

Active Directory Integration with Cisco ISE

Active Directory configuration in Cisco ISE 2

Active Directory key features in Cisco ISE 2

Prerequisites for integrating Active Directory and Cisco ISE 4

Add an Active Directory join point and join a Cisco ISE node to the join point 6

Leave the Active Directory domain 8

Configure authentication domains 9

Supported security group types 10

Configure Active Directory user and machine attributes 11

Test users for Active Directory authentication 11

Support for Active Directory multijoin configuration 12

Read-Only Domain Controllers 13

Authentication protocols and features supported by Active Directory 14

Authorization against an Active Directory instance 17

Identity rewrite 20

Identity resolution settings 22

Sample scenarios 23

Troubleshooting tools 26

AD connector internal operations 30

Revised: September 30, 2026

Active Directory configuration in Cisco ISE

Active Directory key features in Cisco ISE

These are some of the key features of Active Directory in Cisco ISE:

Multi-Join support

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.

Authentication domains

When Cisco ISE is joined to an Active Directory domain, it will automatically discover the join point's trusted domains. However, not all domains may be relevant to Cisco ISE for authentication and authorization. Cisco ISE allows you to select a subset of domains from the trusted domains for authentication and authorization. This subset of domains is called authentication domains. It is recommended to define the domains where users or machines are located that you intend to authenticate, as authentication domains. Defining authentication domains enhances security by blocking domains thus restricting user authentications from taking place on these domains. It also helps optimize performance because you can skip domains that are not relevant for policies and authentication and help Cisco ISE to perform identity search operations more efficiently.

Identity rewrite

This feature allows Cisco ISE to modify the username that is received from the client or a certificate, before sending it toward Active Directory for authentication. For example, the username jdoe@amer.acme.com can be rewritten as jdoe@acme.com. Using this feature, you can fix a username or hostname that would otherwise fail to authenticate.

You can also rewrite identities in certificates and process requests that come with incorrectly provisioned certificates. The same identity rewrite rules are applicable for incoming usernames or machine names, whether they come from a non-certificate based authentication or from within certificates.

Ambiguous identity resolution

If the user or machine name received by Cisco ISE is ambiguous, that is, it is not unique, it can cause problems for users when they try to authenticate. Identity clashes occur in cases when the user does not have a domain markup, or when there are multiple identities with the same username in more than one domain. For example, userA exists on domain1 and another userA exists on domain2. You can use the identity resolution setting to define the scope for the resolution for such users. Cisco highly recommends you to use qualified names such as UPN or NetBIOS. Qualified name reduces chances of ambiguity and increases performance by reducing delays.

Group membership evaluation based on security identifiers

ISE uses security identifiers (SIDs) for optimization of group membership evaluation. SIDs are useful for two reasons, firstly for efficiency (speed) when the groups are evaluated, and secondly, resilience against delays if a domain is down and user is a member of groups from that domain. When you delete a group and create a new group with same name as original, you must update SIDs to assign new SID to the newly created group.

Username-Based Authentication Test (Test User)

Test authentication is useful to troubleshoot authentication and authorization issues for end users. You can use the Test User feature to test Active Directory authentications. The test returns the results along with group and attribute details (authorization information) that can be viewed on the Admin Portal.

Diagnostic tool

The Diagnostic Tool allows you to automatically test and diagnose the Active Directory deployment for general connectivity issues. This tool provides information on:

- The Cisco ISE node on which the test is run
- Connectivity to the Active Directory
- Detailed status about the domain
- Detailed status about Cisco ISE-DNS server connectivity

The tool provides a detailed report for each test that you run.

Certificate Authentication profiles

- Any subject or alternative name attributes in the certificate (for Active Directory only) option—You can use this option to use Active Directory UPN as the username for logs and try all subject names and alternative names in a certificate to look up a user. This option is available only if you choose Active Directory as the identity source.
- Only to resolve identity ambiguity option—You can use this options to resolve identity issues in EAP-TLS authentications. You can have multiple identities from TLS certificates. If the usernames are ambiguous, for example, if there are two “jdoe” from an acquisition, and if the client certificates are present in Active Directory, Cisco ISE can use binary comparison to rule out the ambiguity.

Node view

You can use this page to view the status of the join points on each node in the Cisco ISE deployment. The node view is a read-only page and provides only the status. This page does not support any join, leave, or test option. However, it provides a link for each join point to the main join point page, where these operations can be performed. This page also shows the last diagnostics status and a link to diagnostics tool.

Reports and alarms

Cisco ISE provides new AD Connector Operations report and new alarms in dashboard to monitor and troubleshoot Active Directory related activities.

Advanced tuning

The advanced tuning feature provides node-specific changes and settings to adjust the parameters deeper in the system. This page allows configuration of preferred DCs, GCs, DC failover parameters, and timeouts. This page also provide troubleshooting options like disable encryption. These settings are not intended for normal administration flow and should be used only under Cisco Support guidance.

