TCP/UDP)	88	Domain Controllers	Yes (Kerberos)	MS AD/KDC
LDAP (TCP/UDP)	389	Domain Controllers	Yes	—
LDAP (GC)	3268	Global Catalog Servers	Yes	—
NTP	123	NTP Servers/Domain Controllers	No	—
IPC	80	Other ISE Nodes in the Deployment	Yes (Using RBAC credentials)	—

DNS Server

While configuring your DNS server, make sure that you take care of the following:

- The DNS servers that you configure in Cisco ISE must be able to resolve all forward and reverse DNS queries for the domains that you want to use.
- The Authoritative DNS server is recommended to resolve Active Directory records, as DNS recursion can cause delays and have significant negative impact on performance.

- All DNS servers must be able to answer SRV queries for DCs, GCs, and KDCs with or without additional Site information.
- Cisco recommends that you add the server IP addresses to SRV responses to improve performance.
- Avoid using DNS servers that query the public Internet. They can leak information about your network when an unknown name has to be resolved.

Configure Active Directory as an External Identity Source

Configure Active Directory as an external identity source as part of the configuration for features such as Easy Connect and the PassiveID Work Center. For more information about these features, see Easy Connect, on page 49 and PassiveID Work Center , on page 53.

Before you configure Active Directory as an External Identity Source, make sure that:

- The Microsoft Active Directory server does not reside behind a network address translator and does not have a Network Address Translation (NAT) address.
- The Microsoft Active Directory account intended for the join operation is valid and is not configured with the Change Password on Next Login.
- You have the privileges of a Super Admin or System Admin in ISE.

Note If you see operational issues when Cisco ISE is connected to Active Directory, see the AD Connector Operations Report under **Operations** > **Reports**.

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

1. Add an Active Directory Join Point and Join Cisco ISE Node to the Join Point, on page 21
2. Configure Authentication Domains, on page 25
3. Configure Active Directory User Groups, on page 26
4. Configure Active Directory User and Machine Attributes, on page 27
5. (Optional) Modify Password Changes, Machine Authentications, and Machine Access Restriction Settings, on page 27

Add an Active Directory Join Point and Join Cisco ISE Node to the Join Point

Before you begin

Ensure that the Cisco ISE node can communicate with the networks where the NTP servers, DNS servers, domain controllers, and global catalog servers are located. You can check these parameters by running the Domain Diagnostic tool.

Join points must be created in order to work with Active Directory as well as with the Agent, Syslog, SPAN and Endpoint probes of the Passive ID Work Center.

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

Step 2 Click **Add** and enter the domain name and identity store name from the **Active Directory Join Point Name** settings.

Step 3 Click **Submit**.

A pop-up appears asking if you want to join the newly created join point to the domain. Click **Yes** if you want to join immediately.

If you clicked **No**, then saving the configuration saves the Active Directory domain configuration globally (in the primary and secondary policy service nodes), but none of the Cisco ISE nodes are joined to the domain yet.

Step 4 Check the check box next to the new Active Directory join point that you created and click **Edit**, or click on the new Active Directory join point from the navigation pane on the left. The deployment join/leave table is displayed with all the Cisco ISE nodes, the node roles, and their status.

Step 5 In case the join point was not joined to the domain during Step 3, check the check box next to the relevant Cisco ISE nodes and click **Join** to join the Cisco ISE node to the Active Directory domain.

You must do this explicitly even though you saved the configuration. To join multiple Cisco ISE nodes to a domain in a single operation, the username and password of the account to be used must be the same for all join operations. If different username and passwords are required to join each Cisco ISE node, the join operation should be performed individually for each Cisco ISE node.

Step 6 Enter the Active Directory username and password in the **Join Domain**dialog box.

It is strongly recommended that you choose **Store credentials**, in which case your administrator's user name and password will be saved in order to be used for all Domain Controllers (DC) that are configured for monitoring.

The user used for the join operation should exist in the domain itself. If it exists in a different domain or subdomain, the username should be noted in a UPN notation, such as jdoe@acme.com.

Step 7 (Optional) Check the **Specify Organizational Unit** check box.

You should check this check box in case the Cisco ISE node machine account is to be located in a specific Organizational Unit other than CN=Computers,DC=someDomain,DC=someTLD. Cisco ISE creates the machine account under the specified organizational unit or moves it to this location if the machine account already exists. If the organizational unit is not specified, Cisco ISE uses the default location. The value should be specified in full distinguished name (DN) format. The syntax must conform to the Microsoft guidelines. Special reserved characters, such as /'+,;=<> line feed, space, and carriage return must be escaped by a backslash (\). For example, OU=Cisco ISE\,US,OU=IT Servers,OU=Servers\, and Workstations,DC=someDomain,DC=someTLD. If the machine account is already created, you need not check this check box. You can also change the location of the machine account after you join to the Active Directory domain.

Step 8 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. Click the failure message for each node to view detailed logs for that node.

Note When the join is complete, Cisco ISE updates its AD groups and corresponding security identifiers (SIDs). Cisco ISE automatically starts the SID update process. You must ensure that this process is allowed to complete.

Note You might not be able to join Cisco ISE with an Active Directory domain if the DNS service (SRV) records are missing (the domain controllers do not advertise their SRV records for the domain that you are trying to join to). Refer to the following Microsoft Active Directory documentation for troubleshooting information:

- http://support.microsoft.com/kb/816587
- http://technet.microsoft.com/en-us/library/bb727055.aspx

Add Domain Controllers

Step 1 Choose **Work Centers** > **PassiveID** > **Providers** and then from the left panel choose **Active Directory**.

Step 2 Check the check box next to the Active Directory join point that you created and click **Edit**. The deployment join/leave table is displayed with all the Cisco ISE nodes, the node roles, and their statuses.

Step 3 **Note** To add a new Domain Controller (DC) for Passive Identity services, you need the login credentials of that DC.

Go to the PassiveID tab and click **Add DCs**.

Step 4 Check the check box next to the domain controllers that you would like to add to the join point for monitoring and click **OK**.
The domain controllers appear in the Domain Controllers list of the PassiveID tab.

Step 5 Configure the domain controller:

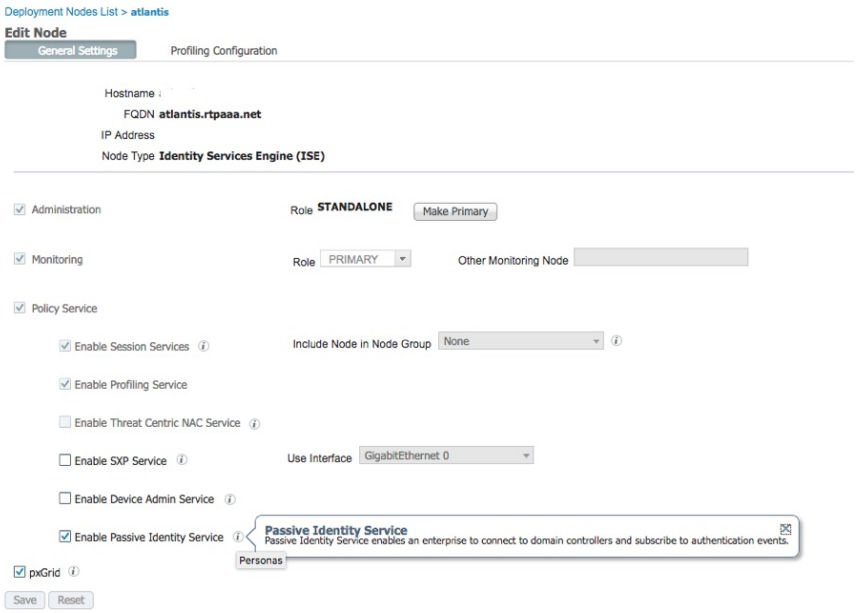
a) Checkmark the domain controller and click **Edit**. The **Edit Item** screen appears.
b) Optionally, edit the different domain controller fields.
c) If you selected WMI protocol, click **Configure** to configure WMI automatically and click **Test** to test the connection.

Configure WMI for Passive ID

Before you begin

Ensure you have Active Directory Domain Admin credentials, required in order to make changes to any of the AD domain configurations. Ensure that you enabled Passive ID for this node under **Administration** > **System** > **Deployment**.

Figure 1:

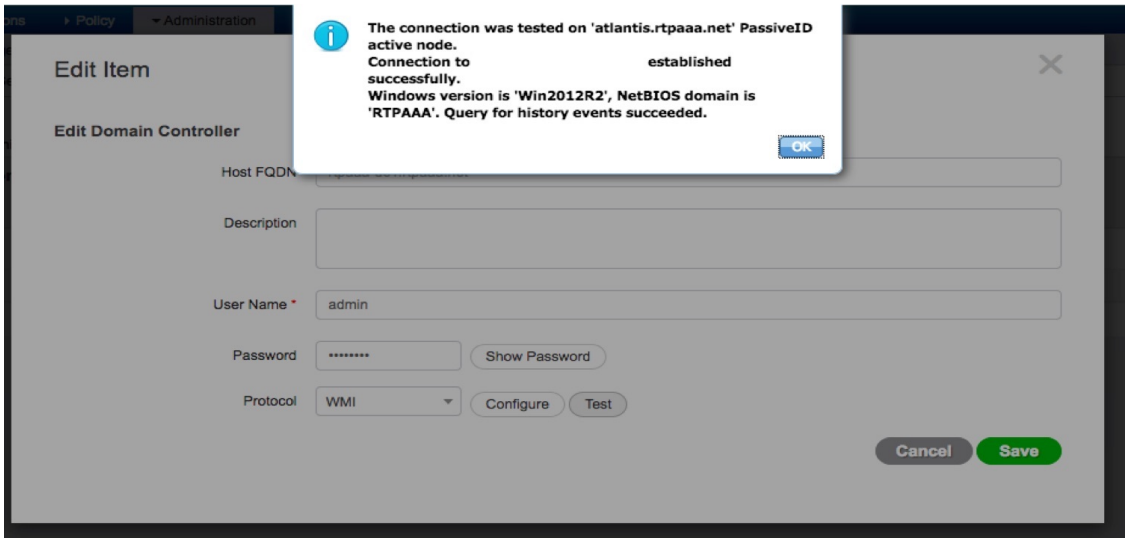


Step 1 Choose **Administration** > **Identity Management** > **External Identity Sources** > **Active Directory**.

Step 2 Check the check box next to the Active Directory join point that you created and click **Edit**. The deployment join/leave table is displayed with all the Cisco ISE nodes, the node roles, and their statuses.

Step 3 Go to the Passive ID tab, check the check box next to the relevant domain controllers and click **Config WMI** to enable ISE to automatically configure the domain controllers you selected.

Figure 2:



To configure Active Directory and Domain Controllers manually, or to troubleshoot any problems with configuration, see Prerequisites for Integrating Active Directory and Cisco ISE , on page 18.

Figure 3:

Leave the Active Directory Domain

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

When you reset the Cisco ISE application configuration from the command-line interface or restore configuration after a backup or upgrade, it performs a leave operation, disconnecting the Cisco 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 because it also removes the node account from the Active Directory domain. This is also recommended when you change the Cisco ISE hostname.

Before you begin

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), authentications may fail.

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

Step 2 Check the checkbox next to the Active Directory join point that you created and click **Edit**. The deployment join/leave table is displayed with all the Cisco ISE nodes, the node roles, and their statuses.

Step 3 Check the checkbox next to the Cisco ISE node and click **Leave**.

Step 4 Enter the Active Directory username and password, and click **OK** to leave the domain and remove the machine account from the Cisco ISE database.

If you enter the Active Directory credentials, the Cisco ISE node leaves the Active Directory domain and deletes the Cisco ISE machine account from the Active Directory database.

Note To delete the Cisco ISE machine account from the Active Directory database, the Active Directory credentials that you provide here must have the permission to remove machine account from domain.

Step 5 If you do not have the Active Directory credentials, check the **No Credentials Available** checkbox, and click **OK**.

If you check the **Leave domain without credentials** checkbox, the primary Cisco ISE node leaves the Active Directory domain. The Active Directory administrator must manually remove the machine account that was created in Active Directory during the time of the join.

Configure Authentication Domains

The domain to which Cisco ISE is joined to has visibility to other domains with which it has a trust relationship. By default, Cisco ISE is set to permit authentication against all those trusted domains. You can restrict interaction with the Active Directory deployment to a subset of authentication domains. Configuring authentication domains enables you to select specific domains for each join point so that the authentications are performed against the selected domains only. Authentication domains improves security because they instruct Cisco ISE to authenticate users only from selected domains and not from all domains trusted from join point. Authentication domains also improve performance and latency of authentication request processing because authentication domains limit the search area (that is, where accounts matching to incoming username

or identity will be searched). It is especially important when incoming username or identity does not contain domain markup (prefix or suffix). Due to these reasons, configuring authentication domains is a best practice, and we highly recommended it.

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

Step 2 Click **Active Directory** join point.

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

A table appears with a list of your trusted domains. By default, Cisco ISE permits authentication against all trusted domains.

Step 4 To allow only specified domains, uncheck **Use all Active Directory domains for authentication** check box.

Step 5 Check the check box next to the domains for which you want to allow authentication, and click **Enable Selected**. In the **Authenticate** column, the status of this domain changes to Yes.

You can also disable selected domains.

Step 6 Click **Show Unusable Domains** to view a list of domains that cannot be used. Unusable domains are domains that Cisco ISE cannot use for authentication due to reasons such as one-way trust, selective authentication and so on.

What to do next

Configure Active Directory user groups.

Configure Active Directory User Groups

You must configure Active Directory user groups for them to be available for use in authorization policies. Internally, Cisco ISE uses security identifiers (SIDs) to help resolve group name ambiguity issues and to enhance group mappings. SID provides accurate group assignment matching.

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

Step 2 Click the **Groups** tab.

Step 3 Do one of the following:

a) Choose **Add** > **Select Groups From Directory** to choose an existing group.

b) Choose **Add** > **Add Group** to manually add a group. You can either provide both group name and SID or provide only the group name and press **Fetch SID**.

Do not use double quotes (”) in the group name for the user interface login.

Step 4 If you are manually selecting a group, you can search for them using a filter. For example, enter **admin*** as the filter criteria and click **Retrieve Groups** to view user groups that begin with admin. You can also enter the asterisk (*) wildcard character to filter the results. You can retrieve only 500 groups at a time.

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 If you choose to manually add a group, enter a name and SID for the new group.

Step 7 Click **OK**.

Step 8 Click **Save**.

Note If you delete a group and create a new group with the same name as original, you must click **Update SID Values** to assign new SID to the newly created group. After an upgrade, the SIDs are automatically updated after the first join.

What to do next

Configure Active Directory user attributes.

Configure Active Directory User and Machine Attributes

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

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

Step 2 Click the **Attributes** tab.

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

Step 4 If you choose to add attributes from the directory, enter the name of a user in the **Sample User or Machine Account** field, and click **Retrieve Attributes** to obtain a list of attributes for users. For example, enter **administrator** to obtain a list of administrator attributes. You can also enter the asterisk (*) wildcard character to filter the results.

Note When you enter an example username, 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/” or use the SAM$ format. For example, you might use host/myhost. The example value displayed when you retrieve attributes are provided for illustration only and are not stored.

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

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

Step 7 Click **Save**.

Modify Password Changes, Machine Authentications, and Machine Access Restriction Settings

Before you begin

You must join Cisco ISE to the Active Directory domain. For more information, see Add an Active Directory Join Point and Join Cisco ISE Node to the Join Point, on page 21.

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

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

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

Step 4 Modify as required, the Password Change, Machine Authentication, and Machine Access Restrictions (MARs) settings.

Step 5 Check the **Enable dial-in check** check box to check the dial-in permissions of the user during authentication or query. The result of the check can cause a reject of the authentication in case the dial-in permission is denied.

Step 6 Check the **Enable callback check for dial-in clients** check box if you want the server to call back the user during authentication or query. The IP address or phone number used by the server can be set either by the caller or the network administrator. The result of the check is returned to the device on the RADIUS response.

Step 7 Check the **Use Kerberos for Plain Text Authentications** check box if you want to use Kerberos for plain-text authentications. The default and recommended option is MS-RPC.

Machine Access Restriction Cache

Cisco ISE stores the Machine Access Restriction (MAR) cache content, calling-station-ID list, and the corresponding time stamps to a file on its local disk when you manually stop the the application services. Cisco ISE does not store the MAR cache entries of an instance when there is an accidental restart of the application services. Cisco ISE reads the MAR cache entries from the file on its local disk based on the cache entry time to live when the application services restart. When the application services come up after a restart, Cisco ISE compares the current time of that instance with the MAR cache entry time. If the difference between the current time and the MAR entry time is greater than the MAR cache entry time to live, then Cisco ISE does not retrieve that entry from disk. Otherwise, Cisco ISE retrieves that MAR cache entry and updates its MAR cache entry time to live.

To Configure MAR Cache

On **Advanced Settings** tab of the Active Directory defined in External Identity Sources, verify that the following options are checked:

- **Enable Machine Authentication**: To enable machine authentication.
- **Enable Machine Access Restriction**: To combine user and machine authentication before authorization.

To Use MAR Cache in Authorization

Use `WasMachineAuthenticated is True` in an authorization policy. You can use this rule plus a credentials rule to do dual-authentication. Machine authentication must be done before AD credentials.

If you created a Node Group on the **System > Deployment** page, enable MAR Cache Distribution. MAR cache distribution replicates the MAR cache to all the PSNs in the same node group.

For more information, see the following Cisco ISE Community pages:

- https://community.cisco.com/t5/policy-and-access/mar-why-is-it-useful/td-p/3213527
- https://community.cisco.com/t5/policy-and-access/ise-2-1-mar-aging-time-eap-tls/td-p/3209628

Related Topics

Configure Active Directory as an External Identity Source, on page 21

Configure Custom Schema

Before you begin

You must join Cisco ISE to the Active Directory domain.

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

Step 2 Select the Join point.

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

Step 4 Under the **Schema** section, select the **Custom** option from the **Schema** drop-down list. You can update the user information attributes based on your requirements. These attributes are used to collect user information, such as, first name, last name, email, telephone, locality, and so on.

Predefined attributes are used for the Active Directory schema (built-in schema). If you edit the attributes of the predefined schema, Cisco ISE automatically creates a custom schema.

Support for Active Directory Multijoin Configuration

Cisco ISE supports multiple joins to Active Directory domains. Cisco ISE supports up to 50 Active Directory joins. Cisco ISE can connect with multiple Active Directory domains that do not have a two-way trust or have zero trust between them. Active Directory multi-domain join comprises a set of distinct Active Directory domains with their own groups, attributes, and authorization policies for each join.

You can join the same forest more than once, that is, you can join more than one domain in the same forest, if necessary.

Cisco ISE now allows to join domains with one-way trust. This option helps bypass the permission issues caused by a one-way trust. You can join either of the trusted domains and hence be able to see both domains.

- Join Point: In Cisco ISE, each independent join to an Active Directory domain is called a join point. The Active Directory join point is an Cisco ISE identity store and can be used in authentication policy. It has an associated dictionary for attributes and groups, which can be used in authorization conditions.
- Scope: A subset of Active Directory join points grouped together is called a scope. You can use scopes in authentication policy in place of a single join point and as authentication results. Scopes are used to authenticate users against multiple join points. Instead of having multiple rules for each join point, if you use a scope, you can create the same policy with a single rule and save the time that Cisco ISE takes to process a request and help improve performance. A join point can be present in multiple scopes. A scope can be included in an identity source sequence. You cannot use scopes in an authorization policy condition because scopes do not have any associated dictionaries.

  When you perform a fresh Cisco ISE install, by default no scopes exist. This is called the no scope mode. When you add a scope, Cisco ISE enters multi-scope mode. If you want, you can return to no scope mode. All the join points will be moved to the Active Directory folder.

  - Initial_Scope is an implicit scope that is used to store the Active Directory join points that were added in no scope mode. When multi-scope mode is enabled, all the Active Directory join points move into the automatically created Initial_Scope. You can rename the Initial_Scope.
  - All_AD_Instances is a built-in pseudo scope that is not shown in the Active Directory configuration. It is only visible as an authentication result in policy and identity sequences. You can select this scope if you want to select all Active Directory join points configured in Cisco ISE.

Create a New Scope to Add Active Directory Join Points

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

Step 2 Click **Scope Mode**.
A default scope called Initial_Scope is created, and all the current join points are placed under this scope.

Step 3 To create more scopes, click **Add**.

Step 4 Enter a name and a description for the new scope.

Step 5 Click **Submit**.

Identity Rewrite

Identity rewrite is an advanced feature that directs Cisco ISE to manipulate the identity before it is passed to the external Active Directory system. You can create rules to change the identity to a desired format that includes or excludes a domain prefix and/or suffix or other additional markup of your choice.

Identity rewrite rules are applied on the username or hostname received from the client, before being passed to Active Directory, for operations such as subject searches, authentication, and authorization queries. Cisco ISE will match the condition tokens and when the first one matches, Cisco ISE stops processing the policy and rewrites the identity string according to the result.

During the rewrite, everything enclosed in square bracket [ ] (such as [IDENTITY]) is a variable that is not evaluated on the evaluation side but instead added with the string that matches that location in the string. Everything without the brackets is evaluated as a fixed string on both the evaluation side and the rewrite side of the rule.

The following are some examples of identity rewrite, considering that the identity entered by the user is ACME\jdoe:

- If identity matches **ACME\[IDENTITY]**, rewrite as **[IDENTITY]**.

  The result would be jdoe. This rule instructs Cisco ISE to strip all usernames with the ACME prefix.

- If the identity matches **ACME\[IDENTITY]**, rewrite as **[IDENTITY]@ACME.com**.

  The result would be jdoe@ACME.com. This rule instructs Cisco ISE to change the format from prefix for suffix notation or from NetBIOS format to UPN formats.

- If the identity matches **ACME\[IDENTITY]**, rewrite as **ACME2\[IDENTITY]**.

  The result would be ACME2\jdoe. This rule instructs Cisco ISE to change all usernames with a certain prefix to an alternate prefix.

- If the identity matches **[ACME]\jdoe.USA**, rewrite as **[IDENTITY]@[ACME].com**.

  The result would be jdoe\ACME.com. This rule instructs Cisco ISE to strip the realm after the dot, in this case the country and replace it with the correct domain.

- If the identity matches **E=[IDENTITY]**, rewrite as **[IDENTITY]**.

  The result would be jdoe. This is an example rule that can be created when an identity is from a certificate, the field is an email address, and Active Directory is configured to search by Subject. This rule instructs Cisco ISE to remove ‘E=’.

- If the identity matches **E=[EMAIL],[DN]**, rewrite as **[DN]**.

  This rule will convert certificate subject from E=jdoe@acme.com, CN=jdoe, DC=acme, DC=com to pure DN, CN=jdoe, DC=acme, DC=com. This is an example rule that can be created when identity is taken from a certificate subject and Active Directory is configured to search user by DN . This rule instructs Cisco ISE to strip email prefix and generate DN.

The following are some common mistakes while writing the identity rewrite rules:

- If the identity matches **[DOMAIN]\[IDENTITY]**, rewrite as **[IDENTITY]@DOMAIN.com**.

  The result would be jdoe@DOMAIN.com. This rule does not have [DOMAIN] in square brackets [ ] on the rewrite side of the rule.

- If the identity matches **DOMAIN\[IDENTITY]**, rewrite as **[IDENTITY]@[DOMAIN].com**.

  Here again, the result would be jdoe@DOMAIN.com. This rule does not have [DOMAIN] in square brackets [ ] on the evaluation side of the rule.

Identity rewrite rules are always applied within the context of an Active Directory join point. Even if a scope is selected as the result of an authentication policy, the rewrite rules are applied for each Active Directory join point. These rewrite rules also applies for identities taken from certificates if EAP-TLS is being used.

Enable Identity Rewrite

Note This configuration task is optional. You can perform it to reduce authentication failures that can arise because of various reasons such as ambiguous identity errors.

Before you begin

You must join Cisco ISE to the Active Directory domain.

