

Realms

The following topics describe realms and identity policies:

- Realms and realm sequences, on page 1
- License requirements for realms, on page 9
- Requirements and prerequisites for realms, on page 9
- Prerequisites for kerberos authentication, on page 9
- Realm fields, on page 10
- Realm directory and synchronize fields, on page 14
- Create a Microsoft Azure AD Realm, on page 16
- Create an LDAP realm or an Active Directory realm and realm directory, on page 26
- Create a realm sequence, on page 33
- Cross-domain trust setups with Firewall Management Center, on page 34
- Manage a realm, on page 42
- Compare realms, on page 43
- Troubleshoot realms and user downloads, on page 43
- History for realms, on page 51

Realms and realm sequences

Realms are connections between the Secure Firewall Management Center and the user accounts on the servers you monitor that

- specify the connection settings and authentication filter settings for the server,
- specify the users and user groups whose activity you want to monitor, and
- query the user repository for user metadata on authoritative users, as well as some non-authoritative users: POP3 and IMAP users detected by traffic-based detection and users detected by traffic-based detection, a TS Agent, or ISE/ISE-PIC.

(Microsoft AD realm only.) A *realm sequence* is an ordered list of two or more Active Directory realms to use in identity policy. When you associate a realm sequence with an identity rule, the system searches the Active Directory domains in order from first to last as specified in the realm sequence.

Realm configuration requirements

You can add multiple domain controllers as directories in a realm, but they must share the same basic realm information. The directories in a realm must be exclusively LDAP or exclusively Active Directory (AD) servers. After you enable a realm, your saved changes take effect next time the Secure Firewall Management Center queries the server.

To perform user awareness, you must configure a realm for any of the supported server types. The system uses these connections to query the servers for data associated with POP3 and IMAP users, and to collect data about LDAP users discovered through traffic-based detection.

The system uses the email addresses in POP3 and IMAP logins to correlate with LDAP users on an Active Directory, Microsoft Azure Active Directory, or OpenLDAP. For example, if a managed device detects a POP3 login for a user with the same email address as an LDAP user, the system associates the LDAP user's metadata with that user.

To perform user control, you can configure any of these:

- A realm or realm sequence for an Active Directory, Microsoft Azure Active Directory, server, or for ISE/ISE-PIC

Note Configuring a Microsoft AD realm or realm sequence is optional if you plan to configure SGT ISE attribute conditions but not user, group, realm, Endpoint Location, or Endpoint Profile conditions; or if you use your identity policy only to filter network traffic.

Realm sequence is not available for Microsoft Azure AD realms.

- A realm or realm sequence for a Microsoft AD server for the TS Agent.
- For captive portal, an LDAP realm.

  A realm sequence is not supported for LDAP.

You can nest Microsoft AD groups and the Firewall Management Center downloads those groups and the users they contain. You can optionally restrict which groups and users get downloaded as discussed in Create an LDAP realm or an Active Directory realm and realm directory, on page 26.

User synchronization

You can configure a realm or realm sequence to establish a connection between the Firewall Management Center and an LDAP or Microsoft AD server to retrieve user and user group metadata for certain detected users:

- LDAP and Microsoft AD users authenticated by captive portal or reported by ISE/ISE-PIC. This metadata can be used for user awareness and user control.
- POP3 and IMAP user logins detected by traffic-based detection, if those users have the same email address as an LDAP or AD user. This metadata can be used for user awareness.

The Firewall Management Center obtains this information and metadata about each user:

- LDAP user name
- First and last names

- Email address
- Department
- Telephone number



Important To reduce latency between the Firewall Management Center and your Active Directory domain controller, we strongly recommend you configure a realm directory (that is, domain controller) that is as close as possible geographically to the Firewall Management Center.

For example, if your Firewall Management Center is in North America, configure a realm directory that is also in North America. Failure to do so can cause problems such as timeout downloading users and groups.