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. These 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.



Note When integrating Cisco ISE CLI with Active Directory, the AD password must not contain the special character "!". If the password includes this character, the integration will fail with the error message "Pre-Authentication Failed". This restriction applies only to CLI-based integration; the GUI integration does not have this limitation.

Active Directory account permissions required to perform various operations

Join operations	Leave operations	Cisco ISE machine accounts
The join operation requires these account permissions: • Search Active Directory (to verify 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 these account permissions: • Search Active Directory (to verify 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 these 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 this 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, refer to this document.

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 these prerequisites:

- 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.

Add an Active Directory join point and join a 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.

If you want to use IPv6 when integrating with Active Directory, then you must ensure that you have configured an IPv6 address for the relevant ISE nodes.

If you use the Google Chrome browser and have ad blocking software enabled, you must disable the ad blocker. This task contains Cisco ISE GUI elements that are affected by ad blockers. Alternatively, you can carry out this task in a Google Chrome Incognito browser.

Procedure

Step 1 In the Cisco ISE GUI, navigate to **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 these pointers while configuring the join points:

- When using multiple join points, if alternate UPN suffix is configured only for a single join point or domain, identity lookup is performed only in that join point or domain. Authentication might fail in such cases. As a workaround, you can configure the alternate UPN suffix for all the joint points or domains.
- You can only add up to 200 Domain Controllers on ISE. On exceeding the limit, you will receive the error "Error creating <*DC FQDN*> - Number of DCs Exceeds allowed maximum of 200". For more information on the tested scale limit of domain controllers for deployment, refer to Performance and Scalability Guide for Cisco Identity Services Engine.
- 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.
- 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).
- We recommended that you rejoin AD after a designated maintenance window. This ensures that the AD cache is refreshed with the most recent updates.

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.

Procedure

Step 1 In the Cisco ISE GUI, navigate to **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.

Procedure

Step 1 In the Cisco ISE GUI, navigate to **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.

Supported security group types

Cisco ISE supports these security group types:

- Universal
- Global
- Builtin

  Builtin groups do not have a unique security identifier (SID) across domains and to overcome this, Cisco ISE prefixes their SIDs with the domain name to which they belong.

Cisco ISE uses the AD attribute tokenGroups to evaluate a user's group membership. Cisco ISE machine account must have permission to read tokenGroups attribute. This attribute can contain approximately the first 1015 groups that a user may be a member of (the actual number depends on Active Directory configuration and can be increased by reconfiguring Active Directory.) If a user is a member of more groups than this, Cisco ISE does not use more than the first 1015 in policy rules.

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.

Procedure

Step 1 In the Cisco ISE GUI, navigate to **Administration** > **Identity Management** > **External Identity Sources** > **Active Directory**.

Step 2 Click the **Groups** tab.

Step 3 Perform one of these actions:

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.

Procedure

Step 1 In the Cisco ISE GUI, navigate to **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.

Cisco ISE allows you to configure the AD with IPv4 or IPv6 address for user authentication when you manually add the attribute type IP.

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**.

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.

Procedure

Step 1 In the Cisco ISE GUI, navigate to **Administration** > **Identity Management** > **External Identity Sources** > **Active Directory**.

Step 2 Choose one of these 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.

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.

Scopes and join points in identity source sequences and authentication policies

Cisco ISE allows you to define multiple Active Directory join points, where each join point represents a connection to a different Active Directory domain. Each join point can be used in authentication and authorization policies and in identity sequences, as a separate identity store. Join points can be grouped to form a scope that you can use in authentication policy, as authentication results, and in identity source sequences.

You can select individual join points as the result of authentication policy or identity source sequences, when you want to treat each join point as a completely independent group of policy. For example, in a multi-tenant scenario, where the Cisco ISE deployment supports independent groups with their own network devices, network device groups can be used for selection of the Active Directory domain.

However, if Active Directory domains are regarded as part of the same enterprise without any trust between the domains, you can use scopes to join multiple disconnected Active Directory domains and create a common authentication policy. You can thus avoid the need for every join point represented by a different identity store to be defined in the authentication policy and to provide duplicate rules for each domain. The actual join point that is used is included in the authentication identity store for use in the authorization policy.

Identity ambiguity occurs when there are multiple identities in multiple domains, where the username is same. For example, if a username without any domain markup is not unique and Cisco ISE is configured to use a passwordless protocol such as EAP-TLS, there are no other criteria to locate the right user, so Cisco ISE fails the authentication with an ambiguous identity error. If you encounter such ambiguous identities, you can use specific scopes or join points in authentication policy rules or use identity source sequences. For example, you can direct users of specific network device groups to use a specific Active Directory scope or even a single join point, to limit the search scope. Similarly, you can create a rule such as: if the identity ends with @some.domain, use a specific Active Directory join point. This helps to direct authentications to the right join point.