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

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

Step 3 Under the **Identity Rewrite** section, choose whether you want to apply the rewrite rules to modify usernames.

Step 4 Enter the match conditions and the rewrite results. You can remove the default rule that appears and enter the rule according to your requirement. Cisco ISE processes the policy in order, and the first condition that matches the request username is applied. You can use the matching tokens (text contained in square brackets) to transfer elements of the original username to the result. If none of the rules match, the identity name remains unchanged. You can click the **Launch Test** button to preview the rewrite processing.

Identity Resolution Settings

Some type of identities include a domain markup, such as a prefix or a suffix. For example, in a NetBIOS identity such as ACME\jdoe, “ACME” is the domain markup prefix, similarly in a UPN identity such as jdoe@acme.com, “acme.com” is the domain markup suffix. Domain prefix should match to the NetBIOS (NTLM) name of the Active Directory domain in your organization and domain suffix should match to the

DNS name of Active Directory domain or to the alternative UPN suffix in your organization. For example jdoe@gmail.com is treated as without domain markup because gmail.com is not a DNS name of Active Directory domain.

The identity resolution settings allows you to configure important settings to tune the security and performance balance to match your Active Directory deployment. You can use these settings to tune authentications for usernames and hostnames without domain markup. In cases when Cisco ISE is not aware of the user's domain, it can be configured to search the user in all the authentication domains. Even if the user is found in one domain, Cisco ISE will wait for all responses in order to ensure that there is no identity ambiguity. This might be a lengthy process, subject to the number of domains, latency in the network, load, and so on.

Avoid Identity Resolution Issues

It is highly recommended to use fully qualified names (that is, names with domain markup) for users and hosts during authentication. For example, UPNs and NetBIOS names for users and FQDN SPNs for hosts. This is especially important if you hit ambiguity errors frequently, such as, several Active Directory accounts match to the incoming username; for example, jdoe matches to jdoe@emea.acme.com and jdoe@amer.acme.com. In some cases, using fully qualified names is the only way to resolve issue. In others, it may be sufficient to guarantee that the users have unique passwords. So, it is more efficient and leads to less password lockout issues if unique identities are used initially.

Configure Identity Resolution Settings

Note This configuration task is optional. You can perform it to reduce authentication failures that can arise because of various reasons such as ambiguous identity errors.

Before you begin

You must join the Cisco ISE node to the Active Directory domain.

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

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

Step 3 Define the following settings for identity resolution for usernames or machine names under the **Identity Resolution** section. This setting provides you advanced control for user search and authentication.

The first setting is for the identities without a markup. In such cases, you can select any of the following options:

- **Reject the request**: This option will fail the authentication for users who do not have any domain markups, such as a SAM name. This is useful in case of multi join domains where Cisco ISE will have to look up for the identity in all the joined global catalogs, which might not be very secure. This option forces the users to use names with domain markups.
- **Only search in the "Authentication Domains" from the joined forest**: This option will search for the identity only in the domains in the forest of the join point which are specified in the authentication domains section. This is the default option and identical to Cisco ISE 1.2 behavior for SAM account names.
- **Search in all the "Authentication Domains" sections**: This option will search for the identity in all authentication domains in all the trusted forests. This might increase latency and impact performance.

The selection is made based on how the authentication domains are configured in Cisco ISE. If only specific authentication domains are selected, only those domains will be searched (for both "joined forest" or "all forests" selections).

The second setting is used if Cisco ISE cannot communicate with all Global Catalogs (GCs) that it needs to in order to comply with the configuration specified in the "Authentication Domains" section. In such cases, you can select any of the following options:

- **Proceed with available domains**: This option will proceed with the authentication if it finds a match in any of the available domains.
- **Drop the request**: This option will drop the authentication request if the identity resolution encounters some unreachable or unavailable domain.

Test Users for Active Directory Authentication

The Test User tool can be used to verify user authentication from Active Directory. You can also fetch groups and attributes and examine them. You can run the test for a single join point or for scopes.

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

Step 2 Choose one of the following options:

- To run the test on all join points, choose **Advanced Tools** > **Test User for All Join Points**.
- To run the test for a specific join point, select the joint point and click **Edit**. Select the Cisco ISE node and click **Test User**.

Step 3 Enter the username and password of the user (or host) in Active Directory.

Step 4 Choose the authentication type. Password entry in Step 3 is not required if you choose the Lookup option.

Step 5 Select the Cisco ISE node on which you want to run this test, if you are running this test for all join points.

Step 6 Check the Retrieve Groups and Attributes check boxes if you want to retrieve the groups and attributes from Active Directory.

Step 7 Click **Test**.
The result and steps of the test operation are displayed. The steps can help to identify the failure reason and troubleshoot.

You can also view the time taken (in milliseconds) for Active Directory to perform each processing step (for authentication, lookup, or fetching groups/attributes). Cisco ISE displays a warning message if the time taken for an operation exceeds the threshold.

Delete 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 the checkbox next to the configured Active Directory.

Step 3 Check and ensure that the Local Node status is listed as Not Joined.

Step 4 Click **Delete**.

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.

View Active Directory Joins for a Node

You can use the **Node View** button on the **Active Directory** page to view the status of all Active Directory join points for a given Cisco ISE node or a list of all join points on all Cisco ISE nodes.

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

Step 2 Click **Node View**.

Step 3 Select a node from the **ISE Node** drop-down list.
The table lists the status of Active Directory by node. If there are multiple join points and multiple Cisco ISE nodes in a deployment, this table may take several minutes to update.

Step 4 Click the join point **Name** link to go to that Active Directory join point page and perform other specific actions.

Step 5 Click the link in the **Diagnostic Summary** column to go to the **Diagnostic Tools** page to troubleshoot specific issues. The diagnostic tool displays the latest diagnostics results for each join point per node.

Diagnose Active Directory Problems

The Diagnostic Tool is a service that runs on every Cisco ISE node. It allows you to automatically test and diagnose the Active Directory deployment and execute a set of tests to detect issues that may cause functionality or performance failures when Cisco ISE uses Active Directory.

There are multiple reasons for which Cisco ISE might be unable to join or authenticate against Active Directory. This tool helps ensure that the prerequisites for connecting Cisco ISE to Active Directory are configured correctly. It helps detect problems with networking, firewall configurations, clock sync, user authentication, and so on. This tool works as a step-by-step guide and helps you fix problems with every layer in the middle, if needed .

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

Step 2 Click the **Advanced Tools** drop-down and choose **Diagnostic Tools**.

Step 3 Select a Cisco ISE node to run the diagnosis on.

If you do not select a Cisco ISE node then the test is run on all the nodes.

Step 4 Select a specific Active Directory join point.

If you do not select an Active Directory join point then the test is run on all the join points.

Step 5 Click **Run All Tests on Node** to start the test.

Step 6 Click **View Test Details** to view the details for tests with Warning or Failed status.

This table allows you to rerun specific tests, stop running tests, and view a report of specific tests.

Enable 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. Enabling Active Directory debug logs may affect ISE performance.

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. This will include errors, warnings, and verbose logs. To get full logs, choose **TRACE**.

Step 5 Click **Save**.

Obtain the Active Directory Log File for Troubleshooting

Download and view the Active Directory debug logs to troubleshoot issues you may have.

Before you begin

Active Directory debug logging must be enabled.

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.

Active Directory Alarms and Reports

Cisco ISE provides various alarms and reports to monitor and troubleshoot Active Directory related activities.

Alarms

The following alarms are triggered for Active Directory errors and issues:

- Configured nameserver not available
- Joined domain is unavailable
- Authentication domain is unavailable

- Active Directory forest is unavailable
- AD Connector had to be restarted
- AD: ISE account password update failed
- AD: Machine TGT refresh failed

Reports

You can monitor Active Directory related activities through the following two reports:

- RADIUS Authentications report: This report shows detailed steps of the Active Directory authentication and authorization. You can find this report here: **Operations** > **Reports** > **Auth Services Status** > **RADIUS Authentications**.
- AD Connector Operations report: The AD Connector Operations report provides a log of background operations performed by AD connector, such as Cisco ISE server password refresh, Kerberos ticket management, DNS queries, DC discovery, LDAP, and RPC connections management. If you encounter any Active Directory failures, you can review the details in this report to identify the possible causes. You can find this report here: **Operations** > **Reports** > **Auth Services Status** > **AD Connector Operations**.

Active Directory Advanced Tuning

The advanced tuning feature provides node-specific settings used for support action under the supervision of Cisco support personnel, to adjust the parameters deeper in the system. These settings are not intended for normal administration flow, and should be used only under guidance.

Active Directory Identity Search Attributes

Cisco ISE identifies users using the attributes SAM, CN, or both. Cisco ISE, Release 2.2 Patch 5 and above, and 2.3 Patch 2 and above, use sAMAccountName attribute as the default attribute. In earlier releases, both SAM and CN attributes were searched by default. This behavior has changed in Release 2.2 Patch 5 and above, and 2.3 Patch 2 and above, as part of CSCvf21978 bug fix. In these releases, only the sAMAccountName attribute is used as the default attribute.

You can configure Cisco ISE to use SAM, CN, or both, if your environment requires it. When SAM and CN are used, and the value of the SAMAccountName attribute is not unique, Cisco ISE also compares the CN attribute value.

Configure Attributes for Active Directory Identity Search

1. Choose **Administration** > **Identity Management** > **External Identity Sources** > **Active Directory** .
2. In the **Active Directory** window, click **Advanced Tools**, and choose **Advanced Tuning**. Enter the following details:
   - **ISE Node**: Choose the ISE node that is connecting to Active Directory.
   - **Name**: Enter the registry key that you are changing. To change the Active Directory search attributes, enter: `REGISTRY.Services\lsass\Parameters\Providers\ActiveDirectory\IdentityLookupField`
   - **Value**: Enter the attributes that ISE uses to identify a user:

- *SAM*: To use only SAM in the query (this option is the default).
- *CN*: To use only CN in the query.
- *SAMCN*: To use CN and SAM in the query.

- **Comment**: Describe what you are changing, for example: Changing the default behavior to SAM and CN

3. Click **Update Value** to update the registry.

   A pop-up window appears. Read the message and accept the change. The AD connector service in ISE restarts.

Example Search Strings

For the following examples, assume that the username is *userd2only*:

- SAM search string—

```
filter=[(&(|(objectCategory=person)(objectCategory=computer))(|(cn=userd2only)(sAMAccountName=userd2only)))]
```

- SAM and CN search string—

```
filter=[(&(|(objectCategory=person)(objectCategory=computer))(sAMAccountName=userd2only))]
```

Supplemental Information for Setting Up Cisco ISE with Active Directory

For configuring Cisco ISE with Active Directory, you must configure group policies, and configure a supplicant for machine authentication.

Configure Group Policies in Active Directory

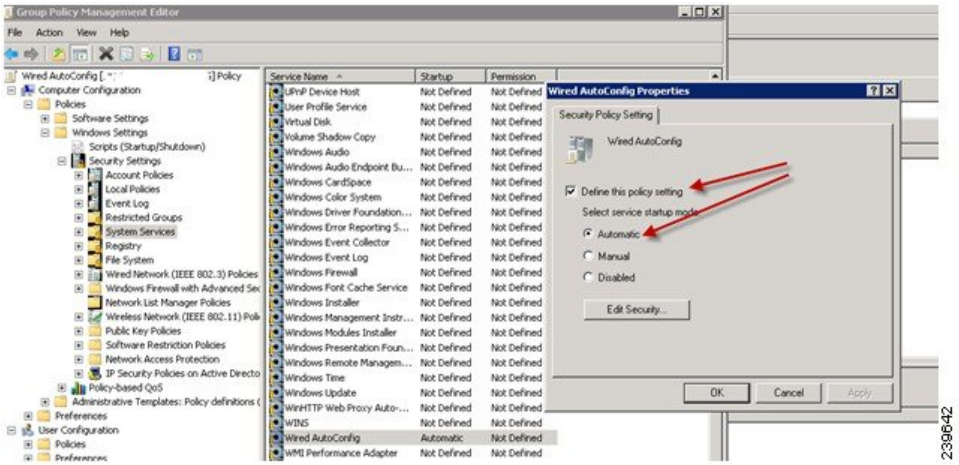
For more information about how to access the Group Policy management editor, refer to the Microsoft Active Directory documentation.

Step 1 Open the Group Policy management editor as shown in the following illustration.

Step 2 Create a new policy and enter a descriptive name for it or add to an existing domain policy.

In example below, we used Wired Autoconfiguration for the policy name.

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



Step 4 Apply the policy at the desired organizational unit or domain Active Directory level.

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 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** window, 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.

Active Directory Requirements to Support Easy Connect and Passive Identity services

Easy Connect and Passive Identity services use Active Directory login audit events generated by the Active Directory domain controller to gather user login information. The Active Directory server must be configured properly so the ISE user can connect and fetch the user login information. The following sections show how to configure the Active Directory domain controller (configurations from the Active Directory side) to support Easy Connect and Passive Identity services.

To configure Active Directory domain controllers (configurations from the Active Directory side) to support Easy Connect and Passive Identity services, follow these steps:

Note You must configure all the domain controllers in all the domains.

1. Set up Active Directory join points and domain controllers from ISE. See Add an Active Directory Join Point and Join Cisco ISE Node to the Join Point, on page 21 and #unique_537.
2. Configure WMI per domain controller. See #unique_538.
3. Perform the following steps from Active Directory:
   - Configure Active Directory for Passive Identity service, on page 39
   - Set the Windows Audit Policy, on page 42
4. (Optional) Troubleshoot automatic configurations performed by ISE on Active Directory with these steps:
   - Set Permissions when Microsoft Active Directory Users are in Domain Admin Group
   - Permissions for Microsoft Active Directory Users Not in Domain Admin Group
   - Permissions to Use DCOM on the Domain Controller
   - Set Permissions for Access to WMI Root and CIMv2 Namespace
   - Grant Access to the Security Event Log in the AD Domain Controller, on page 47

Configure Active Directory for Passive Identity service

ISE Easy Connect and Passive Identity services use Active Directory login audit events generated by the Active Directory domain controller to gather user login information. ISE connects to Active Directory and fetches the user login information.

The following steps should be performed from the Active Directory domain controller:

Step 1 Make sure relevant Microsoft patches are installed on the Active Directory domain controllers.

- The following patches for Windows Server 2008 are required:
  - http://support.microsoft.com/kb/958124

This patch fixes a memory leak in Microsoft's WMI, which prevents ISE to establish successful connection with the domain controller.

- http://support.microsoft.com/kb/973995

  This patch fixes different memory leak in Microsoft's WMI, which sporadically prevents the Active Directory domain controller from writing the necessary user login events to the Security Log of the domain controller.

- The following patches for Windows Server 2008 R2 are required (unless SP1 is installed):
  - http://support.microsoft.com/kb/981314

    This patch fixes memory leak in Microsoft's WMI, which sporadically prevents the Active Directory domain controller from writing the necessary user login events to the Security Log of the domain controller.

  - http://support.microsoft.com/kb/2617858

    This patch fixes unexpectedly slow startup or logon process in Windows Server 2008 R2.

- The patches listed at the following link, for WMI related issues on Windows platform are required:
  - http://support.microsoft.com/kb/2591403

These hot fixes are associated with the operation and functionality of the WMI service and its related components.

Step 2 Make sure the Active Directory logs the user login events in the Windows Security Log.

Verify that the Audit Policy settings (part of the Group Policy Management settings) allows successful logons to generate the necessary events in the Windows Security Log (this is the default Windows setting, but you must explicitly ensure that this setting is correct).

Step 3 You must have an Active Directory user with sufficient permissions for ISE to connect to the Active Directory. The following instructions show how to define permissions either for admin domain group user or none admin domain group user:

- Permissions Required when an Active Directory User is a Member of the Domain Admin Group
- Permissions Required when an Active Directory User is Not a Member of the Domain Admin Group

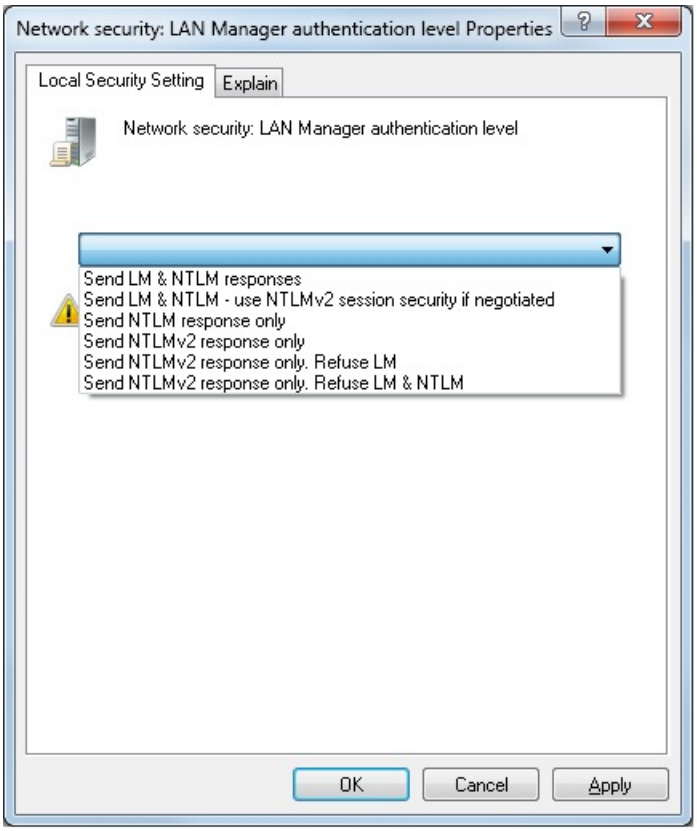
Step 4 The Active Directory user used by ISE can be authenticated either by NT Lan Manager (NTLM) v1 or v2. You need to verify that the Active Directory NTLM settings are aligned with ISE NTLM settings to ensure successful authenticated connection between ISE and the Active Directory Domain Controller. The following table shows all Microsoft NTLM options, and which ISE NTLM actions are supported. If ISE is set to NTLMv2, all six options described in are supported. If ISE is set to support NTLMv1, only the first five options are supported.

Table 3: Supported Authentication Types Based on ISE and AD NTLM Version Settings

ISE NTLM Setting Options / Active Directory (AD) NTLM Setting Options NTLMv1 NTLMv2	**NTLMv1**	**NTLMv2**
Send LM & NTLM responses connection is allowed connection is allowed	Connection is allowed	Connection is allowed

ISE NTLM Setting Options / Active Directory (AD) NTLM Setting Options NTLMv1 NTLMv2	NTLMv1	NTLMv2
Send LM & NTLM - use NTLMv2 session security if negotiated connection is allowed connection is allowed	Connection is allowed	Connection is allowed
Send NTLM response only connection is allowed connection is allowed	Connection is allowed	Connection is allowed
Send NTLMv2 response only connection is allowed connection is allowed	Connection is allowed	Connection is allowed
Send NTLMv2 response only. Refuse LM connection is allowed connection is allowed	Connection is allowed	Connection is allowed
Send NTLMv2 response only. Refuse LM & NTLM connection is refused connection is allowed	Connection is refused	Connection is allowed

Figure 4: MS NTLM Authentication Type Options



Step 5 Make sure that you have created a firewall rule to allow traffic to `dllhost.exe` on Active Directory domain controllers.

You can either turn the firewall off, or allow access on a specific IP (ISE IP address) to the following ports:

- TCP 135: General RPC Port. When doing asynchronous RPC calls, the service listening on this port tells the client which port the component servicing this request is using.
- UDP 137: Netbios Name Resolution
- UDP 138: Netbios Datagram Service
- TCP 139: Netbios Session Service
- TCP 445: SMB

Higher ports are assigned dynamically or you can configure them manually. We recommend that you add %SystemRoot%\System32\dllhost.exe as a target. This program manages ports dynamically.

All firewall rules can be assigned to specific IP (ISE IP).

Set the Windows Audit Policy

Ensure that the **Audit Policy** (part of the **Group Policy Management** settings) allows successful logons. This is required to generate the necessary events in the Windows Security Log of the AD domain controller machine. This is the default Windows setting, but you must verify that this setting is correct.

Step 1 Choose **Start** > **Programs** > **Administrative Tools** > **Group Policy Management**.

Step 2 Navigate under Domains to the relevant domain and expand the navigation tree.

Step 3 Choose **Default Domain Controller Policy**, right click and choose **Edit**.

The Group Policy Management Editor appears.

Step 4 Choose **Default Domain Controllers Policy** > **Computer Configuration** > **Policies** > **Windows Settings** > **Security Settings**.

- For Windows Server 2003 or Windows Server 2008 (non-R2), choose **Local Policies** > **Audit Policy**. For the two Policy items, **Audit Account Logon Events** and **Audit Logon Events**, ensure that the corresponding **Policy Setting** either directly or indirectly includes the **Success** condition. To include the Success condition indirectly, the **Policy Setting** must be set to **Not Defined**, indicating that the effective value will be inherited from a higher level domain, and the **Policy Setting** for that higher level domain must be configured to explicitly include the **Success** condition.
- For Windows Server 2008 R2 and Windows 2012, choose **Advanced Audit Policy Configuration** > **Audit Policies** > **Account Logon**. For the two Policy items, **Audit Kerberos Authentication Service** and **Audit Kerberos Service Ticket Operations**, ensure that the corresponding Policy Setting either directly or indirectly includes the Success condition, as described above.

Step 5 If any Audit Policy item settings have been changed, you should then run `gpupdate /force` to force the new settings to take effect.

Set Permissions when Microsoft Active Directory Users are in Domain Admin Group

For Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2, the Domain Admin group does not have full control of certain registry keys in the Windows operating system by default. The Microsoft Active Directory administrator must give the Microsoft Active Directory user full control permissions on the following registry keys:

- **HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}**
- **HKLM\Software\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}**

The following Microsoft Active Directory versions require no registry changes:

- Windows 2003
- Windows 2003R2
- Windows 2008

To grant full control, the Microsoft Active Directory admin must first take ownership of the key:

Step 1 Right-click the key icon and choose the **Owner** tab.

Step 2 Click **Permissions**.

Step 3 Click **Advanced**.

Permissions for Microsoft Active Directory Users Not in Domain Admin Group

For Windows Server 2012 R2, give the Microsoft AD user full control permissions on the following registry keys:

- `HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}`
- `HKLM\Software\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}`

Use the following commands in Windows PowerShell to check if full permission is given to the registry keys:

- ```
  get-acl -path
  "Microsoft.PowerShell.Core\Registry::HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}"
  | format-list
  ```
- ```
  get-acl -path
  "hklm:\Software\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}" |
  format-list
  ```

The following permissions are required when a Microsoft AD user is not in the Domain Admin group, but is in the Domain Users group:

- Add registry keys to allow Cisco ISE to connect to the domain controller.
- Permissions to Use DCOM on the Domain Controller

- Set Permissions for Access to WMI Root and CIMv2 Namespace

These permissions are only required for the following Microsoft AD versions:

- Windows 2003
- Windows 2003R2
- Windows 2008
- Windows 2008 R2
- Windows 2012
- Windows 2012 R2
- Windows 2016

Add Registry Keys to Allow Cisco ISE to Connect to the Domain Controller

You must manually add some registry keys to the domain controller to allow Cisco ISE to connect as a domain user, and retrieve login authentication events. An agent is not required on the domain controllers or on any machines in the domain.

The following registry script shows the keys to add. You can copy and paste this into a text file, save the file with a .reg extension, and double click the file to make the registry changes. To add registry keys, the user must be an owner of the root key.

```
Windows Registry Editor Version 5.00

[HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}]
"AppID"="{76A64158-CB41-11D1-8B02-00600806D9B6}"

[HKEY_CLASSES_ROOT\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6}]
"DllSurrogate"="  "

[HKEY_CLASSES_ROOT\Wow6432Node\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6}]
"DllSurrogate"="  "
```

Make sure that you include two spaces in the value of the DllSurrogate key. If the registry is manually updated, you must include only the two spaces and do not include the quotes. While updating the registry manually, ensure that quotes are not included for AppID, DllSurrogate, and its values.

Retain the empty lines as shown in the preceding script, including the empty line at the end of the file.