User activity data

User activity data is stored in the user activity database and user identity data is stored in the users database. The maximum number of users you can store and use in access control depends on your Firewall Management Center model. When choosing which users and groups to include, make sure the total number of users is less than your model limit. If your access control parameters are too broad, the Firewall Management Center obtains information on as many users as it can and reports the number of users it failed to retrieve in the Tasks tab page of the Message Center.

To optionally limit the subnets on which a managed device watches for user awareness data, you can use the **configure identity-subnet-filter** command as discussed in the *Cisco Secure Firewall Threat Defense Command Reference*.



Note If you remove a user that has been detected by the system from your user repository, the Firewall Management Center does *not* remove that user from its users database; you must manually delete it. However, your LDAP changes *are* reflected in access control rules when the Firewall Management Center next updates its list of authoritative users.

Realms and trusted domains

When you configure a Microsoft Active Directory (AD) *realm* in the Firewall Management Center, it is associated with a Microsoft Active Directory or LDAP *domain*.

Microsoft active directory forests and trust relationships

A grouping of Microsoft Active Directory (AD) domains that trust each other is commonly referred to as a *forest*. This trust relationship can enable domains to access each other's resources in different ways. For example, a user account defined in domain A can be marked as a member of a group defined in domain B.



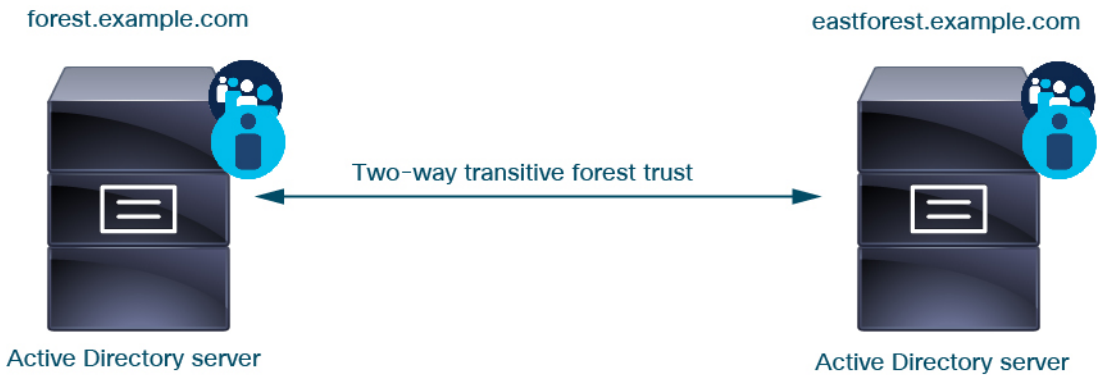
Note Trusted domains apply to Microsoft Active Directory domains only. They do *not* apply to either Microsoft Azure Active Directory or LDAP domains.

The system supports AD forests that are configured in a trust relationship. There are several types of trust relationships; this guide discusses two-way, transitive forest trust relationships. This simple example shows two forests: **forest.example.com** and **eastforest.example.com**. Users and groups in each forest can be authenticated by AD in the other forest, provided you configure the forests that way.

If you set up the system with one realm for each domain and one directory for each domain controller, the system can discover up to 100,000 foreign security principals (users and groups). If these foreign security principals match a user downloaded in another realm, then they can be used in access control policy.