Create a new scope to add Active Directory join points

Procedure

Step 1	In the Cisco ISE GUI, navigate to **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**.

Read-Only Domain Controllers

These operations are supported on Read-Only Domain Controllers:

- Kerberos user authentication
- User lookup
- Attribute and group fetch

Authentication protocols and features supported by Active Directory

Active Directory supports features such as user and machine authentications, changing Active Directory user passwords with some protocols.

This table lists the authentication protocols and the respective features that are supported by Active Directory.

Table 1: 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
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 user authentication process flow

When authenticating or querying a user, Cisco ISE checks these pointers:

- 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.

Supported username formats

These are the supported username types:

- SAM, for example: jdoe
- NetBIOS prefixed SAM, for example: ACME\jdoe
- UPN, for example: jdoe@acme.com
- Alt UPN, for example: john.doe@acme.co.uk
- Subtree, for example: johndoe@finance.acme.com
- SAM machine, for example: laptop$
- NetBIOS prefixed machine, for example: ACME\laptop$
- FQDN DNS machine, for example: host/laptop.acme.com
- Hostname only machine, for example: host/laptop

Password-based authentication in Active Directory

Password Authentication Protocol (PAP) and Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) are password-based protocols. MS-CHAP credentials can be authenticated only by MS-RPC. Cisco ISE provides two options for PAP authentication - MS-RPC and Kerberos. Both MS-RPC and Kerberos are equally secure options. MS-RPC for PAP authentication is a default and recommended option because:

- It provides consistency with MS-CHAP.
- It provides more clear error reporting.
- It allows more efficient communication with Active Directory. In case of MS-RPC, Cisco ISE sends authentication requests to a domain controller from the joined domain only and the domain controller handles the request.

In case of Kerberos, Cisco ISE needs to follow Kerberos referrals from the joined domain to the user's account domain (that is, Cisco ISE needs to communicate with all domains on the trust path from the joined domain to the user's account domain).

Cisco ISE examines the username format and calls the domain manager to locate the appropriate connection. After the domain controller for the account domain is located, Cisco ISE tries to authenticate the user against it. If the password matches, the user is granted access to the network.

Password-based machine authentication is very similar to user-based authentication, except if the machine name is in host/prefix format. This format (which is a DNS namespace) cannot be authenticated as is by Cisco ISE and is converted to NetBIOS-prefixed SAM format before it is authenticated.

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.

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.

Procedure

Step 1 In the Cisco ISE GUI, navigate to **Administration** > **Identity Management** > **External Identity Sources** > **Certificate Authentication Profile** > **Add**.

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 Identity From** 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.

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, refer to Add an Active Directory join point and join a Cisco ISE node to the join point, on page 6.

Security hotpatch requirement for Windows server 2025: When using a domain controller that is running Windows Server 2025, you must install the windows security hotpatch KB5068861 (or a later cumulative update that supersedes it). Cisco ISE cannot join the Active Directory domain if this hotpatch is not installed.

Procedure

Step 1 In the Cisco ISE GUI, navigate to **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 these options as needed:

- **Enable Password Change**

  From Cisco ISE release 3.3 patch 12, Cisco ISE supports joining Windows Server 2025 Active Directory domains without any manual configuration on the domain controller. However, because of the default security settings in Windows Server 2025, domain controllers deny user password change requests initiated through EAP-MS-CHAPv2 or EAP-GTC. Therefore, the **Enable Password Change** setting in Cisco ISE is disabled by default.

- **Enable Machine Authentication**
- **Enable Machine Access Restrictions (MARs)**

Step 5 Check the **Enable dial-in check** check box to verify the dial-in permissions of the user during machine authentication or query. If a dial-in permission is denied, the authentication check will result in a rejection.

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. If dial-in permission is denied, the authentication check will result in a rejection.

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.

Note
Check this check box to allow AD-protected accounts to authenticate.

Authorization against an Active Directory instance

These sections explain the mechanism that Cisco ISE uses to authorize a user or a machine against Active Directory.

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 these restrictions on group memberships in Active Directory:

- Policy rule conditions may reference any of the these: 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.
- Cisco ISE limits SASL (Simple Authentication and Security Layer) LDAP frames to 128 KiB. To avoid error 40286, ensure the total size of the Active Directory `userCertificate` attribute remains under approximately 126 KiB. As a workaround, modify the **Certificate Authentication Profile** by setting **Match Client Certificate Against Certificate In Identity Store** to either `Never` or `Only to resolve identity ambiguity`.

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.

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.

In a multi join point configuration, if authentication is successful for the same identity from each of the join points individually, then this authentication fails if it is done against the identity source sequence "All_AD_Join_Points".