Use the following commands in the Windows command prompt to confirm if the registry keys are created and have the correct values:

- `reg query "HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}" /f "{76A64158-CB41-11D1-8B02-00600806D9B6}" /e`
- `reg query HKEY_CLASSES_ROOT\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6} /f "  " /e`
- `reg query HKEY_CLASSES_ROOT\Wow6432Node\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6} /f "  " /e`

Permissions to Use DCOM on the Domain Controller

The Microsoft Active Directory user who is used for Cisco ISE Passive Identity service must have the permissions to use DCOM on the domain controller server. Configure permissions with the **dcomcnfg** command line tool.

Step 1 Run the **dcomcnfg** tool from the command line.

Step 2 Expand **`Component Services`**.

Step 3 Expand **Computers** > **My Computer**.

Step 4 Choose **Action** from the menu bar, click **Properties**, and click **COM Security**.

Step 5 The account that Cisco ISE uses for both access and launch must have Allow permissions. Add the Microsoft Active Directory user to all the four options, **Edit Limits** and **Edit Default** for both **Access Permissions** and **Launch and Activation Permissions**.

Step 6 Allow all local and remote accesses for both **Access Permissions** and **Launch and Activation Permissions**.

Figure 5: Local and Remote Accesses for Access Permissions

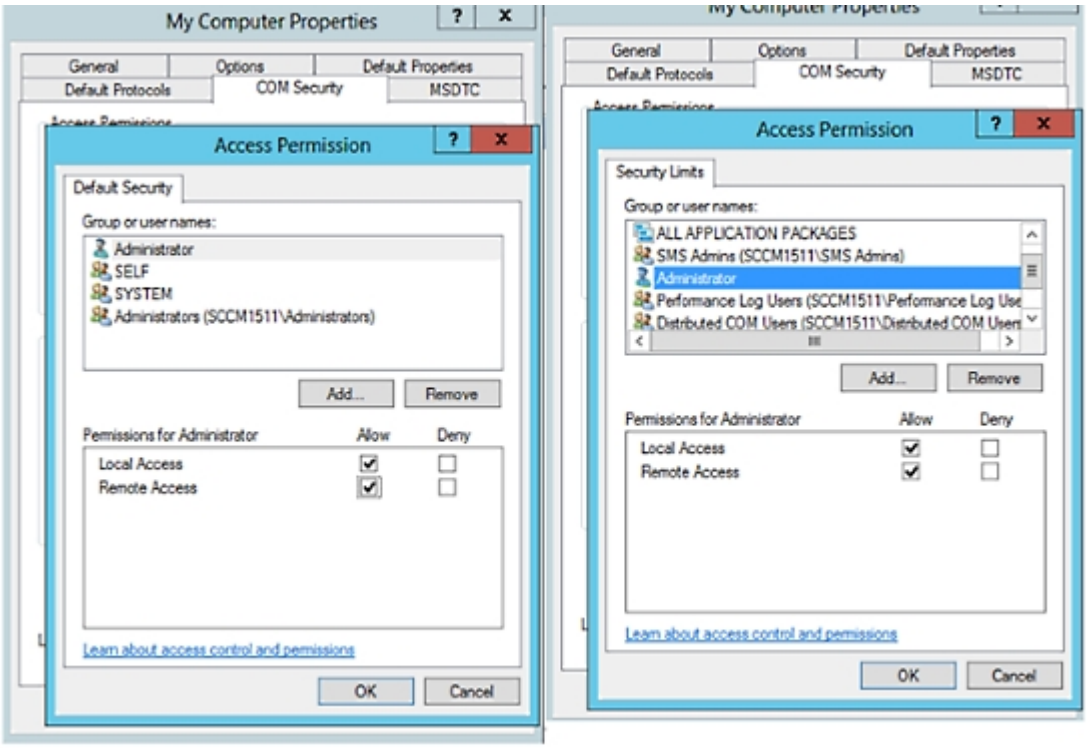
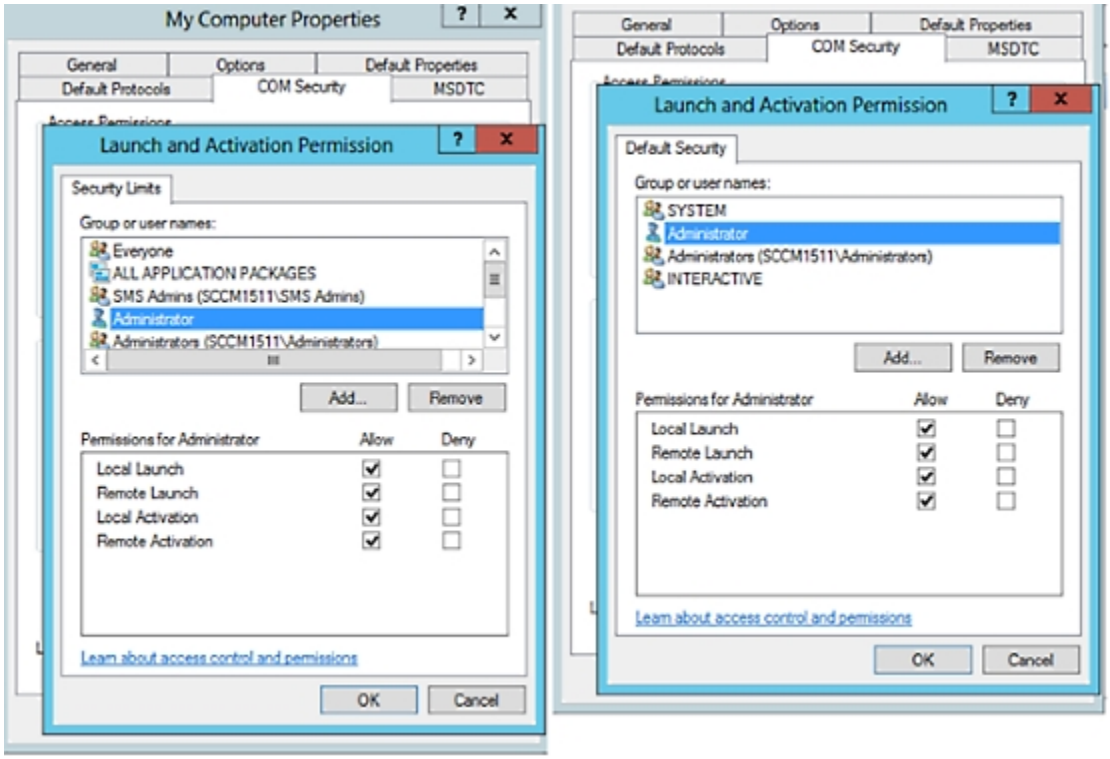


Figure 6: Local and Remote Accesses for Launch and Activation Permissions



Set Permissions for Access to WMI Root and CIMv2 Namespace

By default, Microsoft Active Directory users do not have permissions for the Execute Methods and Remote Enable. You can grant access using the wmimgmt.msc MMC console.

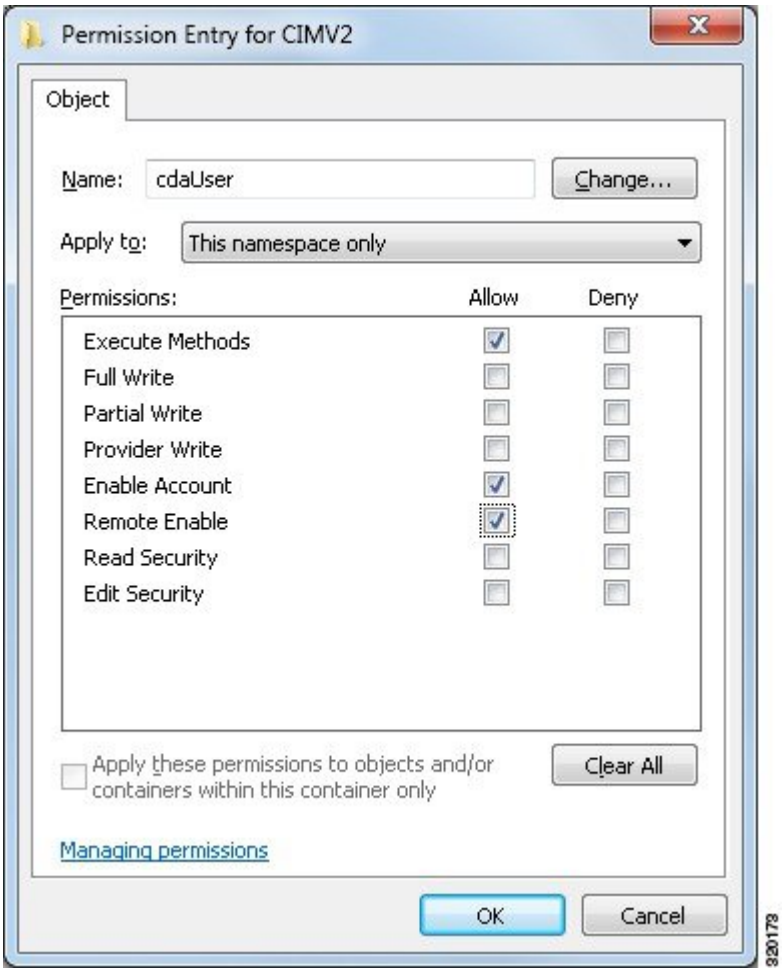
Step 1 Choose **Start** > **Run** and enter `wmimgmt.msc`.

Step 2 Right-click **WMI Control** and click **Properties**.

Step 3 Under the **Security** tab, expand **Root** and choose **CIMV2**.

Step 4 Click **Security**.

Step 5 Add the Microsoft Active Directory user, and configure the required permissions as shown in the following image.



Grant Access to the Security Event Log in the AD Domain Controller

On Windows 2008 and later, you can grant access to the AD Domain controller logs by adding the ISE ID Mapping user to a group called Event Log Readers.

On all older versions of Windows, you must edit a registry key, as shown below.

Step 1 To delegate access to the Security event logs, find the SID for the account .

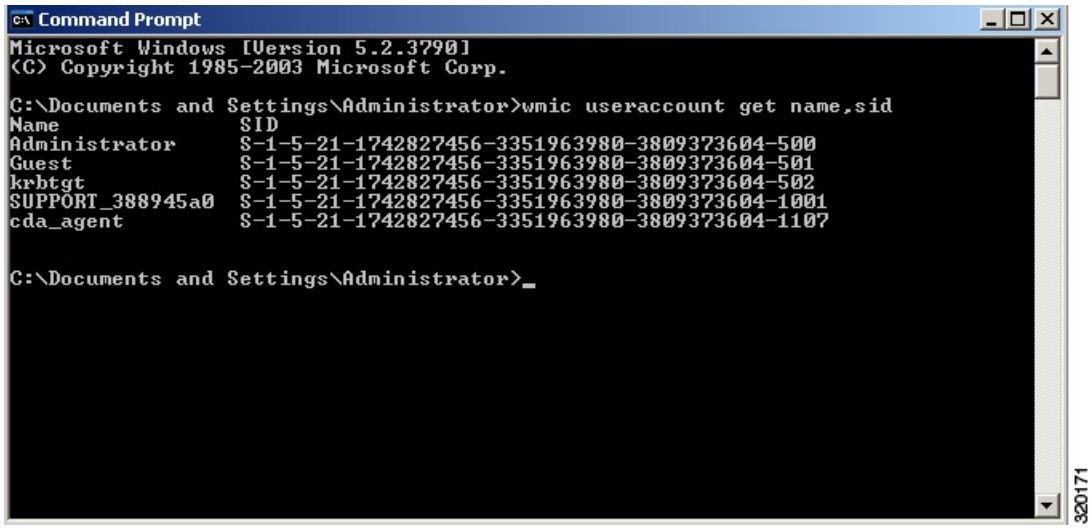
Step 2 Use the following command from the command line, also shown in the diagram below, to list all the SID accounts.

```
wmic useraccount get name,sid
```

You can also use the following command for a specific username and domain:

```
wmic useraccount where name="iseUser" get domain,name,sid
```

Figure 7: List All the SID Accounts



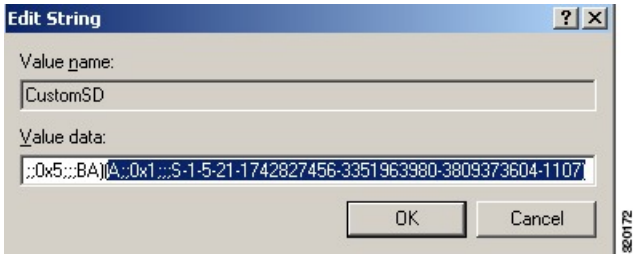
Step 3 Find the SID, open the Registry Editor, and browse to the following location:

`HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Services/Eventlog`

Step 4 Click on **Security**, and double click **CustomSD**.

For example, to allow read access to the ise_agent account `(SID - S-1-5-21-1742827456-3351963980-3809373604-1107)`, enter `(A;;0x1;;;S-1-5-21-1742827456-3351963980-3809373604-1107)`.

Figure 8: Edit CustomSD String



Step 5 Restart the WMI service on the Domain Controller. You can restart the WMI services in the following two ways:

a) Run the following commands from the CLI:

net stop winmgmt

net start winmgmt

b) Run `Services.msc`, which opens the Windows Services Management tool. In the Windows Services Management window, locate the **Windows Management Instrumentation** service, right click, and select **Restart**.

Easy Connect

Easy Connect enables you to easily connect users from a wired endpoint to a network in a secure manner and monitor those users by authenticating them through an Active Directory Domain Controller and not by Cisco ISE. With Easy Connect, Cisco ISE collects user authentication information from the Active Directory Domain Controller. Easy Connect connects to a Windows system (Active Directory) using the MS WMI interface and queries logs from the Windows event messaging, hence it currently only supports Windows-installed endpoints. Easy Connect supports wired connections using MAB, which is much easier to configure than 802.1X. Unlike 802.1X, with Easy Connect and MAB:

- You don't need to configure supplicants
- You don't need to configure PKI
- ISE issues a CoA after the external server (AD) authenticates the user

Easy Connect supports these modes of operation:

- Enforcement-mode: ISE actively downloads the authorization policy to the network device for enforcement based on the user credentials.
- Visibility-mode: Cisco ISE publishes session merge and accounting information received from the NAD device sensor in order to send that information to pxGrid.

In both cases, users authenticated with Active Directory (AD) are shown in the Cisco ISE live sessions view, and can be queried from the session directory using Cisco pxGrid interface by third-party applications. The known information is the user name, IP address, the AD DC host name, and the AD DC NetBios name. For more information about pxGrid, see Cisco pxGrid Node.

Once you have set up Easy Connect, you can then filter certain users, based on their name or IP address. For example, if you have an administrator from IT services who logs in to an endpoint in order to assist the regular user with that endpoint, you can filter out the administrator activity so it does not appear in Live Sessions, but rather only the regular user of that endpoint will appear. To filter passive identity services, see Filter Passive Identity Services, on page 95.

Easy Connect Restrictions

- MAC Authentication Bypass (MAB) supports Easy Connect. Both MAB and 802.1X can be configured on the same port, but you must have a different ISE policy for each service.
- Only MAB connections are currently supported. You do not need a unique authentication policy for connections, because the connection is authorized and permissions are granted by an Easy Connect condition defined in the authorization policy.
- Easy Connect is supported in High Availability mode. Multiple nodes can be defined and enabled with a Passive ID. ISE then automatically activates one PSN, while the other nodes remain in standby.
- Only Cisco Network Access Devices (NADs) are supported.
- IPv6 is not supported.
- Wireless connections are not currently supported.
- Only Kerberos auth events are tracked and therefore Easy Connect enables only user authentication and does not support machine authentication.

Easy Connect requires configuration in ISE, while the Active Directory Domain server must also have the correct patches and configuration based on instructions and guidelines issued by Microsoft. For information about configuring the Active Directory domain controller for Cisco ISE, see Active Directory Requirements to Support Easy Connect and Passive Identity services, on page 39

Easy Connect Enforcement Mode

Easy Connect enables users to log on to a secure network from a wired endpoint (usually a PC) with a Windows operating system, by using MAC address bypass (MAB) protocol, and accessing Active Directory (AD) for authentication. Easy Connect listens for a Windows Management Instrumentation (WMI) event from the Active Directory server for information about authenticated users. When AD authenticates a user, the Domain Controller generates an event log that includes the user name and IP address allocated for the user. Cisco ISE receives notification of log in from AD, and then issues a RADIUS Change of Authorization (CoA).

Note MAC address lookup is not done for a MAB request when the Radius service-type is set to call-check. Therefore the return to the request is access-accept. This is the default configuration.

Easy Connect Enforcement Mode Process Flow

The Easy Connect Enforcement mode process is as follows:

1. The user connects to the NAD from a wired endpoint (such as a PC for example).
2. The NAD (which is configured for MAB) sends an access request to Cisco ISE. Cisco ISE responds with access, based on user configuration, allowing the user to access AD. Configuration must allow at least access to DNS, DHCP, and AD.
3. The user logs in to the domain and a security audit event is sent to Cisco ISE.
4. ISE collects the MAC address from RADIUS and the IP address and domain name, as well as accounting information (login information) about the user, from the security audit event.
5. After all data is collected and merged in the session directory, Cisco ISE issues a CoA to the NAD (based on the appropriate policy managed in the policy service node), and the user is provided access by the NAD to the network based on that policy.

Figure 9: Easy Connect Enforcement Mode Basic Flow

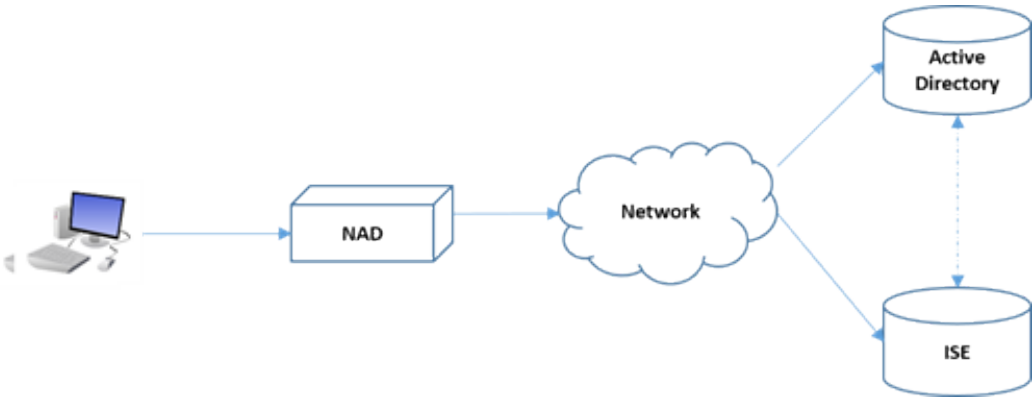
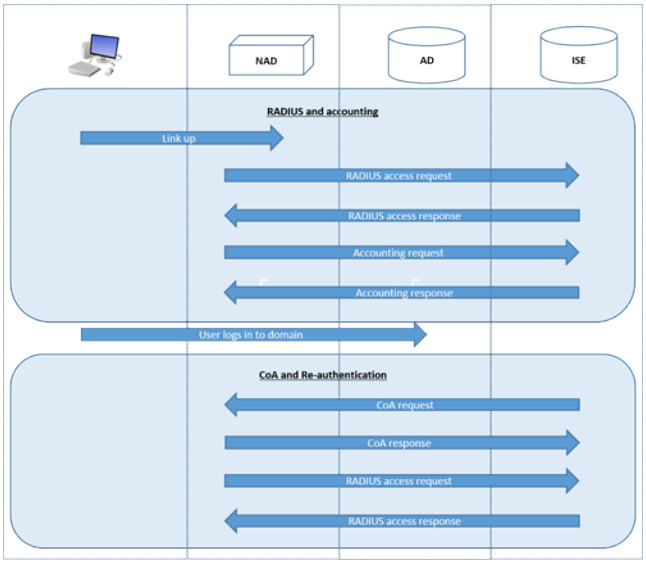


Figure 10: Easy Connect Enforcement Mode Detailed Flow

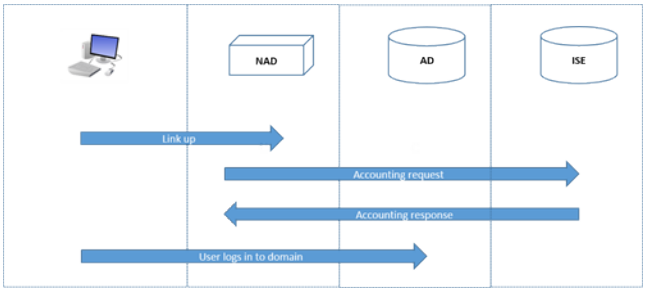


For more information about configuring Enforcement mode, see Configure Easy Connect Enforcement Mode, on page 51.

Easy Connect Visibility Mode

With the Visibility mode, Cisco ISE only monitors accounting information from RADIUS (part of the device sensor feature in the NAD) and does not perform authorization. Easy Connect listens for RADIUS Accounting and WMI events, and publishes that information to logs and reports, (and optionally, to pxGrid). Both RADIUS accounting start and session termination are published to pxGrid during user login using Active Directory when pxGrid is setup.

Figure 11: Easy Connect Visibility Mode Flow



For more information about configuring Easy Connect Visibility mode, see Configure Easy Connect Visibility Mode, on page 52 .

Configure Easy Connect Enforcement Mode

Before you begin

- For best performance, deploy a dedicated PSN to recieve WMI events.

- Create a list of Active Directory Domain Controllers for the WMI node, which receives AD login events.
- Determine the Microsoft Domain that Cisco ISE must join to fetch user groups from Active Directory.
- Determine the Active Directory groups that are used as a reference in the authorization policy.
- If you are using pxGrid to share session data from network devices with other pxGrid-enabled systems, then define a pxGrid persona in your deployment. For more information about pxGrid, see Cisco pxGrid Node
- After successful MAB, the NAD must provide a limited-access profile, which allows the user on that port access to the Active Directory server.

Note Passive Identity Service can be enabled on multiple nodes, but Easy Connect can only operate on one node at a time. If you enable the service for multiple nodes, ISE will automatically determine which node to use for the active Easy Connect session.

Step 1 Choose **Administration** > **System** > **Deployment**, open a node, and under **General Settings**, enable **Enable Passive Identity Service**.

Step 2 Configure an Active Directory join point and domain controller to be used by Easy Connect. For more information, see Active Directory Requirements to Support Easy Connect and Passive Identity services, on page 39.

Step 3 (Optional) Choose **Administration** > **Identity Management** > **External Identity Sources** > **Active Directory**. Click the **Groups** tab, and add the Active Directory groups you plan to use in your authorization policies.
The Active Directory groups that you map for the Domain Controller are dynamically updated in the PassiveID dictionary and can then be used when you set up your policy conditions rules.

Step 4 **Note** **Passive Identity Tracking** must be enabled for all profiles used for Easy Connect authorization in order for the Easy Connect process to run properly and enable ISE to issue a CoA.

Choose **Policy** > **Policy Elements** > **Results** > **Authorization** > **Authorization Profiles**. For any profiles to be used by Easy Connect, open the profile and enable **Passive Identify Tracking**.

Step 5 Choose **Policy** > **Policy Elements** > **Conditions** > **Authorization** > **Simple Conditions**, to create rules for Easy Connect. Click **Add** and define the condition:

a) Enter a name and description.
b) From **Attribute**, go to the PassiveID dictionary and select either PassiveID_Groups to create a condition for domain controller groups, or select PassiveID_user to create a condition for individual users.
c) Enter the correct operation.
d) Enter the user name or group name to be included in the policy.

Step 6 Click **Submit**.

Configure Easy Connect Visibility Mode

Before you begin

- For best performance, deploy a dedicated PSN to recieve WMI events.

- Create a list of Active Directory Domain Controllers for the WMI node, which receives AD login events.
- Determine the Microsoft Domain that Cisco ISE must join to fetch user groups from Active Directory.
- If you are using pxGrid to share session data from network devices with other pxGrid-enabled systems, then define a pxGrid persona in your deployment. For more information about pxGrid, see Cisco pxGrid Node

Step 1 Choose **Administration** > **System** > **Deployment**, open a node, and under **General Settings**, enable **Enable Passive Identity Service**.