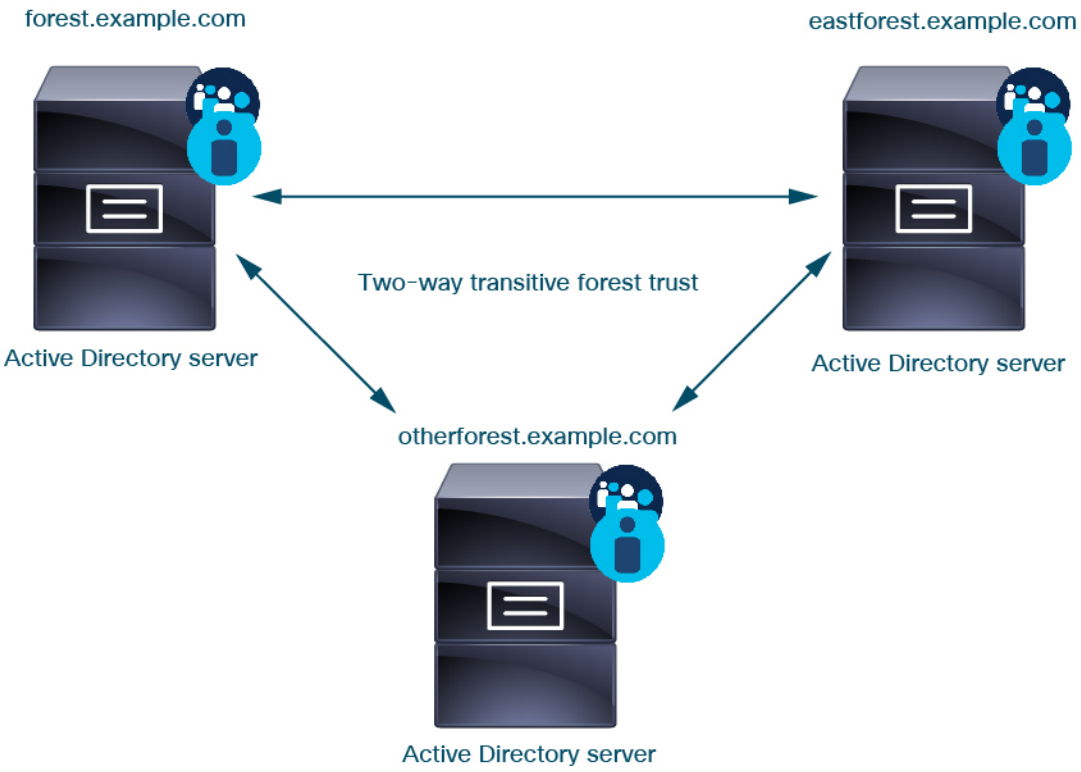
You need not configure a realm for any domain that has no users you wish to use in access control policies.

Figure 1: Two-forest configuration with two-way transitive trust



To continue the example, suppose you have three AD forests (one of which could be a subdomain or an independent forest), all set up as two-way transitive forest relationships, all users and groups are available in all three forests as well as in the system. (As in the preceding example, all three AD domains must be set up as realms and all domain controllers must be configured as directories in those realms.)