In a multi join point configuration, if Active Directory group retrieval is successful for the same identity from each of the join points individually, then Active Directory group retrieval fails if:

- different join points are used for authentication and authorization.
- authentication uses EAP-TLS without Binary Comparison (**Match Client Certificate Against Certificate In Identity Store** is set to **Never** in the **Certificate Authentication Profile**) and there is an unmatched authorization rule with a different join point ahead of the matched authorization rule.
- authentication uses EAP-TLS without Binary Comparison (**Match Client Certificate Against Certificate In Identity Store** is set to **Never** in **Certificate Authentication Profile**) and Machine Access Restriction (MAR) is enabled with the endpoint using a different join point within the MAR period, from the join point in the current matched authorization rule.

Note In a multi join point configuration, Active Directory group retrieval is successful for each of the join points individually, but it fails if the authentication rule is configured with an identity source sequence that includes "All_AD_Join_Points". Active Directory group retrieval also fails if different join points are used for authorization and authentication.

Refer to Microsoft-imposed limits on the maximum number of usable Active Directory groups in their documentation.

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 these 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.

Authorization policy dictionary attributes

Authorization policy is determined by conditions based on dictionary attributes. Each Active Directory join point has an associated dictionary that includes attributes and groups.

Dictionary	Attribute	Description
Network Access	AD-User-Join-Point	This attribute indicates which join point was used for the user authentication.
Network Access	AD-Host-Join-Point	This attribute indicates which join point was used for the machine authentication.
Network Access	AD-User-DNS-Domain	This attribute indicates which domain DNS qualified name was used for the user authentication.
Network Access	AD-Host-DNS-Domain	This attribute indicates which domain DNS qualified name was used for the machine authentication.
Network Access	MachineAuthenticationIdentityStore	This attribute indicates which identity store was used for machine authentication.
Network Access	WasMachineAuthenticated	This attribute indicates whether the user's machine was authenticated or not.
Join point	ExternalGroups	This attribute indicates the Active Directory group to which the user belongs to.
Join point	IdentityAccessRestricted	This attribute indicates that the user account is disabled or is outside of logon hours and so is prevented from granting access.
Join point	<ATTR name>	This attribute indicates the Active Directory attribute for the user.

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.

These 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.

These 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

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.

Procedure

Step 1 In the Cisco ISE GUI, navigate to **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

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.

Procedure

Step 1 In the Cisco ISE GUI, navigate to **Administration** > **Identity Management** > **External Identity Sources** > **Active Directory**.

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

Step 3 Define these 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 these 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.
- **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 these 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.

Sample scenarios

This section describes some basic scenarios related to Active Directory configuration flow with Cisco ISE.

Enterprise acquisition

Scenario

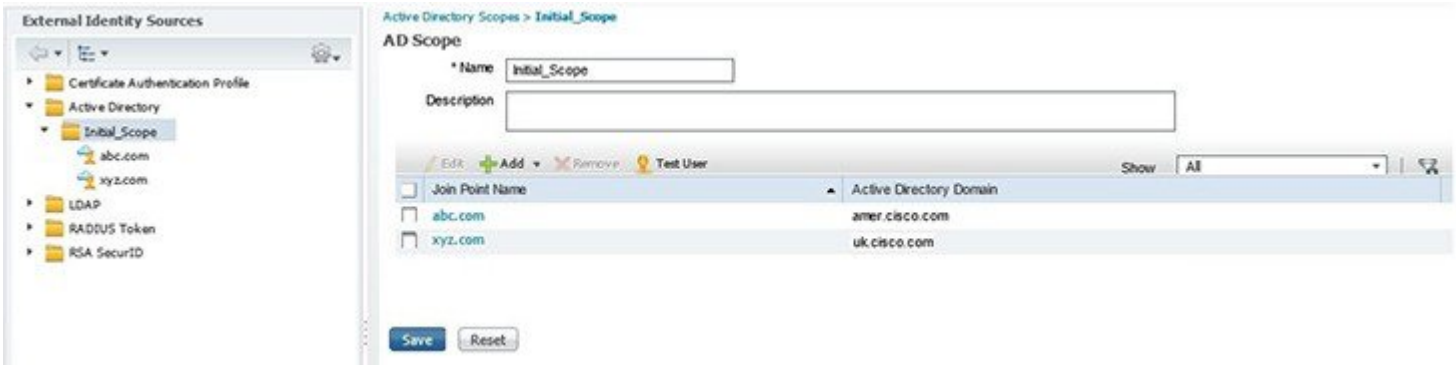
Enterprise, abc.com has acquired or merged with enterprise xyz.com. As an administrator of abc.com, you would like to allow a unified network authentication infrastructure that allows the users of both abc.com and xyz.com to gain access to the same physical network.