Step 2 Configure an Active Directory join point and domain controller to be used by Easy Connect. For more information, see Active Directory Requirements to Support Easy Connect and Passive Identity services, on page 39.

PassiveID Work Center

Passive Identity Connector (the PassiveID work center) offers a centralized, one-stop installation and implementation enabling you to easily and simply configure your network in order to receive and share user identity information with a variety of different security product subscribers such as Cisco Firepower Management Center (FMC) and Stealthwatch. As the full broker for passive identification, the PassiveID work center collects user identities from different provider sources, such as Active Directory Domain Controllers (AD DC), maps the user login information to the relevant IP addresses in use and then shares that mapping information with any of the subscriber security products that you have configured.

What is Passive Identity?

Standard flows offered by Cisco Identity Services Engine (ISE), which provide an authentication, authorization and accounting (AAA) server, and utilize technologies such as 802.1X or Web Authentication, communicate directly with the user or endpoint, requesting access to the network, and then using their login credentials in order to verify and actively authenticate their identity.

Passive identity services do not authenticate users directly, but rather gather user identities and IP addresses from external authentication servers such as Active Directory, known as providers, and then share that information with subscribers. the PassiveID work center first receives the user identity information from the provider, usually based on the user login and password, and then performs the necessary checks and services in order to match the user identity with the relevant IP address, thereby delivering the authenticated IP address to the subscriber.

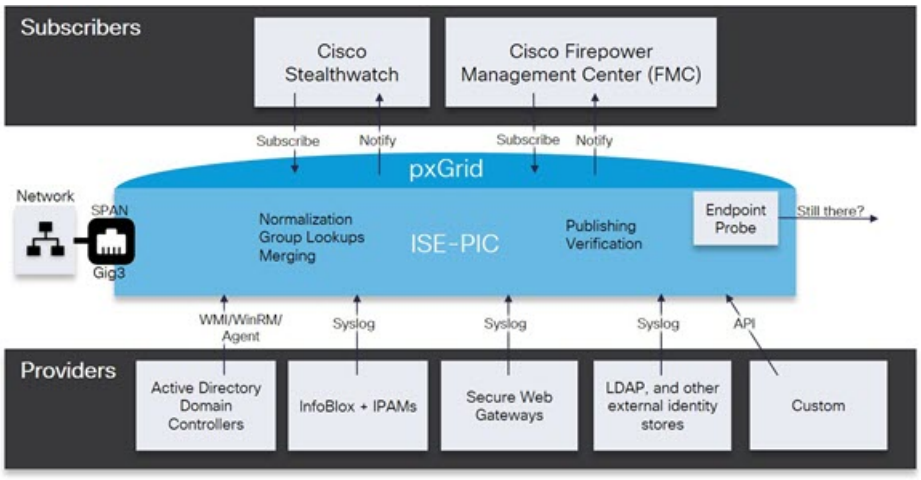
Passive Identity Connector (PassiveID work center) Flow

The flow for the PassiveID work center is as follows:

1. Provider performs the authentication of the user or endpoint.
2. Provider sends authenticated user information to Cisco ISE.
3. Cisco ISE normalizes, performs lookups, merges, parses and maps user information to IP addresses and publishes mapped details to pxGrid.
4. pxGrid subscribers receive the mapped user details.

The following diagram illustrates the high-level flow offered by Cisco ISE.

Figure 12: High Level Flow



Initial Setup and Configuration

To get started using Cisco PassiveID work center quickly, follow this flow:

1. Ensure you have properly configured the DNS server, including configuring reverse lookup for the client machine from Cisco ISE. For more information, see DNS Server, on page 20.
2. Enable the Passive Identity and pxGrid services on the dedicated Policy server (PSN) you intend to use for any of the Passive Identity services. Choose **Administration** > **System** > **Deployment**, open the relevant node, and under **General Settings**, enable **Enable Passive Identity Service** and **pxGrid**.
3. Synchronize clock settings for the NTP servers.
4. Configure an initial provider with the ISE Passive Identity Setup. For more information, see Getting Started with the PassiveID Setup, on page 56
5. Configure a single or multiple subscribers. For more information, see Subscribers, on page 98

After setting up an initial provider and subscriber, you can easily create additional providers (see Additional Passive Identity Service Providers, on page 61) and manage your passive identification from the different providers in the PassiveID work center.

PassiveID Work Center Dashboard

The Cisco PassiveID Work Center dashboard displays consolidated and correlated summary and statistical data that is essential for effective monitoring and troubleshooting, and is updated in real time. Dashlets show activity over the last 24 hours, unless otherwise noted. To access the dashboard, choose **Work Centers** > **PassiveID** and then from the left panel choose **Dashboard**. You can only view the Cisco PassiveID Work Center Dashboard in the Primary Administration Node (PAN).

- The **Main** view has a linear Metrics dashboard, chart dashlets, and list dashlets. In the PassiveID Work Center, the dashlets are not configurable. Available dashlets include:

- **Passive Identity Metrics**: Displays the total number of unique live sessions currently being tracked, the total number of identity providers configured in the system, the total number of agents actively delivering identity data, and the total number of subscribers currently configured.
- **Providers**: Providers provide user identity information to PassiveID Work Center. You configure the ISE probe (mechanisms that collect data from a given source) through which to receive information from the provider sources. For example, an Active Directory (AD) probe and an Agents probe both help ISE-PIC collect data from AD (each with different technology) while a Syslog probe collects data from a parser that reads syslog messages.
- **Subscribers**: Subscribers connect to ISE to retrieve user identity information.
- **OS Types**: The only OS type that can be displayed is Windows. Windows types display by Windows versions. Providers do not report the OS type, but ISE can query Active Directory to get that information. Up to 1000 entries are displayed in the dashlet.
- **Alarms**: User identity-related alarms.

Active Directory as a Probe and a Provider

Active Directory (AD) is a highly secure and precise source from which to receive user identity information, including user name, IP address, and domain name.

The AD probe, a Passive Identity service, collects user identity information from AD through WMI technology, while other probes use AD as a user identity provider through other technologies and methods. For more information about other probes and provider types offered by ISE, see Additional Passive Identity Service Providers, on page 61.

By configuring the Active Directory probe you can also then quickly configure and enable these other probes (which also use Active Directory as their source):

- Active Directory Agents, on page 63

Note The Active Directory agents are only supported on Windows Server 2008 and higher.

- SPAN, on page 72
- Endpoint Probe, on page 96

In addition, configure the Active Directory probe in order to use AD user groups when collecting user information. You can use AD user groups for the AD, Agents, SPAN, and Syslog probes. For more information about AD groups, see Configure Active Directory User Groups, on page 26.

Set Up an Active Directory (WMI) Probe

To configure Active Directory and WMI for Passive Identity service you can use the Passive ID Work Center Wizard (see Getting Started with the PassiveID Setup, on page 56) or you can follow the steps as follows:

1. Configure the Active Directory probe. See Add an Active Directory Join Point and Join Cisco ISE Node to the Join Point, on page 21.

2. Create a list of Active Directory Domain Controllers for the WMI-configured node (or nodes) that receives AD login events. See #unique_537.
3. Configure the Active Directory in order for it to integrate with ISE. See #unique_538.
4. (Optional) Manage the Active Directory Provider, on page 58.

For more information, see Active Directory Requirements to Support Easy Connect and Passive Identity services, on page 39.

Getting Started with the PassiveID Setup

ISE-PIC offers a wizard from which you can easily and quickly configure Active Directory as your first user identity provider, in order to receive user identities from Active Directory. By configuring Active Directory for ISE-PIC, you also simplify the process for configuring other provider types later on. Once you have configured Active Directory, you must then configure a Subscriber (such as Cisco Firepower Management Center (FMC) or Stealthwatch), in order to define the client that is to receive the user data. For more information about subscribers, see Subscribers, on page 98.

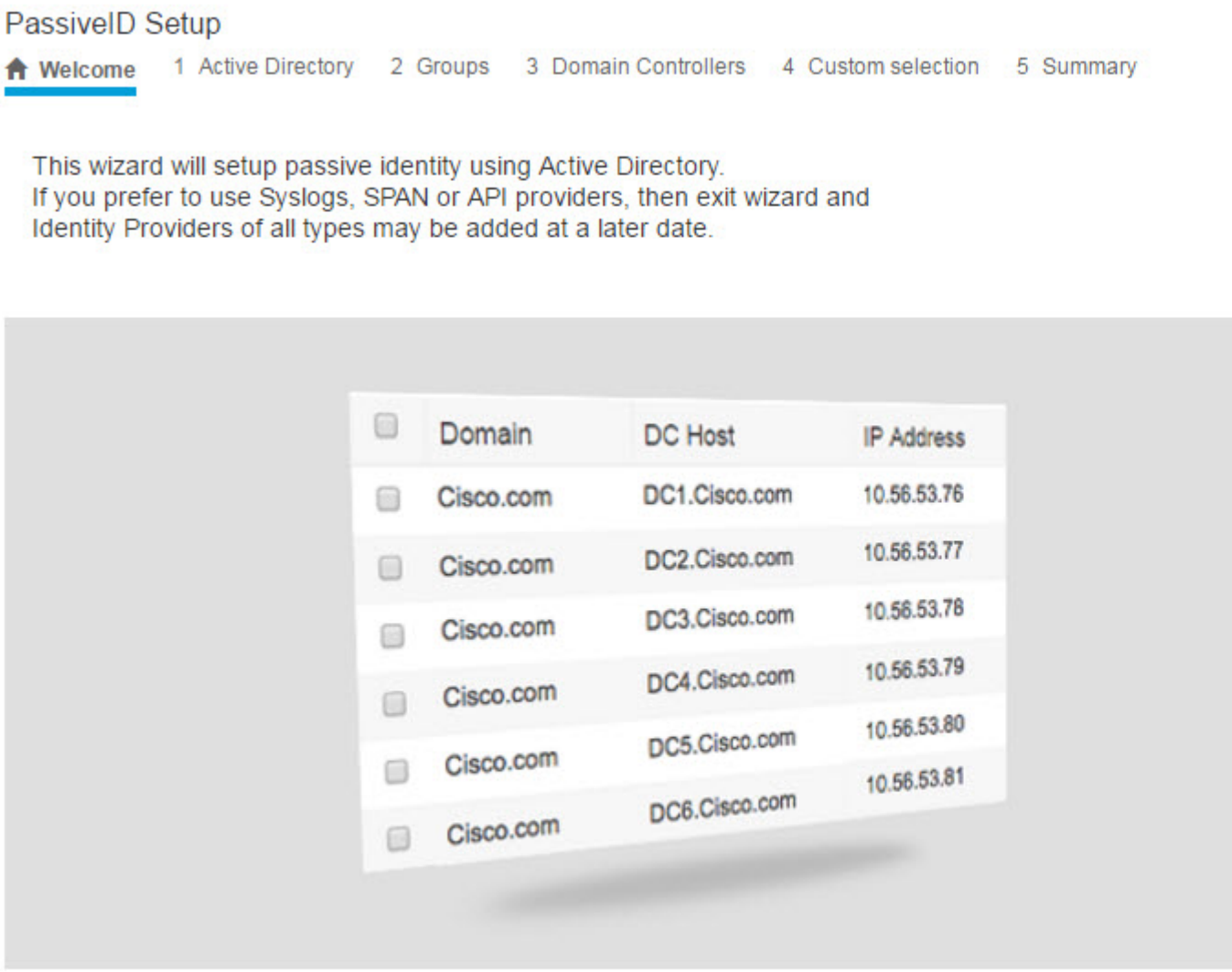
Before you begin

- Ensure the Microsoft Active Directory server does not reside behind a network address translator and does not have a Network Address Translation (NAT) address.
- Ensure the Microsoft Active Directory account intended for the join operation is valid and is not configured with the Change Password on Next Login.
- Ensure you have the privileges of a Super Admin or System Admin in ISE.
- Enable the Passive Identity and pxGrid services on the dedicated Policy server (PSN) you intend to use for any of the Passive Identity services. Choose **Administration** > **System** > **Deployment**, open the relevant node, and under **General Settings**, enable **Enable Passive Identity Service** and **pxGrid**.
- Ensure that ISE has an entry in the domain name server (DNS). Ensure you have properly configured reverse lookup for the client machine from ISE. For more information, see DNS Server, on page 20

Step 1 Choose **Work Centers** > **PassiveID**. From the Passive Identity Connector Overview screen, click **Passive Identity Wizard**.

The PassiveID Setup window appears.

Figure 13: The PassiveID Setup



Step 2 Click **Next** to begin the wizard.

Step 3 Enter a unique name for this Active Directory join point. Enter the domain name for the Active Directory Domain to which this node is connected, and enter your Active Directory administrator user name and password.

It is strongly recommended that you choose **Store credentials**, in which case your administrator's user name and password will be saved in order to be used for all Domain Controllers (DC) that are configured for monitoring.

Step 4 Click **Next** to define Active Directory groups and check any user groups to be included and monitored.
The Active Directory user groups automatically appear based on the Active Directory join point you configured in the previous step.

Step 5 Click **Next**. Select the DCs to be monitored. If you choose Custom, then from the next screen select the specific DCs for monitoring. When finished, click **Next**.

Step 6 Click **Exit** to complete the wizard.

What to do next

When you finish configuring Active Directory as your initial provider, you can easily configure additional provider types as well. For more information, see Additional Passive Identity Service Providers, on page 61. Furthermore, you can now also configure a subscriber, designated to receive the user identity information that is collected by any of the providers you have defined. For more information, see Subscribers, on page 98.

Manage the Active Directory Provider

Once you have created and configured your Active Directory join points, continue to manage the Active Directory probe with these tasks:

- Test Users for Active Directory Authentication, on page 33
- View Active Directory Joins for a Node, on page 34
- Diagnose Active Directory Problems, on page 34
- Leave the Active Directory Domain, on page 25
- Delete Active Directory Configurations, on page 33
- Enable Active Directory Debug Logs, on page 35

Active Directory Settings

Active Directory (AD) is a highly secure and precise source from which to receive user information, including user name and IP address.

To create and manage Active Directory probes by creating and editing join points, choose **Work Centers** > **PassiveID** > **Providers** > **Active Directory**.

For more information, see Add an Active Directory Join Point and Join Cisco ISE Node to the Join Point, on page 21.

Table 4: Active Directory Join Point Name Settings and Join Domain Window

Field Name	Description
Join Point Name	A unique name that distinguishes this configured join point quickly and easily.
Active Directory Domain	The domain name for the Active Directory Domain to which this node is connected.
Domain Administrator	This is the user principal name or the user account name for the Active Directory user with administrator priveleges.

Field Name	Description
Password	This is the domain administrator's password as configured in Active Directory.
Specifiy Organizational Unit	Enter the administrator's organizational unit information
Store Credentials	It is strongly recommended that you choose **Store credentials**, in which case your administrator's user name and password will be saved in order to be used for all Domain Controllers (DC) that are configured for monitoring. For the Endpoint probe, you must choose **Store credentials**.

Table 5: Active Directory Join/Leave Window

Field Name	Description
ISE Node	The URL for the specific node in the installation.
ISE Node Role	Indicates whether the node is the Primary or Secondary node in the installation.
Status	Indicates whether the node is actively joined to the Active Directory domain.
Domain Controller	For nodes that are joined to Active Directory, this column indicates the specific Domain Controller to which the node is connected in the Active Directory Domain.
Site	When an Active Directory forest is joined with ISE, this field indicates the specific Active Directory site within the forest as it appears in the Active Directory Sites and Services area.

Table 6: Passive ID Domain Controllers (DC) List

Field	Description
Domain	The fully qualified domain name of the server on which the domain controller is located.
DC Host	The host on which the domain controller is located.
Site	When an Active Directory forest is joined with ISE, this field indicates the specific Active Directory site within the forest as it appears in the Active Directory Sites and Services area.
IP Address	The IP address of the domain controller.

Field	Description
Monitor Using	Monitor Active Directory domain controllers for user identity information by one of these methods: • WMI: Monitor Active Directory directly with the WMI infrastructure. • Agent name: If you have defined agents to monitor Active Directory for user information, select the Agent protocol and choose the agent from the dropdown list that you would like to use. For more information about agents, see Active Directory Agents, on page 63.

Table 7: Passive ID Domain Controllers (DC) Edit Window

Field Name	Description
Host FQDN	Enter the fully qualified domain name of the server on which the domain controller is located.
Description	Enter a unique description for this domain controller in order to easily identiy it.
User Name	The administrator's user name for accessing Active Directory.
Password	The administrator's password for accessing Active Directory.
Protocol	Monitor Active Directory domain controllers for user identity information by one of these methods: • WMI: Monitor Active Directory directly with the WMI infrastructure. • Agent name: If you have defined agents to monitor Active Directory for user information, select the Agent protocol and choose the agent from the dropdown list that you would like to use. For more information about agents, see Active Directory Agents, on page 63.

Active Directory groups are defined and managed from Active Directory and the groups for the Active Directory that is joined to this node can be viewed from this tab. For more information about Active Directory, see https://msdn.microsoft.com/en-us/library/bb742437.aspx.

Table 8: Active Directory Advanced Settings

Field Name	Description
History interval	The time during which the Passive Identity service reads user login information that already occurred. This is required upon startup or restart of the Passive Identity service to catch up with events generated while it was unavailable. When the Endpoint probe is active, it maintains the frequency of this interval.
User session aging time	The amount of time the user can be logged in. The Passive Identity service identifies new user login events from the DC, however the DC does not report when the user logs off. The aging time enables Cisco ISE to determine the time interval for which the user is logged in.
NTLM Protocol settings	You can select either NTLMv1 or NTLMv2 as the communications protocol between Cisco ISE and the DC. NTLMv2 is the recommended default.

Additional Passive Identity Service Providers

In order to enable ISE to provide identity information (Passive Identity Service) to consumers that subscribe to the service (subscribers), you must first configure an ISE probe, which connects to the identity provider.

The table below provides details about all of the provider and probe types available from ISE. For more information about Active Directory, see Active Directory as a Probe and a Provider, on page 55.

You can define these provider types:

Table 9: Provider Types

Provider Type (Probe)	Description	Source System (Provider)	Technology	User Identity Information Collected	Document Link
Active Directory (AD)	A highly secure and precise source, as well as the most common, from which to receive user information. As a probe, AD works with WMI technology to deliver authenticated user identities. In addition, AD itself, rather than the probe, functions as a source system (a provider) from which other probes retrieve user data as well.	Active Directory Domain Controller	WMI	• User name • IP address • Domain	Active Directory as a Probe and a Provider, on page 55
Agents	A native 32-bit application installed on Active Directory domain controllers or on member servers. The Agent probe is a quick and efficient solution when using Active Directory for user identity information.		Agents installed on the domain controller or on a member server.	• User name • IP address • Domain	Active Directory Agents, on page 63
Endpoint	Always runs in the background in addition to other configured probes, in order to verify whether the user is still connected.		WMI	Whether the user is still connected	Endpoint Probe, on page 96
SPAN			SPAN, installed on the switch, and Kerberos messages	• User name • IP address • Domain	SPAN, on page 72

Provider Type (Probe)	Description	Source System (Provider)	Technology	User Identity Information Collected	Document Link
	Sits on the network switch in order to listen to network traffic, and extract user identity information based on Active Directory data.				
API providers	Gather user identity information from any system programmed to communicate with a RESTful API client, using the RESTful API service offered by ISE.	Any system programmed to communicate with a REST API client.	RESTful APIs. User identity sent to subscribers in JSON format.	• User name • IP address • Port range • Domain	API Providers, on page 67
Syslog	Parse syslog messages and retrieve user identities, including MAC addresses.	• Regular syslog message providers • DHCP servers	Syslog messages	• User name • IP address • MAC address • Domain	Syslog Providers, on page 74

Note pxGrid sends 200 events per second for session topics to avoid overloading the clients. If the publisher sends more than 200 events, the additional events are queued and sent in next batch.

If pxGrid consistently receives more than 200 events per second for a prolonged period of time, it might consume more memory than usual for storing the backlog events. This might affect the performance of pxGrid.

Active Directory Agents

From the Passive Identity service work center install the native 32-bit application, Domain Controller (DC) agents, anywhere on the Active Directory (AD) domain controller (DC) or on a member server (based on your configurations) to retrieve user identity information from AD and then send those identities to the subscribers you have configured. The Agent probe is a quick and efficient solution when using Active Directory for user identity information. Agents can be installed on a separate domain, or on the AD domain, and once installed, they provide status updates to ISE once every minute.

The agents can be either automatically installed and configured by ISE, or you can manually install them. Upon installation, the following occurs:

- The agent and its associated files are installed at the following path: **`Program Files/Cisco/Cisco ISE PassiveID Agent`**

- A config file called **`PICAgent.exe.config`** is installed indicating the logging level for the agent. You can manually change the logging level from within the config file.
- The CiscoISEPICAgent.log file is stored with all logging messages.
- The nodes.txt file contains the list of all nodes in the deployment with which the agent can communicate. The agent contacts the first node in the list. If that node cannot be contacted, the agent continues to attempt communication according to the order of the nodes in the list. For manual installations, you must open the file and enter the node IP addresses. Once installed (manually or automatically), you can only change this file by manually updating it. Open the file and add, change or delete node IP addresses as necessary.
- The Cisco ISE PassiveID Agent service runs on the machine, which you can manage from the Windows Services dialog box.
- ISE supports up to 100 domain controllers, while each agent can monitor up to 10 domain controllers. In order to monitor 100 domain controllers, you must configure 10 agents.
- The Active Directory agents are only supported on Windows Server 2008 and higher. If you cannot install agents, then use the Active Directory probe for passive identity services. For more information, see Active Directory as a Probe and a Provider, on page 55.

Note Even if you are running the AD agent on a member server, it still queries the Active Directory for the login requests.

Automatically Install and Deploy Active Directory Agents

When configuring the Agent provider to monitor domain controllers for user identities, the agent must be installed on either a member server or on a domain controller. The agents can be either automatically installed by ISE, or you can manually install them. After installation, automatic or manual, you must then configure the installed agent to monitor specified domain controllers rather than the default WMI. This process describes how to enable automatic installation and configure the agent to monitor a domain controller.

Before you begin

Before you begin:

- Configure reverse lookup for the relevant DNS servers from the server side. For more information about the DNS server configuration requirements for ISE, see DNS Server, on page 20
- Ensure Microsoft .NET Framework is updated for the machine designated for the agents, to a minimum of version 4.0. For more information about the .NET framework, see https://www.microsoft.com/net/framework.
- Active Passive ID and pxGrid services. For more information, see Initial Setup and Configuration, on page 54.
- Create an AD join point and add at least one domain controller. For more information about creating join points, see Active Directory as a Probe and a Provider, on page 55.

  Use AD user groups for the AD, Agents, SPAN and Syslog probes. For more information about AD groups, see Configure Active Directory User Groups, on page 26.

Step 1 Choose **Work Centers** > **PassiveID** > **Providers** and then choose **Agents** from the left panel.

Step 2 To add a new agent, click **Add** from the top of the table.

Step 3 To create the new agent and automatically install it on the host that you indicate in this configuration, select **Deploy New Agent**.

Step 4 Complete all mandatory fields in order to configure the client correctly. For more information, see Active Directory Agent Settings, on page 66.

Step 5 Click **Deploy**.
The agent is automatically installed on the host according to the domain that you indicated in the configuration, and the settings are saved. The agent now also appears in the Agents table and can be applied to monitor specified domain controllers, as described in the following steps.

Step 6 Choose **Work Centers** > **PassiveID** > **Providers** and then choose **Active Directory** from the left panel to view all currently configured join points.

Step 7 Click the link for the join point from which you would like to enable the agent you created.

Step 8 Choose the **Passive ID** tab to configure the domain controllers that you added as part of the prerequisites.

Step 9 Select the domain controller that you would like to monitor with the agent you created and click **Edit**.

Step 10 From the **Protocol** drop-down list, select **Agent**

Step 11 Select the agent you created from the **Agent** drop-down list. Enter the user name and password credentials of the agent that you created, and click **Save**.

The user name and password credentials are used to install the agent on the domain controller. Finally, when you click on **Deploy**, the *picagent.exe* is copied from */opt/pbis/bin* to the specified Windows machine.

Manually Install and Deploy Active Directory Agents

When configuring the Agent provider to monitor domain controllers for user identities, the agent must be installed on either a member server or on a domain controller. The agents can be either automatically installed by ISE, or you can manually install them. After installation, automatic or manual, you must then configure the installed agent to monitor specified domain controllers rather than the default WMI. This process describes how to manually install and configure the agent to monitor a domain controller.

Before you begin

Before you begin:

- Configure reverse lookup for the relevant DNS servers from the server side. For more information about the DNS server configuration requirements for ISE, see DNS Server, on page 20
- Ensure Microsoft .NET Framework is updated for the machine designated for the agents, to a minimum of version 4.0. For more information about the .NET framework, see https://www.microsoft.com/net/framework.
- Active Passive ID and pxGrid services. For more information, see Initial Setup and Configuration, on page 54.
- Create an AD join point and add at least one domain controller. For more information about creating join points, see Active Directory as a Probe and a Provider, on page 55.

Use AD user groups for the AD, Agents, SPAN and Syslog probes. For more information about AD groups, see Configure Active Directory User Groups, on page 26.

Step 1 Choose **Work Centers** > **PassiveID** > **Providers** and then choose **Agents** from the left panel.

Step 2 Click **Download Agent** to download the **`picagent-installer.zip`** file for manual installation.
The file is downloaded to your standard Windows Download folder.

Step 3 Place the zip file on the designated host machine and run the installation.

Step 4 From the ISE GUI, again choose **Work Centers** > **PassiveID** > **Providers** and then choose **Agents** from the left panel.

Step 5 To configure a new agent, click **Add** from the top of the table.

Step 6 To configure the agent that you have already installed on the host machine, select **Register Existing Agent**.

Step 7 Complete all mandatory fields in order to configure the client correctly. For more information, see Active Directory Agent Settings, on page 66.

Step 8 Click **Save**.
The agent settings are saved. The agent now also appears in the Agents table and can be applied to monitor specified domain controllers, as described in the following steps.

Step 9 Choose **Work Centers** > **PassiveID** > **Providers** and then choose **Active Directory** from the left panel to view all currently configured join points.

Step 10 Click the link for the join point from which you would like to enable the agent you created.

Step 11 Choose the **Passive ID** tab to configure the domain controllers that you added as part of the prerequisites.

Step 12 Select the domain controller that you would like to monitor with the agent you created and click **Edit**.

Step 13 From the **Protocol** drop-down list, select **Agent**.

Step 14 Select the agent you created from the **Agent** drop-down list. Enter the user name and password to connect to the agent, and click **Save**

The user account must have the necessary permissions to read security events. A user account for a WMI-based agent must have WMI/DCOM permissions.

Uninstall the Agent

Agents, installed automatically or manually, can be easily (manually) uninstalled directly from Windows.

Step 1 From the Windows dialog, go to **Programs and Features**.

Step 2 Find and select the Cisco ISE PassiveID Agent in the list of installed programs.

Step 3 Click **Uninstall**.

Active Directory Agent Settings

Allow ISE to automatically install agents on a specified host in the network in order to retrieve user identity information from different Domain Controllers (DC) and deliver that information to Passive Identity service subscribers.

To create and manage agents, choose **Providers** > **Agents**. See Automatically Install and Deploy Active Directory Agents, on page 64.

Table 10: Agents Window

Field Name	Description
Name	The agent name as you configured it.
Host	The fully qualified domain name of the host on which the agent is installed.
Monitoring	This is a comma separated list of domain controllers that the specified agent is monitoring.

Table 11: Agents New

Field	Description
Deploy New Agent or Register Existing Agent	• Deploy New Agent: Install a new agent on the specified host. • Register Existing Agent: Manually install the agent on the host and then configure that agent from this screen for Passive Identity service to enable the service.
Name	Enter a name by which you can easily recognize the agent.
Description	Enter a description by which you can easily recognize the agent.
Host FQDN	This is the fully qualified domain name for the host on which the agent is installed (register existing agent), or is to be installed (automatic deployment).
User Name	Enter your user name in order to access the host on which to install the agent. Passive Identity service uses these credentials in order to install the agent for you. The user account must have permissions to connect remotely and install the PIC agent.
Password	Enter your user password in order to access the host on which to install the agent. Passive Identity service uses these credentials in order to install the agent for you.

API Providers

The API Providers feature in Cisco ISE enables you to push user identity information from your customized program or from the terminal server (TS)-Agent to the built-in ISE passive identity services REST API service. In this way, you can customize a programmable client from your network to send user identities that were collected from any network access control (NAC) system to the service. Furthermore, the Cisco ISE API

provider enables you to interface with network applications such as the TS-Agent on a Citrix server, where all users have the same IP address but are assigned unique ports.

For example, an agent running on a Citrix server that provides identity mappings for users authenticated against an Active Directory (AD) server can send REST requests to ISE to add or delete a user session whenever a new user logs in or off. ISE then takes the user identity information, including the IP address and assigned ports, delivered from the client and sends it to pre-configured subscribers, such as the Cisco Firepower Management Center (FMC).

The ISE REST API framework implements the REST service over the HTTPS protocol (no client certificate validation necessary) and the user identity information is delivered in JSON (JavaScript Object Notation) format. For more information about JSON, see http://www.json.org/ .

The ISE REST API service parses user identities and in addition, maps that information to port ranges, in order to distinguish between the different users logged in simultaneously to one system. Everytime a port is allocated to a user, the API sends a message to ISE.

The REST API Provider Flow

After you have configured a bridge to your customized client from ISE by declaring that client as a Provider for ISE and enabling that specific customized program (the client) to send RESTful requests, the ISE REST service works in the following way:

1. For client authentication, Cisco ISE requires an authentication token. A customized program on the client machine sends a request for an authentication token when initiating contact and then every time ISE notifies that the previous token has expired. The token is returned in response to the request, enabling ongoing communication between the client, and the ISE service.
2. After a user has logged into the network, the client retrieves user identity information and posts that information to the ISE REST service using the API Add command.
3. Cisco ISE receives and maps the user identity information.
4. Cisco ISE sends the mapped user identity information to the subscriber.
5. Whenever necessary, the customized machine can send a request to remove user information by sending a Remove API call and including the user ID received as the response when the Add call was sent.

Work with REST API Providers in ISE

Follow these steps to activate the REST service in ISE:

1. Configure the client side. For more information, see the client user documentation.
2. Activate Passive ID and pxGrid services. For more information, see Initial Setup and Configuration, on page 54.
3. Ensure you have properly configured the DNS server, including configuring reverse lookup for the client machine from ISE. For more information about the DNS server configuration requirements for , see DNS Server, on page 20
4. See Configure a Bridge to the ISE REST Service for Passive Identity Services, on page 69.

Note To configure the API Provider to work with a TS-Agent add the TS-Agent information when creating a bridge from ISE to that agent, and then consult with the TS-Agent documentation for information about sending API calls.

5. Generate an authentication token and send add and remove requests to the API service.

Configure a Bridge to the ISE REST Service for Passive Identity Services

In order to enable the ISE REST API service to receive information from a specific client, you must first define the specific client from Cisco ISE. You can define multiple REST API clients with different IP addresses.

Before you begin

Before you begin:

- Ensure you have activated Passive ID and pxGrid services. For more information, see Initial Setup and Configuration, on page 54.
- Ensure you have properly configured the DNS server, including configuring reverse lookup for the client machine from Cisco ISE. For more information about the DNS server configuration requirements for Cisco ISE, see DNS Server, on page 20

Step 1 Choose **Work Centers** > **PassiveID** > **Providers** and then choose **API Providers** from the left panel
The API Providers table is displayed, including status information for each existing client.

Step 2 To add a new client, click **Add** from the top of the table.

Step 3 Complete all mandatory fields in order to configure the client correctly. For more information, see API Provider Settings, on page 70.

Step 4 Click **Submit**.
The client configuration is saved and the screen displays the updated API Providers table. The client can now send posts to the ISE REST service.

What to do next

Set up your customized client to post authentication tokens and user identities to the ISE REST service. See Send API Calls to the Passive ID REST Service, on page 69.

Send API Calls to the Passive ID REST Service

Before you begin

Configure a Bridge to the ISE REST Service for Passive Identity Services, on page 69

Step 1 Enter the Cisco ISE URL in the address bar of your browser (for example, *https://<ise hostname or ip address>/admin/*)

Step 2 Enter the username and password that you specified and configured from the **API Providers** window. For more information, see Configure a Bridge to the ISE REST Service for Passive Identity Services, on page 69.

Step 3 Press **Enter**.

Step 4 Enter the API call in the URL Address field of the target node.

Step 5 Click **Send** to issue the API call.

What to do next

See API Calls, on page 70 for more information and details about the different API calls, their schemas and their results.

API Provider Settings

Note The full API definition and object schemas can be retrieved with a request call as follows:

- For the full API specifications (wadl)—https://YOUR_ISE:9094/application.wadl
- For the API model and object schemas—https://YOUR_ISE:9094/application.wadl/xsd0.xsd

Table 12: API Providers Settings

Field	Description
Name	Enter a unique name for this client that distinguishes it quickly and easily from other clients.
Description	Enter a clear description of this client.
Status	Select **Enabled** to enable the client to interact with the REST services immediately upon completing configuration.
Host/ IP	Enter the IP address for the client host machine. Ensure you have properly configured the DNS server, including configuring reverse lookup for the client machine from ISE.
User name	Create a unique user name to be used when posting to the REST service.
Password	Create a unique password to be used when posting to the REST service.

API Calls

Use these API calls to manage user identity events for Passive Identity services with Cisco ISE.

Purpose: Generate Authentication Token

- **Request**

POST

https://<PIC IP address>:9094/api/fmi_platform/v1/identityauth/generatetoken

The request should contain the BasicAuth authorization header. Provide the API provider's credentials as previously created from the ISE-PIC GUI. For more information see API Provider Settings, on page 70.

- **Response Header**

  The header includes the X-auth-access-token. This is the token to be used when posting additional REST requests.

- **Response Body**

  HTTP 204 No Content

Purpose: Add User

- **Request**

  POST

  https://<PIC IP address>:9094/api/identity/v1/identity/useridentity

  Add X-auth-access-token in the header of the POST request, for example, Header: X-auth-access-token, Value: f3f25d81-3ac5-43ee-bbfb-20955643f6a7

- **Response Header**

  201 Created

- **Response Body**

  {

  "user": "<username>",

  "srcPatRange": {

  "userPatStart": <user PAT start value>,

  "userPatEnd": <user PAT end value>,

  "patRangeStart": <PAT range start value>

  },

  "srcIpAddress": "<src IP address>",

  "agentInfo": "<Agent name>",

  "timestamp": "<ISO_8601 format i.e. “YYYY-MM-DDTHH:MM:SSZ" >",

  "domain": "<domain>"

  }

- **Notes**

  - srcPatRange can be removed in above json to create a single IP user binding.
  - Response body contains the "ID" which is the unique identifier for the user session binding created. Use this ID when sending a DELETE request to indicate which user should be removed.

- This reponse also contains the self link which is the URL for this newly created user session binding.

Purpose: Remove User

- **Request**

  DELETE

  https://<PIC IP address>:9094/api/identity/v1/identity/useridentity/<id>

  In <id> enter the ID as was received from the Add response.

  Add the X-auth-access-token in the header of the DELETE request, for example, Header: X-auth-access-token, Value: f3f25d81-3ac5-43ee-bbfb-20955643f6a7

- **Response Header**

  200 OK

- **Response Body**

  Response body contains the details about the user session binding which got deleted.

SPAN

SPAN is a Passive Identity service that allows you to quickly and easily enable Cisco ISE to listen to the network and retrieve user information without having to configure Active Directory to work directly with Cisco ISE. SPAN sniffs network traffic, specifically examining Kerberos messages, extracts user identity information also stored by Active Directory and sends that information to ISE. ISE then parses the information, ultimately delivering user name, IP address and domain name to the subscribers that you have also already configured from ISE.

In order for SPAN to listen to the network and extract Active Directory user information, ISE and Active Directory must both be connected to the same switch on the network. In this way, SPAN can copy and mirror all user identity data from Active Directory.

With SPAN, user information is retrieved in the following way:

1. The user endpoint logs in to the network.
2. Log in and user data are stored in Kerberos messages.
3. When the user logs in and the user data passes through the switch, SPAN mirrors the network data.
4. Cisco ISE listens to the network for user information and retrieves the mirrored data from the switch.
5. Cisco ISE parses the user information and updates passive ID mappings.
6. Cisco ISE delivers the parsed user information to the subscribers.

Working with SPAN

Before you begin

In order to enable ISE to receive SPAN traffic from a network switch, you must first define which nodes and node interfaces are to listen to the switch. You can configure SPAN in order to listen to the different installed

ISE nodes. For each node, only one interface can be configured to listen to the network and the interface used to listen must be dedicated to SPAN only.

Before you begin, ensure you have activated Passive ID and pxGrid services. Only nodes for which Passive ID has been turned on will appear in the list of available interfaces for configuring SPAN. For more information, see Initial Setup and Configuration, on page 54.

In addition, you must:

- Ensure Active Directory is configured on your network.
- Run a CLI on the switch in the network that is also connected to Active Directory in order to ensure the switch can communicate with ISE.
- Configure the switch to mirror the network from AD.
- Configure a dedicated ISE network interface card (NIC) for SPAN. This NIC is used only for SPAN traffic.
- Ensure the NIC that you have dedicated to SPAN is activated via the command line interface.
- Create a VACL that sends only Kerberos traffic into the SPAN port.

Step 1 Choose **Work Centers** > **PassiveID** > **Providers** and then choose **SPAN** from the left panel to configure SPAN.

Step 2 **Note** We recommend that the GigabitEthernet0 network interface card (NIC) remain available and that you select any other available NIC for configuring SPAN. GigabitEthernet0 is used for system management purposes.

Enter a meaningful description (optional), select status **Enabled**, and choose the nodes and the relevant NICs that will be used to listen to the network switch. For more information, see SPAN Settings, on page 73.

Step 3 Click **Save**.
The SPAN configuration is saved and ISE-PIC ISE is now actively listening to network traffic.

SPAN Settings

From each node that you have deployed, quickly and easily configure ISE to receive user identities by installing SPAN on a client network.

Table 13: SPAN Settings

Field	Description
Description	Enter a unique description to remind you of which nodes and interfaces are currently enabled.
Status	Select **Enabled** to enable the client immediately upon completing configuration.

Field	Description
Interface NIC	Select one or more of the nodes installed for ISE, and then for each selected node, choose the node interface that is to listen to the network for information. **Note** We recommend that the GigabitEthernet0 NIC remain available and that you select any other available NIC for configuring SPAN. GigabitEthernet0 is used for system management purposes.

Syslog Providers

Passive Identity service parses syslog messages from any client (identity data provider) that delivers syslog messages, including regular syslog messages (from providers such as InfoBlox, Blue Coat, BlueCat, and Lucent) as well as DHCP syslog messages, and sends back user identity information, including MAC addresses. This mapped user identity data is then delivered to subscribers.

You can specify the syslog clients from which to receive the user identity data (see Configure Syslog Clients, on page 75). While configuring the provider, you must specify the connection method (TCP or UDP) and the syslog template to be used for parsing.

Note When TCP is the configured connection type, if there is a problem with the message header and the host name cannot be parsed, ISE attempts to match the IP address received in the packet to the IP address of any of the providers in the list of providers that have already been configured for Syslog messages in ISE. To view this list, choose **Work Centers** > **PassiveID** > **Providers** > **Syslog Providers**. We recommend that you check the message headers and customize if necessary to guarantee parsing succeeds. For more information about customizing headers, see Customize Syslog Headers, on page 81.

The syslog probe sends syslog messages that are received to the ISE parser, which maps the user identity information, and publishes that information to ISE. ISE then delivers the parsed and mapped user identity information to the Passive Identity service subscribers.

To parse syslog messages for user identity from ISE-PIC ISE:

- Configure syslog clients from which to receive user identity data. See Configure Syslog Clients, on page 75.
- Customize a single message header. See Customize Syslog Headers, on page 81.
- Customize message bodies by creating templates. See Customize the Syslog Message Body, on page 80.
- Use the message templates pre-defined in ISE when configuring your syslog client as the message template used for parsing, or base your customized header or body templates on these pre-defined templates. See Work with Syslog Predefined Message Templates, on page 84.

Configure Syslog Clients

In order to enable Cisco ISE to listen to syslog messages from a specific client, you must first define the specific client from Cisco ISE. You can define multiple providers with different IP addresses.

Before you begin

Before you begin, ensure you have activated Passive ID and pxGrid services. For more information, see Initial Setup and Configuration, on page 54.

Step 1 Choose **Work Centers** > **PassiveID** > **Providers** and then choose **Syslog Providers** from the left panel. The Syslog Providers table is displayed, including status information for each existing client.

Step 2 To configure a new syslog client, click **Add** from the top of the table.

Step 3 Complete all mandatory fields (see Syslog Settings, on page 75 for more details) and create a message template if necessary (see Customize the Syslog Message Body, on page 80 for more details) to configure the client correctly.

Step 4 Click **Submit**.

Syslog Settings

Configure Cisco ISE to receive user identities, including MAC addresses, by way of syslog messages from a specific client. You can define multiple providers with different IP addresses.

Table 14: Syslog Providers

Field Name	Description
Name	Enter a unique name that distinguishes this configured client quickly and easily.
Description	A meaningful description of this Syslog provider.
Status	Select **Enabled** to enable the client immediately upon completing configuration.
Host	Enter the FQDN of the host machine.

Field Name	Description
Connection Type	Enter UDP or TCP to indicate the channel by which ISE listens for syslog messages. **Note** When TCP is the configured connection type, if there is a problem with the message header and the host name cannot be parsed, then Cisco ISE attempts to match the IP address received in the packet to the IP address of any of the providers in the list of providers that have already been configured for Syslog messages in Cisco ISE. To view this list, choose **Work Centers** > **PassiveID** > **Providers** > **Syslog Providers**. We recommend that you check the message headers and customize if necessary to ensure that parsing succeeds. For more information about customizing headers, see Customize Syslog Headers, on page 81.

Field Name	Description
Template	

Field Name	Description
	A template indicates precise body message structure so that the parser can identify the pieces of information within the syslog message that should be parsed, mapped and delivered. For example, a template can indicate the exact position of the user name so that the parser can find the user name in every message received. From this field, indicate the template (for the body of the syslog message) to be used in order to recognize and correctly parse the syslog message. Choose either from the pre-defined dropdown list, or click **New** to create your own customized template. For more information about creating new templates, see Customize the Syslog Message Body, on page 80. Most of the pre-defined templates use regular expressions, and customized templates should also use regular expressions. **Note** Only customized templates can be edited or removed, while pre-defined system templates in the dropdown cannot be altered. ISE currently offers these pre-defined DHCP provider templates: • InfoBlox • BlueCat • Lucent_QIP • DHCPD • MSAD DHCP **Note** DHCP syslog messages do not contain user names. Therefore, these messages are delivered from the parser with a delay so that Cisco ISE can first check users registered in the local session directory (displayed from Live Sessionss) and attempt to match those users by their IP addresses to the IP addresses listed in the DHCP syslog messages received, in order to correctly parse and deliver user identity information. If the data received from a DHCP syslog message cannot be matched to any of the currently logged in users, then the message

Field Name	Description
	is not parsed and user identity is not delivered. Cisco ISE offers these pre-defined regular syslog provider templates: • ISE • ACS • F5_VPN • ASA_VPN • Blue Coat • Aerohive • Safe connect_NAC • Nortel_VPN For information about templates, see Work with Syslog Predefined Message Templates, on page 84.
Default Domain	If the domain is not identified in the syslog message for the specific user, this default domain is automatically assigned to the user in order to ensure that all users are assigned a domain. With the default domain or with the domain that was parsed from the message, the user name is appended to username@domain, thereby including that domain, in order to get more information about the user and user groups.

Customize Syslog Message Structures (Templates)

A template indicates precise message structure so that the parser can identify the pieces of information within the syslog message that should be parsed, mapped and delivered. For example, a template can indicate the exact position of the user name so that the parser can find the user name in every message received. Templates determine the supported structures for both new and remove mapping messages.

Cisco ISE enables you to customize a single message header and multiple body structures, to be used by the Passive ID parser.

The templates should include regular expressions to define the structure for user name, IP address, MAC address and domain in order to enable the Passive ID parser to correctly identify whether the message is to add or remove user identity mapping and to correctly parse the user details.

When customizing your message templates, you can choose to base your customization on the message templates pre-defined in ISE-PIC ISE by consulting with the regular expressions and message structures used within those pre-defined options. For more information about the pre-defined template regular expressions, message structures, examples and more, see Work with Syslog Predefined Message Templates, on page 84.

You can customize:

- A single message header—Customize Syslog Headers, on page 81
- Multiple message bodies—Customize the Syslog Message Body, on page 80.

Note DHCP syslog messages do not contain user names. Therefore, these messages are delivered from the parser with a delay so that Cisco ISE can first check users registered in the local session directory (displayed from Live Sessionss) and attempt to match those users by their IP addresses to the IP addresses listed in the DHCP syslog messages received, in order to correctly parse and deliver user identity information. If the data received from a DHCP syslog message cannot be matched to any of the currently logged in users, then the message is not parsed and user identity is not delivered.

The delay necessary to properly match, parse and map details from DHCP messages cannot be applied to customized templates, and therefore it is not recommended that DHCP message templates be customized. Instead, use any of the pre-defined DHCP templates.

Customize the Syslog Message Body

Cisco ISE enables you to customize your own syslog message templates (by customizing the message body) to be parsed by the Passive ID parser. The templates should include regular expressions to define the structure for user name, IP address, MAC address and domain.

Note DHCP syslog messages do not contain user names. Therefore, these messages are delivered from the parser with a delay so that Cisco ISE can first check users registered in the local session directory (displayed from Live Sessionss) and attempt to match those users by their IP addresses to the IP addresses listed in the DHCP syslog messages received, to correctly parse and deliver user identity information. If the data received from a DHCP syslog message cannot be matched to any of the currently logged in users, then the message is not parsed and user identity is not delivered.

The delay necessary to properly match, parse and map details from DHCP messages cannot be applied to customized templates, and therefore it is not recommended that DHCP message templates be customized. Instead, use any of the pre-defined DHCP templates.

Create and edit syslog message body templates from within the syslog client configuration screen.

Note You can only edit your own customized templates. Pre-defined templates offered by the system cannot be changed.

Step 1 Choose **Work Centers** > **PassiveID** > **Providers** and then choose **Syslog Providers** from the left panel. The Syslog Providers table is displayed, including status information for each existing client.

Step 2 Click **Add** to add a new syslog client or **Edit** to update an already configured client. For more information about configuring and updating syslog clients, see Configure Syslog Clients, on page 75.

Step 3 In the **Syslog Providers** window, click **New** to create a new message template. To edit an existing template, select the template from the dropdown list and click **Edit**.

Step 4 Complete all mandatory fields.

For information about how to enter the values correctly, see Syslog Customized Template Settings and Examples, on page 82.

Step 5 Click **Test** to ensure the message is correctly parsed based on the strings you have entered.

Step 6 Click **Save**.

Customize Syslog Headers

Syslog headers also contain the host name from which the message originated. If your syslog messages are not recognized by the Cisco ISE message parser, you may need to customize the message header by configuring the delimiter that proceeds the host name, thereby enabling Cisco ISE to recognize the host name and parse the message correctly. For more details about the fields in this screen, see Syslog Customized Template Settings and Examples, on page 82. The customized header configuration is saved and added to the header types that are used by the parser whenever messages are received.

Note You can only customize a single header. After you customize a header, when you click **Custom Header** and create a template, only the newest configuration is saved.