Required configurations

A single Active Directory join point for abc.com is already configured. To add an additional untrusted Active Directory infrastructure:

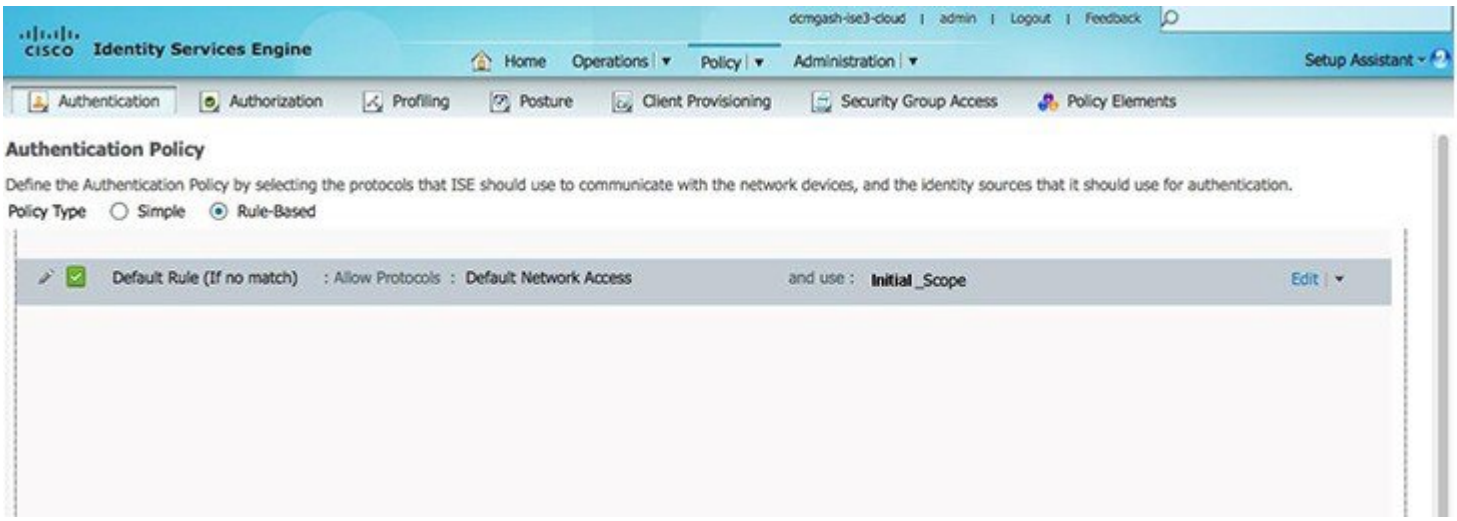
1. Enter scope mode to add Initial_Scope.
2. Add a new join point for xyz.com.

Figure 1: Join points created within Initial_Scope



3. Configure an authentication policy and select Initial_Scope as the result for all authentications.

Figure 2: Initial_Scope selected as the result in authentication policy



By performing the above configurations, you created a scope that configures Cisco ISE to search for users in either company's Active Directory. Scope allows a network to authenticate against multiple Active Directory infrastructures, even if they are completely disconnected and/or do not trust each other.

Multiple tenants

Scenario

For a multi-tenant scenario, you have to define the configuration for multiple customers: CompanyA, CompanyB, and CompanyC. For each customer, you have to:

- Define independent network device groups.
- Define scopes that identity traffic may efficiently scan through.
- Configure and join independent Active Directory join points.

- Define authentication and authorization policy such that Active Directory identity traffic from these device groups is directed to these Active Directory join points.

Required configurations

To provide all the features required:

1. Define the network device group (NDG) type as CompanyA, CompanyB, CompanyC and a add network device for each company.

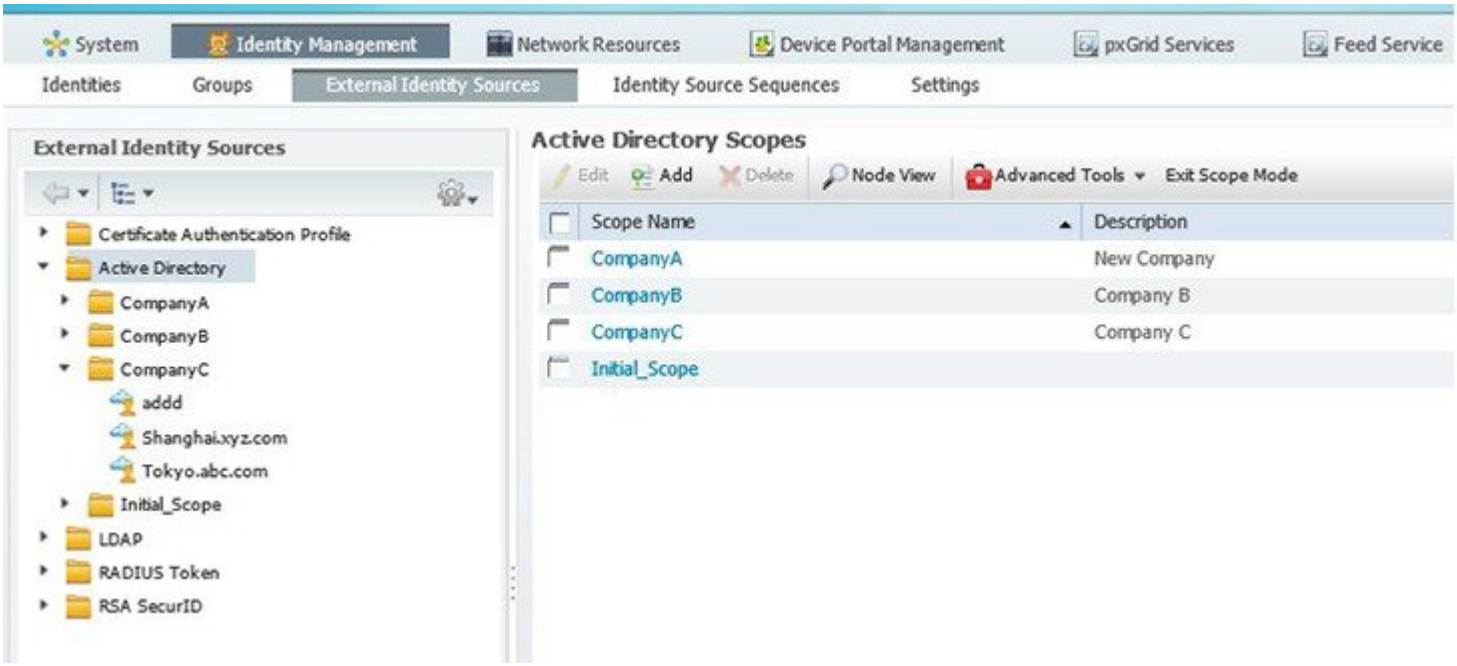
   Figure 3: Define network device group for each Company



2. Define scopes for each company. Define multiple Active Directory join points within the scope of each company.

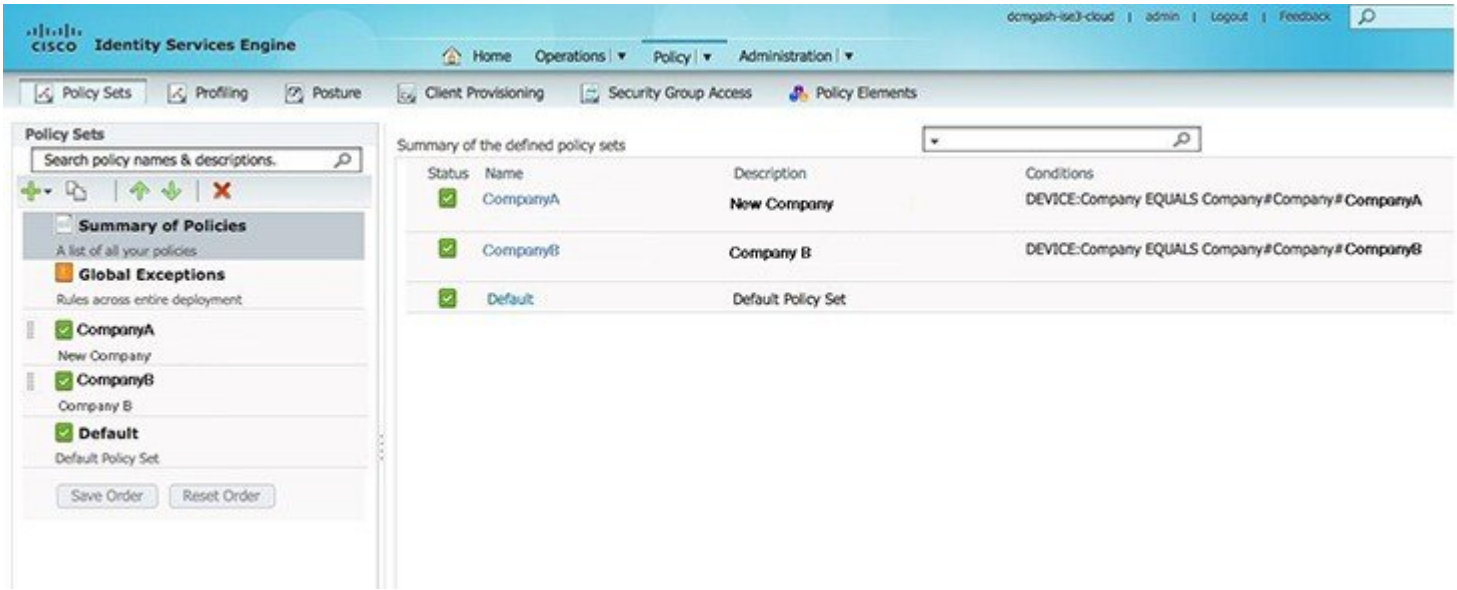
   If all the company's domains were trusted, only a single join point is needed. But in this example, there are a number of untrusted domains, so multiple join points are required.