Step 1 Choose **Work Centers** > **PassiveID** > **Providers** and then choose **Syslog Providers** from the left panel.
The Syslog Providers table is displayed, including status information for each existing client.

Step 2 Click **Custom Header** to open the Syslog Custom Header screen.

Step 3 In the **Paste sample syslog** field, enter an example of the header format in your syslog messages. For example, copy and paste this header from one of your messages: `<181>Oct 10 15:14:08 Cisco.com`.

Step 4 In the **Separator** field, indicate whether words are separated by spaces or tabs.

Step 5 In the **Position of hostname in header** field, indicate which place in the header is the host name. For example, in the header offered above, the host name is the fourth word in the header. Enter 4 to indicate this.

The **Hostname** field displays the host name based on the details indicated in the first three fields. For example, if the header example in **Paste sample syslog** is as follows:

<181>Oct 10 15:14:08 Cisco.com

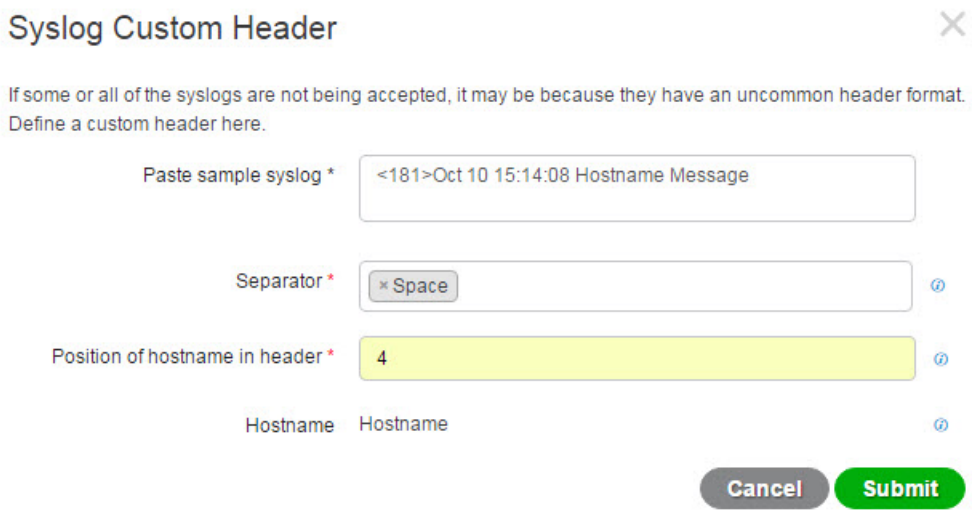
The separator is indicated as **Space** and the **Position of hostname in header** is entered as 4.

The **Hostname** will automatically appear as Cisco.com, which is the fourth word in the header phrase pasted in the **Paste sample syslog** field.

If the host name is incorrectly displayed, check the data you have entered in the **Separator** and **Position of hostname in header** fields.

This example is as in the following screen capture:

Figure 14: Customize Syslog Headers



Step 6 Click **Submit**.
The customized header configuration is saved and added to the header types that are used by the parser whenever messages are received.

Syslog Customized Template Settings and Examples

Cisco ISE enables you to customize your own syslog message templates to be parsed by the Passive ID parser. Customized templates determine the supported structures for both new and remove mapping messages. The templates should include regular expressions to define the structure for user name, IP address, MAC address and domain in order to enable the Passive ID parser to correctly identify whether the message is to add or remove user identity mapping and to correctly parse the user details.

Note Most of the pre-defined templates use regular expressions. Customized templates should also use regular expressions.

Syslog Header Parts

You can customize a single header that is recognized by the Syslog probe by configuring the delimiter that proceeds the host name.

The following table describes the different parts and fields that can be included in your customized syslog header. For more information about regular expressions, see Table 17: Regular Expressions for Customized Templates, on page 84.

Table 15: Syslog Custom Header

Field	Description
Paste sample syslog	Enter an example of the header format in your syslog messages. For example, copy and paste this header: `<181>Oct 10 15:14:08 Hostname Message`
Separator	Indicate whether words are separated by spaces or tabs.
Position of hostname in header	Indicate which place in the header is the host name. For example, in the header offered above, the host name is the fourth word in the header. Enter 4 to indicate this.
Hostname	Displays the hostname based on the details indicated in the first three fields. For example, if the header example in **Paste sample syslog** is as follows: <181>Oct 10 15:14:08 Hostname Message The separator is indicated as **Space** and the **Position of hostname in header** is entered as 4. The **Hostname** will automatically appear as Hostname. If the host name is incorrectly displayed, check the data you have entered in the **Separator** and **Position of hostname in header** fields.

Syslog Template Parts and Descriptions for the Message Body

The following table describes the different parts and fields that can be included in your customized syslog message templates. For more information about regular expressions, see Table 17: Regular Expressions for Customized Templates, on page 84.

Table 16: Syslog Template

Part	Field	Description
	Name	A unique name by which to recognize the purpose of this template.
Mapping Operations	New Mapping	A regular expression that describes the kind of mapping used with this template to add For example, enter "logged on from" in this field to indicate a new user that has logge F5 VPN.
	Removed Mapping	A regular expression that describes the kind of mapping used with this template to rem For example, enter "session disconnect" in this field to indicate a user that should be r ASA VPN.

Part	Field	Description
User Data	IP Address	A regular expression that indicates the IP addresses to be captured. For example, for Bluecat messages, to capture identities for users within this IP address ra enter: (on\s|to\s)((?:(?:25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.){3}(?:25[0-5]|2[0-4][0-9]|[01]?[0-9
	User Name	A regular expression that indicates the user name format to be captured.
	Domain	A regular expression that indicates the domain to be captured.
	Mac Address	A regular expression that indicates the MAC address format to be captured.

Regular Expression Examples

In order to parse messages use regular expressions. This sections offers regular expression examples in order to parse IP address, user name and add mapping messages.

For example, use regular expressions to parse the following messages:

<174>192.168.0.1 %ASA-4-722051: Group <DfltGrpPolicy> User <user1> IP <192.168.0.10> IPv4 Address <192.168.0.6> IPv6 address <::> assigned to session

<174>192.168.0.1 %ASA-6-713228: Group = xyz, Username = user1, IP = 192.168.0.12, Assigned private IP address 192.168.0.8 to remote user

The regular expressions are as defined in the following table.

Table 17: Regular Expressions for Customized Templates

Part	Regular Expression
IP address	Address <([^\s]+)>|address ([^\s]+)
User name	User <([^\s]+)>| Username = ([^\s]+)
Add mapping message	(%ASA-4-722051|%ASA-6-713228)

Work with Syslog Predefined Message Templates

Syslog messages have a standard structure which include a header and the message body.

The predefined templates offered by Cisco ISE are described in this section, including content details for the headers that are supported, as well as the supported body structure, based on the origin of the messages.

In addition, you can create your own templates with customized body content for sources that are not predefined in the system. The supported structure for customized templates is also described in this section. You can configure a single customized header to be used in addition to the headers predefined in the system, when parsing messages, and you can configure multiple customized templates for the message body. For more information about customizing the header, see Customize Syslog Headers, on page 81. For more information about customizing the body, see Customize the Syslog Message Body, on page 80.

Note Most of the predefined templates use regular expressions, and customized templates should also use regular expressions.

Message Headers

There are two header types recognized by the parser, for all message types (new and remove), for all client machines. These headers are as follows:

- <171>Host message
- <171>Oct 10 15:14:08 Host message

Once received, the header is parsed for host name, which can be IP address, hostname, or full FQDN.

Headers can also be customized. To customize your headers, see Customize Syslog Headers, on page 81.

Syslog ASA VPN Pre-Defined Template

The supported syslog message format and types for ASA VPN are as described below.

Headers

Headers supported by the parser are identical for all clients, as described in Work with Syslog Predefined Message Templates, on page 84.

New Mapping Body Messages

There are different ASA VPN body messages that are recognized by the parser as described in the following table.

Body Message	Parsing Example
%ASA-6-109005 Authentication succeeded for user UserA from 10.0.0.11/100 to 10.10.11.11/20 on interface eth1/1	[UserA,10.0.0.11]
%ASA-6-602303 IPSEC: An direction tunnel_type SA (SPI=spi) between local_IP and 10.0.0.11 (UserA) has been created.	
%ASA-6-721016 (device) WebVPN session for client user UserA, IP 10.0.0.11 has been created.	
%ASA-6-603104 PPTP Tunnel created, tunnel_id is number, remote_peer_ip is remote_address, ppp_virtual_interface_id is number,\ client_dynamic_ip is 10.0.0.11,ffg123 #% UserA is UserA, MPPE_key_strength is string	
%ASA-6-603106 L2TP Tunnel created, tunnel_id is number, remote_peer_ip is remote_address, ppp_virtual_interface_id is number,\ client_dynamic_ip is 10.0.0.11, UserA is user	
%ASA-6-113039 Group group User UserA IP 10.0.0.11 AnyConnect parent session started.	
%ASA-6-802001 User UserA IP 10.100.1.1 OS os_name UDID number MDM action session started.	
%ASA-6-713228: Group = xyz, UserA = xxxx227, IP = 192.168.0.11, Assigned private IP address 172.16.0.11 to remote user	[UserA,172.16.0.11] **Note** The parsed IP address from this message type is the private IP address, as indicated in the message.
%ASA-4-722051: Group <DfltGrpPolicy> User <UserA> IP <172.16.0.12> IPv4 Address <172.16.0.21> IPv6 address <::> assigned to session	[UserA,172.16.0.12] **Note** The parsed IP address from this message type is the IPv4 address.

Remove Mapping Body Messages

The Remove Mapping messages supported for ASA VPN by the parser are as described in this section.

Once received, the body is parsed for user details as follows:

[UserA,10.1.1.1]

Body Message
%ASA-4-113019 Group = group, UserA = UserA, IP = 10.1.1.1, Session disconnected. Session Type: type, Duration:\ duration, Bytes xmt: count,Bytes rcv: count, Reason: reason

Body Message
%ASA-4-717052 Group group name User UserA IP 10.1.1.1 Session disconnected due to periodic certificate authentication failure. Subject Name id subject name Issuer Name id issuer name\ Serial Number id serial number
%ASA-6-602304 IPSEC: An direction tunnel_type SA (SPI=spi) between local_IP and 10.1.1.1 (UserA) has been deleted.
%ASA-6-721018 WebVPN session for client user UserA, IP 10.1.1.1 has been deleted.
%ASA-4-722049 Group group User UserA IP 10.1.1.1 Session terminated: SVC not enabled or invalid image on the ASA
%ASA-4-722050 Group group User UserA IP 10.1.1.1 Session terminated: SVC not enabled for the user.
%ASA-6-802002 User UserA IP 10.1.1.1 OS os_name UDID number MDM action session terminated.
%ASA-3-716057 Group group User UserA IP 10.1.1.1 Session terminated, no type license available.
%ASA-3-722046 Group group User UserA IP 10.1.1.1 Session terminated: unable to establish tunnel.
%ASA-4-113035 Group group User UserA IP 10.1.1.1 Session terminated: AnyConnect not enabled or invalid AnyConnect image on the ASA.
%ASA-4-716052 Group group-name User UserA IP 10.1.1.1 Pending session terminated.
%ASA-6-721018 WebVPN session for client user UserA, IP 10.1.1.1 has been deleted.

Syslog Bluecat Pre-Defined Template

The supported syslog message format and types for Bluecat are as described below.

Headers

Headers supported by the parser are identical for all clients, as described in Work with Syslog Predefined Message Templates, on page 84.

New Mapping Body Messages

The messages supported for New Mapping for Bluecat syslog are as described in this section.

Once received, the body is parsed for user details as follows:

[macAddress=nn:xx:nn:ca:xx:nn,ip=172.16.0.12]

Body
Nov 7 23:37:32 xx-campus1 dhcpd: DHCPACK on 172.16.0.13 to nn:xx:nn:ca:xx:nn via 172.16.0.17

Remove Mapping Messages

There are no remove mapping messages known for Bluecat.

Syslog F5 VPN Pre-Defined Template

The supported syslog message format and types for F5 VPN are as described below.

Headers

Headers supported by the parser are identical for all clients, as described in Work with Syslog Predefined Message Templates, on page 84.

New Mapping Body Messages

There are different F5 VPN body messages that are recognized by the parser as described in the following table.

Once received, the body is parsed for user details as follows:

[user=UserA,ip=172.16.0.12]

Body
Apr 10 09:33:58 Oct 2 08:28:32 abc.xyz.org security[nnnnn]: [UserA@vendor-abcr] User UserA logged on from 172.16.0.21 to \ 172.16.0.12 Sid = xyz\

Remove Mapping Messages

Currently there are no remove messages for F5 VPN that are supported.

Syslog Infoblox Pre-Defined Template

The supported syslog message format and types for Infoblox are as described below.

Headers

Headers supported by the parser are identical for all clients, as described in Work with Syslog Predefined Message Templates, on page 84.

New Mapping Body Messages

There are different ASA VPN body messages that are recognized by the parser as described in the following table.

Once received, the body is parsed for user details as follows:

[macAddress= nn:xx:xx:xx:nn:nn,ip=10.0.10.100]

Body Message
Nov 15 11:37:26 user1-lnx dhcpd[3179]: DHCPACK on 10.0.0.14 to nn:xx:xx:nx:nn:nn (android-df67ddcbb1271593) via eth2 relay 10.0.0.24 lease-duration 3600
Nov 15 11:38:11 user1-lnx dhcpd[3179]: DHCPACK on 172.16.0.18 to nn:xx:xx:xn:nn:nn (DESKTOP-HUDGAAQ) via eth2 relay 172.16.0.13 lease-duration 691200 (RENEW)
Nov 15 11:38:11 192.168.0.12 dhcpd[25595]: DHCPACK to 10.0.0.11 (nn:xx:xx:xn:nn:nx) via eth1

Remove Mapping Messages

Once received, the body is parsed for user details as follows:

- If MAC address is included:

  [00:0c:29:a2:18:34,10.0.10.100]

- If MAC address is not included:

  [10.0.10.100]

Body Message
07-11-2016 23:37:32 Daemon.Info 10.0.10.2 Jul 12 10:42:26 10.0.10.2 dhcpd[26083]: DHCPEXPIRE 10.0.10.100 has expired
07-11-2016 23:37:32 Daemon.Info 10.0.10.2 Jul 12 10:42:26 10.0.10.2 dhcpd[26083]: DHCPRELEASE of 10.0.10.100 from 00:0c:29:a2:18:34 \ (win10) via eth1 uid 01:00:0c:29:a2:18:34
07-11-2016 23:37:32 Daemon.Info 10.0.10.2 Jul 12 10:42:26 10.0.10.2 dhcpd[25595]: RELEASE on 10.20.31.172 to c0:ce:cd:44:4f:bd

Syslog Linux DHCPd3 Pre-Defined Template

The supported syslog message format and types for Linux DHCPd3 are as described below.

Headers

Headers supported by the parser are identical for all clients, as described in Work with Syslog Predefined Message Templates, on page 84.

New Mapping Messages

There are different Linux DHCPd3 body messages that are recognized by the parser as described in the following table.

Once received, the body is parsed for user details as follows:

[macAddress=24:ab:81:ca:f2:72,ip=172.16.0.21]

Body Message
Nov 11 23:37:32 dhcpsrv dhcpd: DHCPACK on 10.0.10.100 to 00:0c:29:a2:18:34 (win10) via eth1
Nov 11 23:37:32 dhcpsrv dhcpd: DHCPACK on 10.0.10.100 (00:0c:29:a2:18:34) via eth1

Remove Mapping Body Messages

The Remove Mapping messages supported for Linux DHCPd3 by the parser are as described in this section.

Once received, the body is parsed for user details as follows:

[00:0c:29:a2:18:34 ,10.0.10.100]

Body Message
Nov 11 23:37:32 dhcpsrv dhcpd: DHCPEXPIRE 10.0.10.100 has expired

Body Message
Nov 11 23:37:32 dhcpsrv dhcpd: DHCPRELEASE of 10.0.10.100 from 00:0c:29:a2:18:34 (win10) via eth1

Syslog MS DHCP Pre-Defined Template

The supported syslog message format and types for MS DHCP are as described below.

Headers

Headers supported by the parser are identical for all clients, as described in Work with Syslog Predefined Message Templates, on page 84.

New Mapping Body Messages

There are different MS DHCP body messages that are recognized by the parser as described in the following table.

Once received, the parser divides data by searching for the comma (,) and then messages of these formats are parsed as in the following example:

[macAddress=000C29912E5D,ip=10.0.10.123]

Body Message
Nov 11 23:37:32 10,07/21/16,16:55:22,Assign,10.0.10.123,win10.IDCSPAN.Local,000C29912E5D,,724476048,0,,,,0x4D53465420352E30,MSFT,5.0

Remove Mapping Body Messages

The Remove Mapping messages supported for MS DHCP by the parser are as described in this section.

Once received, the parser divides data by searching for the comma (,) and then messages of these formats are parsed as in the following example:

[macAddress=000C29912E5D,ip=10.0.10.123]

Body Message
Nov 11 23:37:32 12,07/21/16,16:55:18,Release,10.0.10.123,win10.IDCSPAN.Local,000C29912E5D,,3128563632,\ 0,,,,,,,,,0

Syslog SafeConnect NAC Pre-Defined Template

The supported syslog message format and types for SafeConnect NAC are as described below.

Headers

Headers supported by the parser are identical for all clients, as described in Work with Syslog Predefined Message Templates, on page 84.

New Mapping Body Messages

There are different SafeConnect NAC body messages that are recognized by the parser as described in the following table.

Once received, the body is parsed for user details as follows:

[user=galindk1i,p=xxxx.xx.xxx.xxd,domain=Resnet-Macs]

Body Message
Apr 10 09:33:58 nac Safe*Connect: authenticationResult|xxx.xx.xxx.xxx|xxx.xx.xxx.xxx|UserA|true|Resnet-Macs|TCNJ-Chain|001b63b79018|MAC

Remove Mapping Messages

Currently there are no remove messages for Safe Connect that are supported.

Syslog Aerohive Pre-Defined Templates

The supported syslog message format and types for Aerohive are as described below.

Headers

Headers supported by the parser are identical for all clients, as described in Work with Syslog Predefined Message Templates, on page 84.

New Mapping Body Messages

There are different Aerohive body messages that are recognized by the parser as described in the following table.

Details parsed from the body include user name and IP address. The regular expression used for parsing is as in the following examples:

- `New mapping—auth\:`
- `IP—ip ([A-F0-9a-f:.]+)`
- `User name—UserA ([a-zA-Z0-9\_]+)`

Once received, the body is parsed for user details as follows:

[UserA,10.5.50.52]

Body Message
2013-04-01 14:06:05 info ah auth: Station 1cab:a7e6:cf7f ip 10.5.50.52 UserA UserA

Remove Mapping Messages

Currently the system does not support remove mapping messages from Aerohive.

Syslog Blue Coat Pre-Defined Templates—Main Proxy, Proxy SG, Squid Web Proxy

The system supports the following message types for Blue Coat:

- BlueCoat Main Proxy
- BlueCoat Proxy SG
- BlueCoat Squid Web Proxy

The supported syslog message format and types for Bluecoat messages are as described below.

Headers

Headers supported by the parser are identical for all clients, as described in Work with Syslog Predefined Message Templates, on page 84.

New Mapping Body Messages

There are different Blue Coat body messages that are recognized by the parser as described in the following table.

Once received, the body is parsed for user details as follows:

[UserA,192.168.10.24]

Body Message (this example is taken from a BlueCoat Proxy SG message)
2016-09-21 23:05:33 58 10.0.0.1 UserA - - PROXIED "none" http://www.example.com/ 200 TCP_MISS GET application/json;charset=UTF-8 http site.api.example.com 80 /apis/v2/scoreboard/header ?rand=1474499133503 - "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/46.0.2486.0 Safari/537.36 Edge/13.10586" 192.168.10.24 7186 708 - "unavailable

The following table describes the different regular expression structures used per client for new mapping messages.

Client	Regular expressions
BlueCoat Main Proxy	New mapping **(TCP_HIT|TCP_MEM){1}** IP **\s((?:[0-9]{1,3}\.){3}[0-9]{1,3}|(?:[a-zA-Z0-9]{1,}:){1,7}[a-zA-Z0-9]{1,})\s** User name **\s\-\s([a-zA-Z0-9_]+)\s\-\s**
BlueCoat Proxy SG	New mapping **(\-\sPROXIED){1}** IP **\s((?:[0-9]{1,3}\.){3}[0-9]{1,3}|(?:[a-zA-Z0-9]{1,}:){1,7}[a-zA-Z0-9]{1,})\s[a-zA-Z0-9_]+\s** User name **\s[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\s([a-zA-Z0-9_]+)\s\-**

Client	Regular expressions
BlueCoat Squid Web Proxy	New mapping **(TCP_HIT|TCP_MEM){1}** IP **\s(?:[0-9]{1,3}\.){3}[0-9]{1,3}(?:[a-zA-Z0-9]{4,12}){7}[a-zA-Z0-9]{4}\sTCP** User name **\s([a-zA-Z0-9\._]+)\s\-**

Remove Mapping Messages

Remove mapping messages are supported for Blue Coat clients, though no examples are currently available.

The following table describes the different known regular expression structure examples used per client for remove mapping messages.

Client	Regular expressions
BlueCoat Main Proxy	**(TCP_MISS|TCP_NC_MISS){1}**
BlueCoat Proxy SG	No example currently available.
BlueCoat Squid Web Proxy	**(TCP_MISS|TCP_NC_MISS){1}**

Syslog ISE and ACS Pre-Defined Templates

When listening to ISE or ACS clients, the parser receives the following message types:

- Pass authentication: When the user is authenticated by ISE or ACS, the pass authentication message is issued notifying that authentication succeeded, and including user details. The message is parsed and the user details and session ID are saved from this message.
- Accounting start and accounting update messages (new mapping): The accounting start or accounting update message is parsed with the user details and session ID that were saved from the Pass Authentication message and then the user is mapped.
- Accounting stop (remove mapping): The user mapping is deleted from the system.

The supported syslog message format and types for ISE and ACS are as described below.

Pass Authentication Messages

The following messages are supported for Pass Authentication.

- **Header**

  ```
  <181>Sep 13 10:51:41 Server logTag messageId totalFragments currentFragments message
  ```

  For example: <181>Sep 13 10:51:41 Positron CISE_PassiveID 0000005255 1 0 message

- **Body**

  Passed-Authentication 000011 1 0 2016-05-09 12:48:11.011 +03:00 0000012435 5200 NOTICE Passed-Authentication: Authentication succeeded, ConfigVersionId=104, Device IP Address=10.0.0.12,

DestinationIPAddress=10.0.0.18, DestinationPort=1812, UserA=UserA, Protocol=Radius, RequestLatency=45, NetworkDeviceName=DefaultNetworkDevice, User-Name=UserA, NAS-IP-Address=10.0.0.1, Session-Timeout=90, Calling-Station-ID=, cisco-av-pair=audit-session-id=5

- **Parsing Example**

  User name and session ID only are parsed.

  [UserA,5]

Accounting Start/Update (New Mapping) Messages

The following messages are supported for New Mapping.

- **Header**

  ```
  <181>Sep 13 10:51:41 Server logTag messageId totalFragments currentFragments message
  ```

  For example: <181>Sep 13 10:51:41 Positron CISE_PassiveID 0000005255 1 0 message

- **Body**

  CISE_RADIUS_Accounting 000011 1 0 2016-05-09 12:53:52.823 +03:00 0000012451 3000 NOTICE Radius-Accounting: RADIUS Accounting start request, ConfigVersionId=104, Device IP Address=10.0.0.12, RequestLatency=12, NetworkDeviceName=DefaultNetworkDevice, User-Name=UserA, NAS-IP-Address=10.0.0.1, Framed-IP-Address=10.0.0.16, Session-Timeout=90, Calling-Station-ID=, Acct-Status-Type=Start, Acct-Session-Id=6, cisco-av-pair=audit-session-id=5

- **Parsing Example**

  Parsed details include user name, and framed IP address, as well as the MAC address if it is included in the message.

  [UserA,10.0.0.16]

Remove Mapping Messages

The following messages are supported for Remove Mapping.

- **Header**

  ```
  <181>Sep 13 10:51:41 Server logTag messageId totalFragments currentFragments message
  ```

  For example: <181>Sep 13 10:51:41 Positron CISE_PassiveID 0000005255 1 0 message

- **Body**

  2016-05-09 12:56:27.274 +03:00 0000012482 3001 NOTICE Radius-Accounting: RADIUS Accounting stop request, ConfigVersionId=104, Device IP Address=10.0.0.17, RequestLatency=13, NetworkDeviceName=DefaultNetworkDevice, User-Name=UserA, NAS-IP-Address=10.0.0.1, Framed-IP-Address=10.0.0.16, Session-Timeout=90, Calling-Station-ID=, Acct-Status-Type=Stop, Acct-Session-Id=104, cisco-av-pair=audit-session-id=5

- **Parsing Example**

  Parsed details include user name, and framed IP address, as well as the MAC address if it is included in the message.

  [UserA,10.0.0.16]

Syslog Lucent QIP Pre-Defined Template

The supported syslog message format and types for Lucent QIP are as described below.

Headers

Headers supported by the parser are identical for all clients, as described in Work with Syslog Predefined Message Templates, on page 84.

New Mapping Body Messages

There are different Lucent QIP body messages that are recognized by the parser as described in the following table.

The regular expression structure for these messages is as follows:

DHCP_GrantLease|:DHCP_RenewLease

Once received, the body is parsed for user details as follows:

[00:0C:29:91:2E:5D,10.0.0.11]

Body Message
DHCP:subtype=0:Single:$IGNORE_N$ DHCP_GrantLease: Host=$HOSTNAME$ P=10.0.0.11 MAC=00:0C:29:91:2E:5D
DHCP:subtype=0:Single:$IGNORE_N$ DHCP_RenewLease: Host=$HOSTNAME$ P=10.0.0.11 MAC=00:0C:29:91:2E:5D

Remove Mapping Body Messages

The regular expression structure for these messages is as follows:

Delete Lease:|DHCP Auto Release:

Once received, the body is parsed for user details as follows:

[10.0.0.11]

Body Message
DHCP:subtype=0:Single:$IGNORE_N$ Delete Lease: IP=10.0.0.11 $IGNORE_N$
DHCP:subtype=0:Single:$IGNORE_N$ DHCP Auto Release: IP=10.0.0.11 $IGNORE_N$

Filter Passive Identity Services

You can filter certain users, based on their name or IP address. For example, if you have an administrator from IT services who logs in to an endpoint in order to assist the regular user with that endpoint, you can filter out the administrator activity so it does not appear in Live Sessions, but rather only the regular user of that endpoint will appear. The Live Session shows Passive Identity service components that are not filtered out by the Mapping Filters. You can add as many filters as needed. The “OR” logic operator applies between filters. If both the fields are specified in a single filter, the “AND” logic operator applies between these fields.

Step 1 Choose **Work Centers** > **PassiveID** > **Providers** and then from the left panel choose **Mapping Filters**.

Step 2 Choose **Providers** > **Mapping Filters**.

Step 3 Click **Add**, enter the Username and or IP address of the user you want to filter and click **Submit**.

Step 4 To view the non-filtered users that are currently logged into the Monitoring session directory, choose **Operations** > **RADIUS Livelog**.

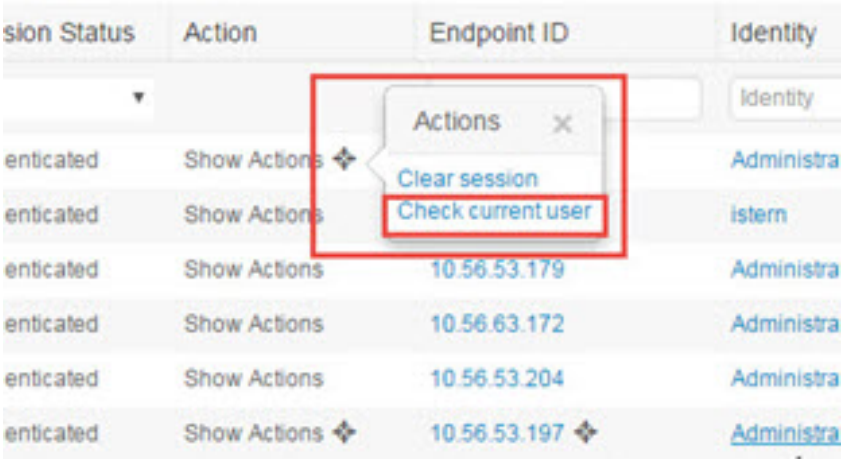
Endpoint Probe

In addition to the customized providers that you can configure the Endpoint probe is enabled in ISE when the Passive Identity service is activated and always runs in the background. The Endpoint probe periodically checks whether each specific user is still logged in to the system.

Note In order to ensure Endpoint runs in the background, you must first configure an initial Active Directory join point and ensure you choose to **Store Credentials**. For more information about configuring the Endpoint probe, see Work with the Endpoint Probe, on page 97.

To manually check for endpoint status go to **Live Sessions** , from the **Actions** column, click **Show Actions** and choose **Check current user**, as in the following figure.

Figure 15: Check Current User



For more information about endpoint user status, and manually running the check, see RADIUS Live Sessions.

When the Endpoint probe recognizes that a user has connected, if 4 hours have passed since the last time the session was updated for the specific endpoint, it checks whether that user is still logged in and collects the following data:

- MAC address
- Operating system version

Based on the this check, the probe does the following:

- When the user is still logged in, the probe updates Cisco ISE with the status Active User.

- When the user has logged out, the session state is updated as Terminated and fifteen minutes later, the user is removed from the Session Directory.
- When the user cannot be contacted, for example, when a firewall prevents contact or the endpoint has shut down, the status is updated as Unreachable and the Subscriber policy will determine how to handle the user session. The endpoint will remain in the Session Directory.

Work with the Endpoint Probe

Before you begin

Create and enable Endpoint probes based on subnet ranges. One Endpoint probe can be created per PSN. To work with Endpoint probes, first ensure you have configured the following:

- Endpoints must have network connectivity to port 445.
- From ISE, configure an initial Active Directory join point and ensure you select **Select Credentials** when prompted. For more information about join points, see Active Directory as a Probe and a Provider, on page 55.

Note In order to ensure Endpoint runs in the background, you must first configure an initial Active Directory join point, which enables the Endpoint probe to run even when the Active Directory probe is not fully configured.

Step 1 Choose **Work Centers** > **Passive ID** > **Providers** and then choose **Endpoint Probes**.

Step 2 Click **Add** to create a new Endpoint probe.

Step 3 Complete the mandatory fields, ensuring you select **Enable** from the **Status** field, and click **Submit**. See Endpoint Probe Settings, on page 97 for more information.

Endpoint Probe Settings

Create a single Endpoint probe per PSN, based on subnet ranges. If you have multiple PSNs in your deployment, then you can allot each PSN for a separate set of subnets.

Table 18: Endpoint Probes Settings

Field Name	Description
Name	Enter a unique name by which to identify the use of this probe.
Description	Enter a unique description that explains the use for this probe.
Status	Choose **Enable** to activate this probe.
Host Name	Choose a PSN for this probe from the list of available PSNs in your deployment.

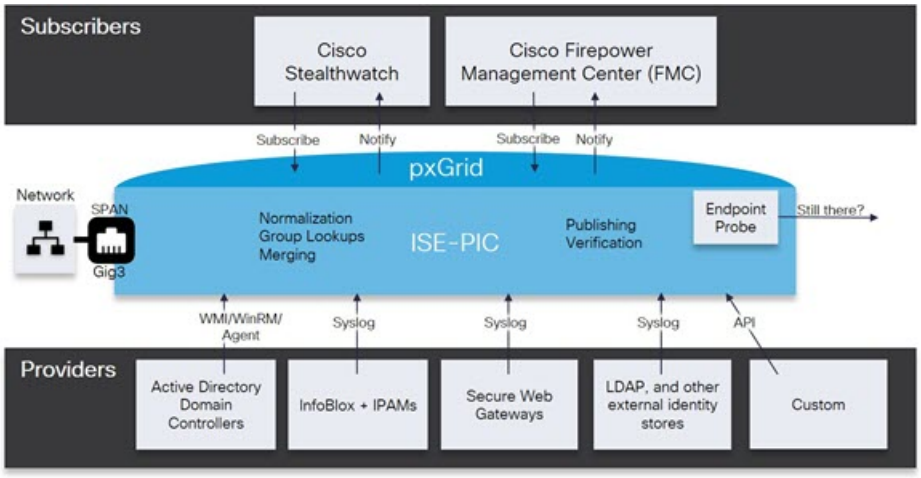
Field Name	Description
Subnets	Enter the subnet range for the group of endpoints that should be checked by this probe. Use standard subnet mask ranges and separate subnet addresses with commas. For example: 10.56.14.111/32,2.55.2.0/16,2.2.3.0/16,1.2.3.4/32 Each range must be unique and separate from all other ranges. For example, you cannot enter the following ranges for the same probe because they overlap with each other: 2.2.2.0/16,2.2.3.0/16

Subscribers

The Passive Identity services use Cisco pxGrid services to deliver authenticated user identities that are collected from various providers and stored by the Cisco ISE session directory, to other network systems such as Cisco Stealthwatch or Cisco Firepower Management Center (FMC).

In the following figure, the pxGrid node collects user identities from external providers. Those identities are parsed, mapped and formatted. pxGrid takes those formatted user identities and sends them to Passive Identity service subscribers.

Figure 16: Passive Identity Service Flow



Subscribers connected to Cisco ISE must register to use the pxGrid services. Subscribers should adopt the pxGrid Client Library available from Cisco through the pxGrid SDK to become the clients. A subscriber can log in to pxGrid using a unique name and certificate-based mutual authentication. Once they have sent a valid certificate, Cisco pxGrid subscribers are automatically approved by ISE.

Subscribers can connect to either a configured pxGrid server hostname or an IP Address. We recommend that you use hostname to avoid unnecessary errors, particularly to ensure the DNS queries work properly. Capabilities are information topics or channels that are created on pxGrid for subscribers to publish and subscribe. In Cisco ISE, only SessionDirectory and IdentityGroup are supported. You can view capability

information that is available from the publisher through publish, directed query, or bulk download query, by navigating to **Subscribers** in the **Capabilities** tab.

To enable subscribers to receive information from ISE, you must:

1. Optionally, generate a certificate from the subscriber's side.
2. Generate pxGrid Certificates for Subscribers, on page 99 from the PassiveID work center.
3. Enable Subscribers, on page 100. Either perform this step, or automatically enable approvals, in order to allow subscribers to receive user identities from ISE. See Configure Subscriber Settings, on page 101.

Generate pxGrid Certificates for Subscribers

Before you begin

You can generate certificates for pxGrid subscribers in order to guarantee mutual trust between pxGrid and the subscribers, thereby enabling user identities to be passed from ISE to the subscribers. To perform the following task, you must be a Super Admin or System Admin.

Step 1 Choose**Work Centers** > **PassiveID** > **Subscribers** and go to the **Certificates** tab.

Step 2 Select one of the following options from the **I want to** drop-down list:

- **Generate a single certificate without a certificate signing request**: You must enter the Common Name (CN) if you select this option. In the Common Name field, enter the pxGrid FQDN which includes pxGrid as the prefix. For example, www.pxgrid-ise.ise.net. Or, alternatively, use wildcards. For example, *.ise.net
- **Generate a single certificate with a certificate signing request**: You must enter the Certificate Signing Request details if you select this option.
- **Generate bulk certificates**: You can upload a CSV file that contains the required details.
- **Download Root Certificate Chain**: Download the ISE public root certificates in order to add them to the pxGrid client's trusted certificate store. The ISE pxGrid node only trusts the newly signed pxGrid client certificate and vice-versa, eliminating the need for outside certificate authorities.

Step 3 (optional) You can enter a description for this certificate.

Step 4 View or edit the pxGrid Certificate template on which this certificate is based. Certificate templates contain properties that are common to all certificates issued by the Certificate Authority (CA) based on that template. The certificate template defines the Subject, Subject Alternative Name (SAN), key type, key size, SCEP RA profile that must be used, validity period of the certificate, and the extended key usage (EKU) that specifies whether the certificate has to be used for client or server authentication or both. The internal Cisco ISE CA (ISE CA) uses a certificate template to issue certificates based on that template. To edit this template, choose **Administration** > **Certificates** > **Certificate Authority** > **Certificate Templates**.

Step 5 Specify the Subject Alternative Name (SAN). You can add multiple SANs. The following options are available:

- **FQDN**: Enter the fully qualified domain name of the ISE node. For example www.isepic.ise.net. Or, alternatively, use wildcards for the FQDN. For example, *.ise.net

  An additional line can be added for FQDN in which the pxGrid FQDN can also be entered. This should be identical to the FQDN you used in the Common Name field.

- **IP address**: Enter the IP address of the ISE node to be associated with the certificate. This information must be entered if the subscriber uses IP addresses instead of an FQDN.

Note This field is not displayed if you have selected the Generate Bulk Certificate option.

Step 6 Select one of the following options from the **Certificate Download Format** drop-down list:

- **Certificate in Private Enhanced Electronic Mail (PEM) format, key in PKCS8 PEM format (including certificate chain)**: The root certificate, the intermediate CA certificates, and the end entity certificate are represented in the PEM format. PEM formatted certificate are BASE64-encoded ASCII files. Each certificate starts with the "--------BEGIN CERTIFICATE-----" tag and ends with the "-------END CERTIFICATE----" tag. The end entity's private key is stored using PKCS* PEM. It starts with the "-----BEGIN ENCRYPTED PRIVATE KEY----" tag and ends with the "-----END ENCRYPTED PRIVATE KEY----" tag.
- **PKCS12 format (including certificate chain; one file for both the certificate chain and key)**: A binary format to store the root CA certificate, the intermediate CA certificate, and the end entity 's certificate and private key in one encrypted file.

Step 7 Enter a certificate password.

Step 8 Click **Create**.

Enable Subscribers

You must perform this task, or alternatively automatically enable approvals, in order to allow subscribers to receive user identities from Cisco ISE. See Configure Subscriber Settings, on page 101.

Before you begin

- Enable the pxGrid persona on at least one node to view the requests from the Cisco pxGrid clients.
- Enable Passive Identity Service. For more information, see Easy Connect, on page 49.

Step 1 Choose **Work Centers** > **PassiveID** > **Subscribers** and ensure you are viewing the **Clients** tab.

Step 2 Check the checkbox next to the subscriber and click **Approve**.

Step 3 Click **Refresh** to view the latest status.

View Subscriber Events from Live Logs

The Live Logs page displays all the Subscriber events. Event information includes the subscriber and capability names along with the event type and timestamp.

Navigate to **Subscribers** and select the **Live Log** tab to view the list of events. You can also clear the logs and resynchronize or refresh the list.

Configure Subscriber Settings

Before you begin

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

Step 1 Choose **Administration** > **pxGrid Services** > **Settings**.

Step 2 Select the following options based on your requirements:

- **Automatically Approve New Accounts**: Check this checkbox to automatically approve the connection requests from new pxGrid clients.
- **Allow Password Based Account Creation**: Check this checkbox to enable username/password based authentication for pxGrid clients. If this option is enabled, the pxGrid clients cannot be automatically approved.

  A pxGrid client can register itself with the pxGrid controller by sending the username via REST API. The pxGrid controller generates a password for the pxGrid client during client registration. The administrator can approve or deny the connection request.

Step 3 Click **Save**.

Monitoring and Troubleshooting Service in PassiveID Work Center

Learn about how you can manage PassiveID Work Center with monitoring, troubleshooting and reporting tools.

- RADIUS Live Sessions
- See the Reports section in Cisco ISE Reports
- TCP Dump Utility to Validate Incoming Traffic

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.

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.

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.

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.

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.

LDAP User Authentication

You can configure LDAP as an external identity store. Cisco ISE uses 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. If the DN and password of the user match the username and password in the LDAP directory, then the user is authenticated.

When Active Directory is used as LDAP, UPN names are used for user authentication. When Sun ONE Directory Server is used as LDAP, SAM names are used for user authentication

Note

- Cisco ISE sends two searchRequest messages for every user authentication. This does not impact Cisco ISE authorization or network performance. The second LDAP request is to make sure the Ciso ISE is talking to the right identity.
- Cisco ISE as a DNS client, uses only the first IP returned in the DNS response to perform the LDAP bind.

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

Note Password change is supported for LDAP only if there are remaining grace logins for the account after the password has expired. If password change is successful, the LDAP server's bindResponse is LDAP_SUCCESS, and includes the remaining grace logins control field in the bindResponse message. If the bindResponse message contains any additional control fields (other than remaining grace logins), Cisco ISE might not be able to decode the message.

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 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 retrieve 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.

You should note the following restrictions on group memberships when Active Directory is configured as an LDAP store:

- Users or computers must be direct members of the group defined in the policy conditions to match the policy rule.
- The defined group may not be a user's or computer's primary group. This restriction is applicable only when Active Directory is configured as an LDAP store.

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).

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.

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.

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

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

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

Add 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.

Configure LDAP Schema

Step 1

Step 2 Select the LDAP instance.

Step 3 Click the **General** tab.

Step 4 Click the drop-down arrow near the **Schema** option.

Step 5 Select the required schema from the **Schema** drop-down list. You can select the **Custom** option to update the attributes based on your requirements.

Predefined attributes are used for the built-in schema, such as Active Directory, Sun directory Server, Novell eDirectory. If you edit the attributes of the predefined schema, Cisco ISE automatically creates a custom schema.

Configure 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 ChooseIn the Cisco ISE GUI, click the **Menu** icon (☰) and 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 Identity Source Settings.

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

Enable 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 ChooseIn the Cisco ISE GUI, click the **Menu** icon (☰) and 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 Identity Source Settings.

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

Retrieve Group Membership Details from the LDAP Server

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

Step 1 ChooseIn the Cisco ISE GUI, click the **Menu** icon (☰) and 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.

Note Active Directory built-in groups are not supported when Active Directory is configured as LDAP Identity Store in Cisco ISE.

Retrieve 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.

Enable Secure Authentication with LDAP Identity Source

When you choose the Secure Authentication option in the LDAP configuration page, Cisco ISE uses SSL to secure communication with the LDAP identity source. Secure connection to LDAP identity source is established using:

- SSL tunnel: Using SSL v3 or TLS v1 (the strongest version supported by the LDAP server)
- Server authentication (authentication of LDAP server): Certificate based
- Client authentication (authentication of Cisco ISE): None (Administrator bind is used inside the SSL tunnel)
- Cipher suites: All cipher suites supported by Cisco ISE

We recommend that you use TLS v1 with the strongest encryption and ciphers that Cisco ISE supports.

To enable Cisco ISE to communicate securely with the LDAP identity source:

Before you begin

- Cisco ISE must be connected to an LDAP server
- TCP port 636 should be open

Step 1 Import the full Certificate Authority (CA) chain of the CA that issued the server certificate to the LDAP server in to Cisco ISE (**Administration** > **System** > **Certificates** > **Trusted Certificates**).

The full CA chain refers to the root CA and intermediate CA certificates; not the LDAP server certificate.

Step 2 Configure Cisco ISE to use secure authentication when communicating with the LDAP identity source (**Administration** > **Identity Management** > **External Identity Sources** > **LDAP**; be sure to check the Secure Authentication check box in the Connection Settings tab).

Step 3 Select the root CA certificate in the LDAP identity store.

ODBC Identity Source

You can use an Open Database Connectivity (ODBC)-compliant database as an external identity source to authenticate users and endpoints. ODBC identity source can be used in an identity store sequence and for Guest and Sponsor authentications. It can also be used for BYOD flow.

The following database engines are supported:

- MySQL
- Oracle
- PostgreSQL
- Microsoft SQL Server
- Sybase

Configuring Cisco ISE to authenticate against an ODBC-compliant database does not affect the configuration of the database. To manage your database, refer to your database documentation.

Note Cisco ISE does not support encryption with ODBC. Hence, ODBC connections are not secured.

Credential Check for ODBC Database

Cisco ISE supports three different types of credential check for an ODBC database. You must configure appropriate SQL stored procedure for each credential check type. Cisco ISE uses the stored procedure to query the appropriate tables in the ODBC database and receive the output parameters or recordset from the ODBC database. The database can return a recordset or a set of named parameters in response to an ODBC query.

The password can be stored in an ODBC database in clear text or encrypted format. The stored procedure can decrypt it back to clear text when it is called by Cisco ISE.

Credential Check Type	ODBC Input Parameters	ODBC Output Parameters	Credential Check	Authentication Protocols
Plain text password authentication in ODBC database	Username Password	Result Group Account Info Error string	If the username and password are matched, relevant user information is returned.	PAP EAP-GTC (as inner method of PEAP or EAP-FAST) TACACS
Plain text password fetching from ODBC database	Username	Result Group Account Info Error string Password	If the username is found, its password and relevant user information is returned by the stored procedure. Cisco ISE calculates the password hash based on the authentication method and compares it with the one that is received from the client.	CHAP MSCHAPv1/v2 EAP-MD5 LEAP EAP-MSCHAPv2 (as inner method of PEAP or EAP-FAST) TACACS
Lookup	Username	Result Group Account Info Error string	If the username is found, relevant user information is returned.	MAB Fast reconnect of PEAP, EAP-FAST, and EAP-TTLS

Note If ODBC is used as the lookup source for authorization, ensure that the ODBC database and incoming request MAB format are same.

The groups that are returned in the output parameters are not used in Cisco ISE. Only the groups that are retrieved by the Fetch Groups stored procedure are used in Cisco ISE. The account information is included only in the authentication audit log.

The following table lists the mapping between the result codes returned by the ODBC database stored procedure and Cisco ISE authentication result codes:

Result code (returned by the stored procedure)	Description	Cisco ISE authentication result code
0	CODE_SUCCESS	NA (authentication passed)
1	CODE_UNKNOWN_USER	UnknownUser
2	CODE_INVALID_PASSWORD	Failed
3	CODE_UNKNOWN_USER_OR_INVALID_PASSWORD	UnknownUser
4	CODE_INTERNAL_ERROR	Error
10001	CODE_ACCOUNT_DISABLED	DisabledUser
10002	CODE_PASSWORD_EXPIRED	NotPerformedPasswordExpired

Note Cisco ISE performs the actual authentication or lookup operation based on this mapped authentication result code.

You can use the stored procedures to fetch groups and attributes from the ODBC database.