Figure 4: Define scopes and join points for each Company



3. Configure policy sets to tie together the NDGs of a company to Active Directory scopes for authentication for a company. Each company should also have its own policy so that authorization policy may be defined in the company's own policy group.

Figure 5: Configure policy sets



Troubleshooting tools

Cisco ISE provides several tools to diagnose and troubleshoot Active Directory errors.

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.

Procedure

Step 1 In the Cisco ISE GUI, navigate to **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 You can run the diagnostic tests either on demand or on a scheduled basis.

- To run tests immediately, choose **Run Tests Now**.
- To run the tests at an scheduled interval, check the **Run Scheduled Tests** check box and specify the start time and the interval (in hours, days, or weeks) at which the tests must be run. When this option is enabled, all the diagnostic tests are run on all the nodes and instances and the failures are reported in the **Alarms** dashlet in the **Home** dashboard.

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.

Active Directory alarms and reports

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

Alarms

These 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 these 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** > **Endpoints and Users** > **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** > **Diagnostics** > **AD Connector Operations**.

Locate ambiguous identity errors

You may encounter more than one identity with the same name in one forest. With multi join scenario this is more likely, especially when you have several non-related companies in your Active Directory domain who have no mutual control over their usernames. Using SAM names also increase the chances of name collision. Even NetBIOS prefix is not unique per forest. UPN works well but alternate UPNs can collide. In all such scenarios you will encounter ambiguous identity errors.

You can use the **Authentications** page under the **Operations** tab to look for these attributes. These attributes can help you understand and control which identities are actually used if you face an ambiguous identity error.

- AD-Candidate-Identities—Whenever ambiguous identities are first located, this attribute shows the located identities. It can be useful in determining why an identity is ambiguous.
- AD-Resolved-Identities—After the identity is located and is used in operations such as authentication, get-groups and get-attributes, this attribute is updated with the identity located. This might be more than one in case of identity clash.
- AD-Resolved-Providers—This attribute provides the Active Directory join point on which the identity was found.

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.

Procedure

Step 1 In the Cisco ISE GUI, navigate to **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.

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.

Procedure

Step 1 In the Cisco ISE GUI, navigate to **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

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

Before you begin

Active Directory debug logging must be enabled.

Procedure

Step 1 In the Cisco ISE GUI, navigate to **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 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.

AD connector internal operations

Domain discovery algorithm

The Cisco ISE performs domain discovery in three phases:

1. Queries joined domains—Discovers domains from its forest and domains externally trusted to the joined domain.
2. Queries root domains in its forest—Establishes trust with the forest.
3. Queries root domains in trusted forests—Discovers domains from the trusted forests.

Additionally, Cisco ISE discovers DNS domain names (UPN suffixes), alternative UPN suffixes and NTLM domain names.

The default domain discovery frequency is every two hours. You can modify this value from the Advanced Tuning page, but only in consultation with the Cisco support personnel.

Domain controller discovery

AD connector selects a domain controller (DC) for a given domain:

1. Performs a DNS SRV query (not scoped to a site) to get a full list of domain controllers in the domain.
2. Performs DNS resolution for DNS SRVs that lack IP addresses.
3. Sends CLDAP ping requests to domain controllers according to priorities in the SRV record and processes only the first response, if any. The CLDAP response contains the DC site and client site (for example, site to which the Cisco ISE machine is assigned).
4. If the DC site and client site are the same, the response originator (that is, DC) is selected.
5. If the DC site and client site are not the same, the AD Connector performs a DNS SRV query scoped to the discovered client site, gets the list of domain controllers serving the client site, sends CLDAP ping requests to these domain controllers, and processes only the first response, if any. The response originator (that is, DC) is selected. If there is no DC in the client's site serving the site or no DC currently available in the site, then the DC detected in Step 2 is selected.

You can influence the domain controllers that Cisco ISE uses by creating and using an Active Directory site. Refer to the Microsoft Active Directory documentation on how to create and use sites.

Cisco ISE also provides the ability to define a list of preferred DCs per domain. This list of DCs will be prioritized for selection before DNS SRV queries. But this list of preferred DCs is not an exclusive list. If the preferred DCs are unavailable, other DCs are selected. You can create a list of preferred DCs in these cases:

- The SRV records are bad, missing or not configured.
- The site association is wrong or missing or the site cannot be used.
- The DNS configuration is wrong or cannot be edited.

Domain controller failover

Domain controller (DC) failover can be triggered by these conditions:

- The AD connector detects if the currently selected DC becomes unavailable during the LDAP, RPC, or Kerberos communication attempt. The DC might be unavailable because it is down or has no network connectivity. In such cases, the AD connector initiates DC selection and fails over to the newly selected DC.

- The DC is up and responds to the CLDAP ping, but AD connector cannot communicate with it for some reason, for example if the RPC port is blocked, the DC is in the broken replication state, or the DC has not been properly decommissioned. In such cases, the AD connector initiates DC selection with a black list ("bad" DC is placed in the black list) and tries to communicate with the selected DC. Neither the DC selected with the blacklist nor the blacklist is cached.

DNS failover

You can configure up to three DNS servers and one domain suffix. If you are using Active Directory identity store sequence in Cisco ISE, you must ensure that all the DNS servers can answer forward and reverse DNS queries for any possible Active Directory DNS domain you want to use. DNS failover happens only when the first DNS is down, the failover DNS should have the same recorder as the first DNS. If a DNS server fails to resolve a query, the DNS client does not try another DNS server. By default, DNS server retries the query twice and timeout the query in 3 seconds.

Resolve identity algorithm

For an identity, different algorithms are used to locate the user or machine object based on the type of identity, whether a password was supplied, and whether any domain markup is present in the identity.

These are the different algorithms used by Cisco ISE to resolve different types of identities.



Note If the identity has been rewritten according to configured identity rewrite rules, then identity resolution is applied to the rewritten identity.

Resolving SAM names

- If the identity is a SAM name (username or machine name without any domain markup), Cisco ISE searchs the forest of each join point (once) looking for the identity. If there is a unique match, Cisco ISE determines its domain or the unique name and proceeds with the AAA flow.
- If the SAM name is not unique and Cisco ISE is configured to use a passwordless protocol such as EAP-TLS, there are no other criteria to locate the right user, so Cisco ISE fails the authentication with an "Ambiguous Identity" error. However, if the user certificate is present in Active Directory, Cisco ISE uses binary comparison to resolve the identity.
- If Cisco ISE is configured to use a password-based protocol such as PAP, or MSCHAP, Cisco ISE continues to check the passwords. If there is a unique match, Cisco ISE proceeds with the AAA flow. However, if there is more than one account with the same password, Cisco ISE fails the authentication with an "Ambiguous Identity" error.

You should avoid username collisions. This not only increases efficiency and security but also prevents accounts from being locked out. For example, there exist two "chris" with different passwords and Cisco ISE receives only the SAM name"chris". In this scenario, Cisco ISE will keep trying both accounts with SAM name "chris," before deciding the correct one. In such cases, Active Directory can lock out one of the accounts due to incorrect password attempts. Therefore, you should try to use unique usernames or ones with domain markup. Alternatively, you can use identity rewrite to qualify SAM names if you use specific network devices for each Active Directory domain.

Resolving UPNs

- If the identity is a UPN, Cisco ISE searches each forest's global catalogs looking for a match to that UPN identity. If there is a unique match, Cisco ISE proceeds with the AAA flow. If there are multiple join points with the same UPN and a password was not supplied or does not help in determining the right account, Cisco ISE fails the authentication with an "Ambiguous Identity" error.

- Cisco ISE also permits an identity that appears to be a UPN to also match the user's mail attribute, that is, it searches for "identity=matching UPN or email". Some users log in with their email name (often via a certificate) and not a real underlying UPN. This is implicitly done if the identity looks like an email address.

Resolving machine identities

- If it is a machine authentication, with the identity having a host/prefix, Cisco ISE searches the forest for a matching servicePrincipalName attribute. If a fully-qualified domain suffix was specified in the identity, for example host/machine.domain.com, Cisco ISE searches the forest where that domain exists. If the identity is in the form of host/machine, Cisco ISE searches all forests for the service principal name. If there is more than one match, Cisco ISE fails the authentication with an "Ambiguous Identity" error.
- If the machine is in another identity format, for example machine@domain.com, ACME\laptop$ or laptop$, Cisco ISE uses the normal UPN, NetBIOS or SAM resolution algorithm.

Resolving NetBIOS identities

If the identity has a NetBIOS domain prefix, for example ACME\jdoe, Cisco ISE searches the forests for the NetBIOS domain. Once found, it then looks for the supplied SAM name ("jdoe" in this example) in the located domain. NetBIOS domains are not necessarily unique, even in one forest, so the search may find multiple NetBIOS domains with the same name. If this occurs, and a password was supplied, it is used to locate the right identity. If there is still ambiguity or no password was supplied, Cisco ISE fails the authentication with an "Ambiguous Identity" error.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2016 Cisco Systems, Inc. All rights reserved.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

Asia Pacific Headquarters
CiscoSystems(USA)Pte.Ltd.
Singapore

Europe Headquarters
CiscoSystemsInternationalBV
Amsterdam,TheNetherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.