Here is a sample procedure that returns recordset for plain text password authentication (for Microsoft SQL Server):

```
CREATE PROCEDURE [dbo].[ISEAuthUserPlainReturnsRecordset]
        @username varchar(64), @password varchar(255)
AS
BEGIN
        IF EXISTS( SELECT  username
        FROM  NetworkUsers
        WHERE  username  = @username
        AND  password  = @password )
        SELECT 0,11,'give full access','No Error'
        FROM  NetworkUsers
        WHERE  username  = @username
        ELSE
        SELECT 3,0,'odbc','ODBC Authen Error'
END
```

Here is a sample procedure that returns recordset for plain text password fetching (for Microsoft SQL Server):

```
CREATE PROCEDURE [dbo].[ISEFetchPasswordReturnsRecordset]
        @username varchar(64)
AS
BEGIN
        IF EXISTS( SELECT  username
        FROM  NetworkUsers
```

```
        WHERE  username  = @username)
        SELECT 0,11,'give full access','No Error',password
        FROM  NetworkUsers
        WHERE  username  = @username
        ELSE
        SELECT 3,0,'odbc','ODBC Authen Error'
END
```

Here is a sample procedure that returns recordset for Lookup (for Microsoft SQL Server):

```
CREATE PROCEDURE [dbo].[ISEUserLookupReturnsRecordset]
        @username varchar(64)
AS
BEGIN
        IF EXISTS( SELECT  username
        FROM  NetworkUsers
        WHERE  username  = @username)
        SELECT 0,11,'give full access','No Error'
        FROM  NetworkUsers
        WHERE  username  = @username
        ELSE
        SELECT 3,0,'odbc','ODBC Authen Error'
END
```

Here is a sample procedure that returns parameters for plain text password authentication (for Microsoft SQL Server):

```
CREATE PROCEDURE [dbo].[ISEAuthUserPlainReturnsParameters]
       @username varchar(64), @password varchar(255), @result INT OUTPUT, @group varchar(255)
 OUTPUT, @acctInfo varchar(255) OUTPUT, @errorString varchar(255) OUTPUT
AS
BEGIN
        IF EXISTS( SELECT  username
        FROM  NetworkUsers
        WHERE  username  = @username
        AND  password  = @password )
        SELECT @result=0, @group=11, @acctInfo='give full access', @errorString='No Error'
        FROM  NetworkUsers
        WHERE  username  = @username
        ELSE
        SELECT @result=3, @group=0, @acctInfo='odbc',  @errorString='ODBC Authen Error'
END
```

Here is a sample procedure that returns parameters for plain text password fetching (for Microsoft SQL Server):

```
CREATE PROCEDURE [dbo].[ISEFetchPasswordReturnsParameters]
        @username varchar(64), @result INT OUTPUT, @group varchar(255) OUTPUT, @acctInfo
varchar(255) OUTPUT, @errorString varchar(255) OUTPUT, @password varchar(255) OUTPUT
AS
BEGIN
        IF EXISTS( SELECT  username
        FROM  NetworkUsers
        WHERE  username  = @username)
       SELECT @result=0, @group=11, @acctInfo='give full access', @errorString='No Error',
 @password=password
        FROM  NetworkUsers
        WHERE  username  = @username
        ELSE
        SELECT @result=3, @group=0, @acctInfo='odbc', @errorString='ODBC Authen Error'
END
```

Here is a sample procedure that returns parameters for Lookup (for Microsoft SQL Server):

```
CREATE PROCEDURE [dbo].[ISEUserLookupReturnsParameters]
        @username varchar(64), @result INT OUTPUT, @group varchar(255) OUTPUT, @acctInfo
varchar(255) OUTPUT, @errorString varchar(255) OUTPUT
```

```
AS
BEGIN
        IF EXISTS( SELECT  username
        FROM  NetworkUsers
        WHERE  username  = @username)
        SELECT @result=0, @group=11, @acctInfo='give full access', @errorString='No Error'
        FROM  NetworkUsers
        WHERE  username  = @username
        ELSE
        SELECT @result=3, @group=0, @acctInfo='odbc', @errorString='ODBC Authen Error'
END
```

Here is a sample procedure that fetches groups from Microsoft SQL Server:

```
CREATE PROCEDURE [dbo].[ISEGroupsH]
        @username varchar(64), @result int output
AS
BEGIN
        if exists (select * from NetworkUsers where username = @username)
        begin
                set @result = 0
                select 'accountants', 'engineers', 'sales','test_group2'
        end
        else
                set @result = 1
END
```

Here is a sample procedure that fetches all the groups of all the users if the username is "*" (for Microsoft SQL Server):

```
ALTER PROCEDURE [dbo].[ISEGroupsH]
                @username varchar(64), @result int output
AS
BEGIN
                if @username = '*'
                begin
                                -- if username is equal to '*' then return all existing
groups
                                set @result = 0
                                select 'accountants', 'engineers',
'sales','test_group1','test_group2','test_group3','test_group4'
                end
                else
                if exists (select * from NetworkUsers where username = @username)
                begin
                                set @result = 0
                                select 'accountants'
                end
                else
                                set @result = 1
END
```

Here is a sample procedure that fetches attributes from Microsoft SQL Server:

```
CREATE PROCEDURE [dbo].[ISEAttrsH]
        @username varchar(64), @result int output
AS
BEGIN
        if exists (select * from NetworkUsers where username = @username)
        begin
                set @result = 0
                                select phone as phone, username as username, department as
 department, floor as floor, memberOf as memberOf, isManager as isManager from NetworkUsers
 where username = @username
        end
        else
```

```
                set @result = 1
END
```

Additional Examples of ODBC Configuration

https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/211581-Configure-ODBC-on-ISE-2-3-with-Oracle-Da.html

https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine-21/200544-Configure-ISE-2-1-with-MS-SQL-using-ODBC.html

https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine-21/200644-Configure-ODBC-on-ISE-2-1-with-PostgreSQ.html

Add ODBC Identity Source

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**.

Step 2 Click **ODBC**.

Step 3 Click **Add**.

Step 4 In the **General** tab, enter a name and description for the ODBC identity source.

Step 5 In the **Connection** tab, enter the following details:

- Hostname or IP address of the ODBC database. If you are using a nonstandard TCP port for the database, you can specify the port number in the following format: hostname or IP address:port
- Name of the ODBC database
- Admin username and password (Cisco ISE connects to the database using these credentials)
- Server timeout in seconds (default is 5 seconds)
- Connection attempts (default is 1)
- Database type. Choose one of the following:
  - **MySQL**
  - **Oracle**
  - **PostgreSQL**
  - **Microsoft SQL Server**
  - **Sybase**

Step 6 Click **Test Connection** to check the connectivity with the ODBC database and to verify the existence of the stored procedures for the configured use cases.

Step 7 In the **Stored Procedures** tab, enter the following details:

Step 8 Add the required attributes in the **Attributes** tab. While adding an attribute, you can specify how the attribute name should appear in the authorization policy rules.

Step 9 Add the user groups in the **Groups** tab. You can also fetch the groups from the ODBC database by specifying the username or MAC address. These groups can be used in authorization policies.

You can rename the groups and attributes. By default, the name that is displayed in the **Name in ISE** field is same as that in ODBC database, however, you can modify this name. This name is used in the authorization policies.

Step 10 Click **Submit**.

Note If you have configured input attributes, you must do the following while duplicating an ODBC identity store. Otherwise, input parameters might be lost in the duplicated ODBC identity store.

1. Click **Advance Settings**.
2. Verify whether the input parameters are set properly.
3. Click **OK** to save these input parameters in the duplicated ODBC identity store.

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.

Note The Process Host Lookup option must be enabled for MAB authentication. We recommend that you don't configure the RADIUS token server that is used as the external identity source, for MAB authentication, because the devices that are using MAB authentication cannot generate an OTP or a RADIUS token (which is required for RADIUS token server authentication). Hence, the authentication will fail. You can use the external RADIUS server option to process the MAB requests.

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

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.

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 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.

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.

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.

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.
- TACACS+ Authorization: Happens after a successful TACACS+ authentication.

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.

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.

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.

The following table lists the different failure cases that are possible with RADIUS identity servers.

Table 19: 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.

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.

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.

Add a RADIUS Token Server

Before you begin

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

Step 1 ChooseIn the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** **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.

a) 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.
b) 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.

Step 4 Check the **Enable Passcode Caching** check box if you want Cisco ISE to store the passcode in the cache after the first successful authentication with an RADIUS token server and use the cached user credentials for the subsequent authentications if they happen within the configured time period.

Enter the number of seconds for which the passcode must be stored in the cache in the **Aging Time** field. Within this period of time, the user can perform more than one authentication with the same passcode. The default value is 30 seconds. The valid range is from 1 to 300 seconds.

Note Cisco ISE clears the cache after the first failed authentication. The user must enter a new, valid passcode.

Note We strongly recommend that you enable this option only when you use a protocol that supports encryption of the passcode, for example, EAP-FAST-GTC. For information on supported authentication protocols for RADIUS Token server, see RADIUS Token Server-Supported Authentication Protocols, on page 115

Step 5 Click the **Authorization** tab.

This tab allows you to configure a name that will appear for the 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. The default value is CiscoSecure-Group-Id.

Note If you want to send any attribute in Access-Accept from External ID source, Ext ID source needs to send <ciscoavpair> as attribute name and value in the format: ACS:<attrname>=<attrvalue> where <attrname> is configured in the **Authorization** tab.

Step 6 Click **Submit**.

Delete 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 ChooseIn the Cisco ISE GUI, click the **Menu** icon (☰) and 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 and 8.0 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 supports only one RSA realm.

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 a latest release of Cisco ISE, 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 sdstatus.12 file is deleted whenever the securid file is reset, or the sdconf.rec or sdopts.rec files are updated.

Add RSA Identity Sources

To create an RSA identity source, you must import the RSA configuration file (sdconf.rec). You must obtain the sdconf.rec file from your RSA administrator. To perform this task, you must be a Super Admin or System Admin.

Adding an RSA identity source involves the following tasks:

Import the RSA Configuration File

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

Step 1 ChooseIn the Cisco ISE GUI, click the **Menu** icon (☰) and 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.
- Configuring Authentication Control Options for RSA Identity Source.

Configure 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.

The Node Secret Status is displayed as *Created* when the user is authenticated against RSA SecurID token server. The Node Secret Status can be one of the following—Created or Not Created. The Node Secret Status is displayed as *Not Created* when it is cleared.

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**.

Configure 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 the second time. The results and the attributes retrieved from the previous authentication are available in the cache.

Configure 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 ChooseIn the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **Identity Management** > **External Identity Sources** > **RSA SecurID**.

Step 2 Click **Prompts**.

Step 3 Enter the values as described in RSA SecurID Identity Source Settings.

Step 4 Click **Submit**.

Configure 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 ChooseIn the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **Identity Management** > **External Identity Sources** > **RSA SecurID**.

Step 2 Click **Prompts**.

Step 3 Click the **Messages** tab.

Step 4 Enter the values as described in RSA SecurID Identity Source Settings.

Step 5 Click **Submit**.

SAMLv2 Identity Provider as an External Identity Source

Security Assertion Markup Language (SAML) is an XML-based open standard data format that enables administrators to access a defined set of applications seamlessly after signing into one of those applications. SAML describes the exchange of security related information between trusted business partners. SAML enables exchange of security authentication information between an Identity Provider (IdP) and a service provider (in this case, ISE).

SAML Single Sign On (SSO) establishes a Circle of Trust (CoT) by exchanging metadata and certificates as part of the provisioning process between the IdP and the Service Provider. The Service Provider trusts the IdP's user information to provide access to the various services or applications.

Enabling SAML SSO results in several advantages:

- It reduces password fatigue by removing the need for entering different user name and password combinations.
- It improves productivity because you spend less time re-entering credentials for the same identity.
- It transfers the authentication from your system that hosts the applications to a third party system.
- It reduces costs as fewer help desk calls are made for password reset, thereby leading to more savings.

The IdP is an authentication module that creates, maintains, and manages identity information for users, systems, or services. The IdP stores and validates the user credentials and generates a SAML response that allows the user to access the service provider protected resources.

Note You must be familiar with your IdP service, and ensure that it is currently installed and operational.

SAML SSO is supported for the following portals:

- Guest portal (sponsored and self-registered)

- Sponsor portal
- My Devices portal
- Certificate Provisioning portal

Note Note that the session services must be enabled on the node on which you want to enable SAML SSO. To enable this option:

1. Choose **Administration** > **System** > **Deployment**.
2. Select the node and click **Edit**.
3. In the **General Settings** tab, enable the **Policy Service** toggle button.
4. Check the **Enable Session Services** check box and click .

You cannot select IdP as external identity source for BYOD portal, but you can select an IdP for a guest portal and enable BYOD flow.

Cisco ISE is SAMLv2 compliant and supports all SAMLv2 compliant IdPs that use Base64-encoded certificates. The IdPs listed below have been tested with Cisco ISE:

- Oracle Access Manager (OAM)
- Oracle Identity Federation (OIF)
- SecureAuth
- PingOne
- PingFederate
- Azure Active Directory

The IdP cannot be added to an identity source sequence.

The SSO session will be terminated and Session Timeout error message will be displayed if there is no activity for the specified time (default is 5 minutes).

If you want to add the Sign On Again button in the Error page of the portal, add the following JavaScript in the Optional Content field in the Portal Error page:

```
<button class="cisco-ise" data-inline="true" data-mini="true" data-theme="b"
id="ui_aup_accept_button" onclick="location.href='PortalSetup.action?portal=<Portal ID>'"
type="button">SignOn Again</button>
```

Add an SAML Identity Provider

Before you begin

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

Step 1 Import the Certificate Authority (CA) certificate in to the Trusted Certificate Store, if the certificate is not self-signed by the IdP. Choose **Administration > System > Certificates > Trusted Certificates > Import** to import the CA certificate.

Step 2 Choose **Work Centers > Network Access > Ext Id Sources**.

Step 3 Click **SAML Id Providers**.

Step 4 Click **Add**.

Step 5 In the **SAML Identity Provider** page, enter the following details:

Step 6 Click **Submit**.

Step 7 Go to the Portal Settings page (Guest, Sponsor, Certificate Provisioning, or My Devices portal) and select the IdP that you want to link to that portal in the **Authentication Method** field.

To access the Portal Settings page:

- Guest portal—Choose **Work Centers** > **Guest Access** > **Portals and Components** > **Guest Portals** > **Create, Edit, or Duplicate** > **Portal Behavior and Flow Settings** > **Portal Settings** (see the Portal Settings for Credentialed Guest Portals section in see Portal Settings for Credentialed Guest Portals).
- Sponsor portal—Choose **Work Centers** > **Guest Access** > **Portals and Components** > **Sponsor Portals** > **Create, Edit, or Duplicate** > **Portal Behavior and Flow Settings** > **Portal Settings** (see Portal Settings for Sponsor Portals).
- My Devices portal—Choose **Work Centers > BYOD > Configure > My Devices Portals > Create, Edit, or Duplicate > Portal Behavior and Flow Settings > Portal Settings** (see Portal Settings for My Devices Portals).
- Certificate Provisioning portal—Choose **Administration > Device Portal Management > Certificate Provisioning > Create, Edit, or Duplicate > Portal Behavior and Flow Settings > Portal Settings** (see Portal Settings for Certificate Provisioning Portal).

Step 8 Click **Save**.

Step 9 Choose **Work Centers > Network Access > Ext Id Sources > SAML Id Providers**. Select the IdP that is linked to that portal and click **Edit**.

Step 10 (Optional) In the **Service Provider Info** tab, add the load balancer details. You can add a load balancer in front of ISE nodes to simplify the configuration on the Identity Provider side and optimize the load on ISE nodes.

The load balancer can be a software-based or hardware-based appliance. It should be able to forward the requests to the ISE nodes in the deployment (by using the port specified at the Portal Settings page).

When a load balancer is used, only the load balancer URL is provided in the service provider metadata file. If load balancer is not configured, multiple AssertionConsumerService URLs will be included in the service provider metadata file.

Note We recommend that you avoid using the same IP address of the load balancer at the portal FQDN setting.

Step 11 In the **Service Provider Info** tab, click **Export** to export the service provider metadata file.

The exported metadata includes the signing certificate of Cisco ISE. The signing certificate is identical to the chosen portal's certificate.

The exported metadata zip file includes a Readme file that contains the basic instructions for configuring each IdP (such as, Azure Active Directory, PingOne, PingFederate, SecureAuth, and OAM).

Note You must re-export the service provider metadata, if a load balancer is not configured or if there are any changes in the portal configuration, such as:

- A new ISE node is registered
- Hostname or IP address of a node is changed
- Fully qualified domain name (FQDN) of My Devices, Sponsor, or Certificate Provisioning portal is changed
- Port or interface settings are changed

If the updated metadata is not re-exported, user authentication may fail at the IdP side.

Step 12 Click **Browse** in the dialog box and save the compressed files locally. Unzip the metadata file folder. When you unzip the folder, you will get a metadata file with the name of the portal. The metadata file includes the Provider ID and Binding URI.

Step 13 Login as Admin user in IdP and import the service provider metadata file. Refer to the Identity Provider user documentation for information on how to import the service provider metadata file.

Step 14 In the **Groups** tab, add the required user groups.

Enter the assertion attribute that specifies the group membership of users in the **Group Membership Attribute** field.

Step 15 Add the user attributes in the **Attributes** tab. While adding an attribute, you can specify how the attribute appears in the assertions returned from the IdP. The name that you specify in the "Name in ISE" field will appear in the policy rules. The following data types are supported for the attributes:

- String
- Integer
- IPv4
- Boolean

Note Adding groups and attributes is not mandatory. These groups and attributes can be used for policy and rule settings. If you are using the sponsor portal, you can add the groups and select these groups while configuring the settings for sponsor groups.

Step 16 Configure the following options in the **Advanced Settings** tab:

- Identity Attribute—Select the attribute that specifies the identity of the user that is being authenticated. You can select the Subject Name attribute or an attribute from the Attribute drop-down list.

  Note Cisco ISE does not support SAML IdP responses that contain subject name (NameID) in transient or persistent formats. Cisco ISE cannot retrieve the Username attribute assertion from the SAML IdP response if these methods are used and the authentication will fail.

- Email attribute—Select the attribute that contains the email address of the sponsor. This is required to match the self-service guest requests with the sponsor.
- Select one of the following options for multi-value attributes:
  - Each value in a separate XML element—Click this option if your IdP returns multiple values of the same attribute in separate XML elements.

- Multiple values in a single XML element—Click this option if your IdP returns multiple values in a single XML element. You can specify the delimiter in the text box.

- Logout Settings
  - Sign Logout Requests—Check this check box if you want the logout requests to be signed. This option is not displayed for OAM and OIF.

    Note SecureAuth does not support SAML Logout.

  - Logout URL—This option is displayed only for OAM and OIF when a load balancer is not configured. When a user logs out of the Sponsor or My Devices portal, the user is redirected to the Logout URL at the IdP to terminate the SSO session and then redirected back to the login page.
  - Redirect Parameter Name—This option is displayed only for OAM and OIF when a load balancer is not configured. The redirect parameter is used to pass the URL of the login page to which the user must be redirected after logging out. The redirect parameter name may differ based on the IdP, for example, end_url or returnURL. This field is case sensitive.

    If logout does not work as expected, check the Identity Provider documentation for the Logout URL and Redirect Parameter Name.

Step 17 Click **Submit**.

Example

For an example of configuring Ping Federate, see **Configure ISE 2.1 Guest Portal with PingFederate SAML SSO**

Delete an Identity Provider

Before you begin

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

Ensure that the IdP that you want to delete is not linked to any portal. If the IdP is linked to any portal, the delete operation fails.

Step 1

Step 2 Check the check box next to the IdP that you want to delete, and then click **Delete**.

Step 3 Click **OK** to delete the IdP that you have selected.

Authentication Failure Log

When authentication against SAML ID Store fails and the IdP redirects the user back to ISE portal (through SAML response), ISE will report a failure reason in the authentication log. For Guest portal (with or without

BYOD flow enabled), you can check the RADIUS Livelog (Operations > RADIUS > Live Log) to know the authentication failure reason. For My Devices portal and Sponsor portal, you can check the My Devices Login/Audit report and Sponsor Login/Audit report (under Operations > Reports > Guest) to know the authentication failure reason.

In case of logout failure, you can check the reports and logs to know the failure reason for My Devices, Sponsor, and Guest portal.

Authentication can fail due to the following reasons:

- SAML Response parse errors
- SAML Response validation errors (for example, Wrong Issuer)
- SAML Assertion validation errors (for example, Wrong Audience)
- SAML Response signature validation errors (for example, Wrong Signature)
- IdP signing certificate errors (for example, Certificate Revoked)

Note Cisco ISE does not support SAML responses with encrypted assertions. If this is configured in the IdP, you will see the following error message in ISE: `FailureReason=24803 Unable to find 'username' attribute assertion`.

If the authentication fails, we recommend that you check the "DetailedInfo" attribute in the authentication log. This attribute provides additional information regarding the cause of failure.

Identity Source Sequences

Identity source sequences define the order in which Cisco ISE looks for user credentials in the different databases.

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.

Create Identity Source Sequences

Before you begin

Ensure that you have configured your external identity sources in Cisco ISE.

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.

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 for certificate-based authentication.

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

Step 5 Rearrange the databases in the **Selected list** field 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**: Choose this option 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**: Choose this option 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 field 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.

Delete 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

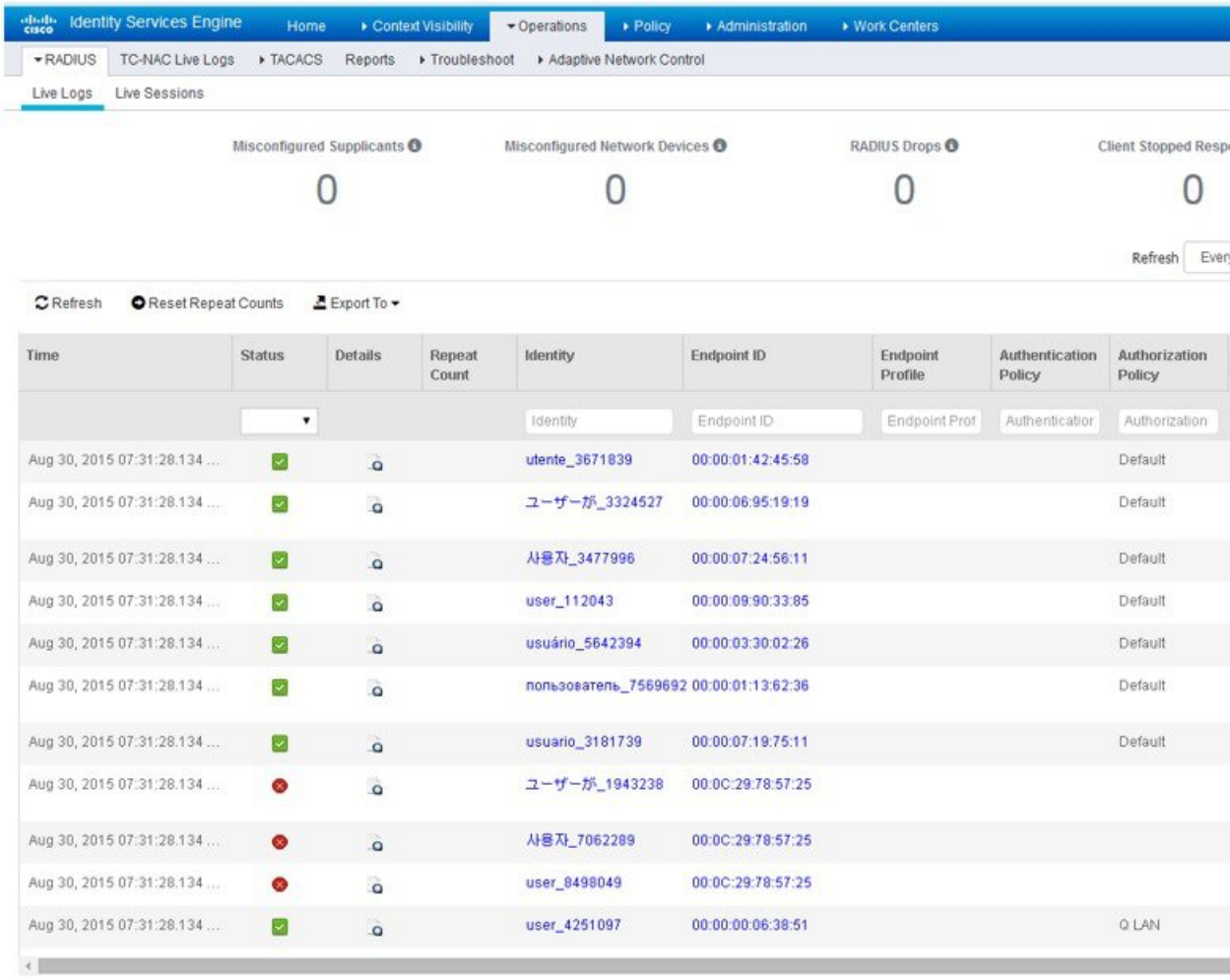
Cisco ISE provides information about the identity sources through the Authentications dashlet and Identity Source reports.

Authentications Dashlet

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

Choose Operations > RADIUS Livelog to view real-time authentication summary. For more information about RADIUS Live Logs, see RADIUS Live Logs.

Figure 17: RADIUS Live Logs



Identity Source Reports

Cisco ISE provides various reports that include information about identity sources. See the Available Reports section for a description of these reports.