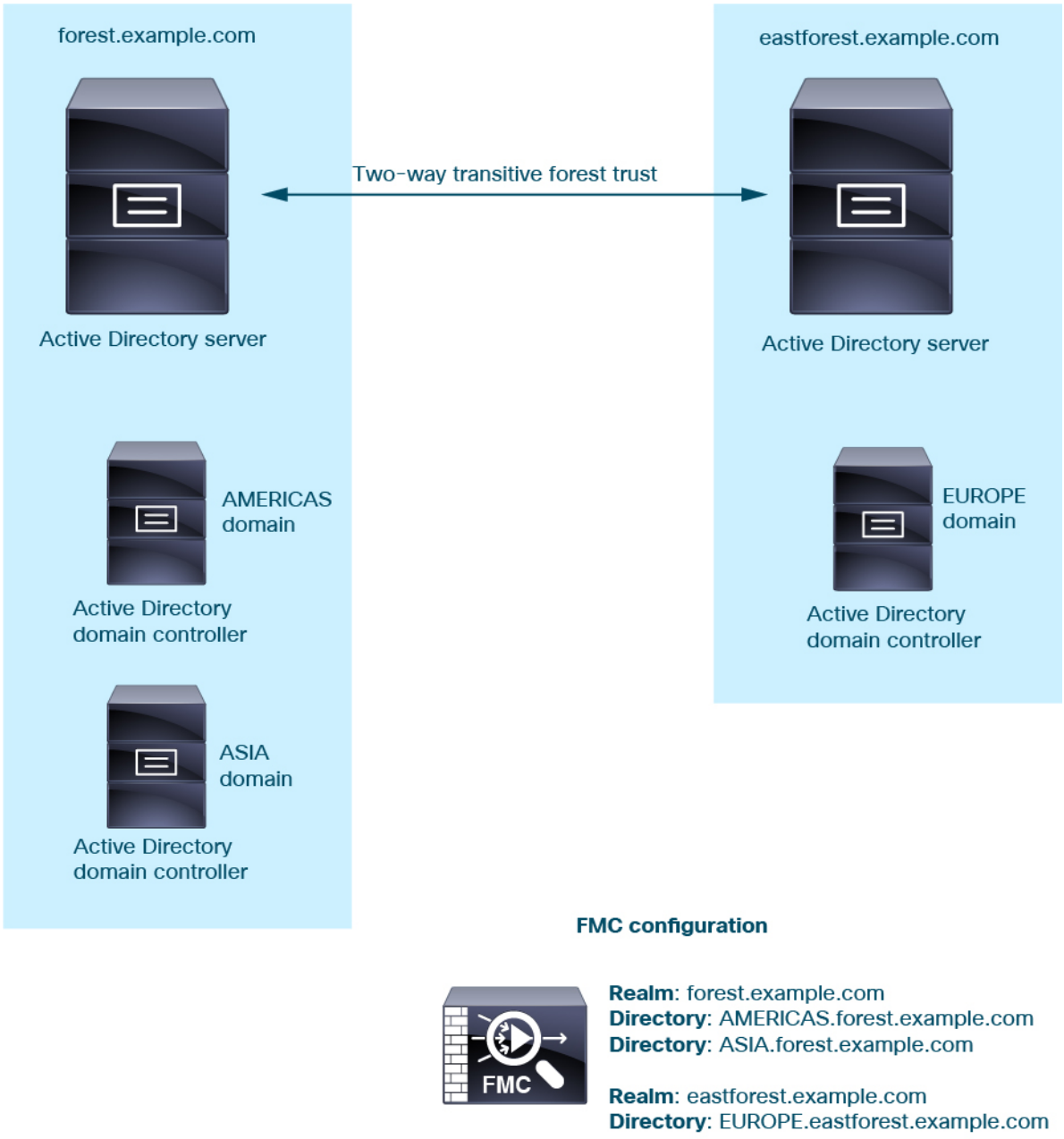
Figure 2: Three-forest configuration with two-way transitive trust



Finally, you can set up the Firewall Management Center to be able to enforce identity policies on users and groups in a two-forest system with two-way transitive forest trust. Suppose each forest has at least one domain controller, each of which authenticates different users and groups. For the Firewall Management Center to be able to enforce identity policies on those users and groups, you must set up each domain containing relevant users as Firewall Management Center realm and each domain controller as Firewall Management Center directory in the respective realm.

Failure to properly configure the Firewall Management Center prevents some of the users and groups from being able to be used in policies. You will see warnings when you try to synchronize users and groups in that case.

Figure 3: Multi-domain forest configuration



Using the preceding example, set up the Firewall Management Center as follows:

- Realm for any domain in **forest.example.com** that contains users you want to control with access control policies
  - Directory in the realm for **AMERICAS.forest.example.com**
  - Directory in the realm for **ASIA.forest.example.com**

- Realm for any domain in **eastforest.example.com** that contains users you want to control with access control policies
  - Directory in the realm for **EUROPE.eastforest.example.com**

Note The Firewall Management Center uses the AD field **msDS-PrincipalName** to resolve references to find user and group names in each domain controller. **msDS-PrincipalName** returns a NetBIOS name.

Supported servers for realms

You can configure realms to connect to the following types of servers, providing they have TCP/IP access from the Firewall Management Center:

Server Type	Supported for ISE/ISE-PIC data retrieval?	Supported for TS Agent data retrieval?	Supported for captive portal data retrieval?
Microsoft Active Directory on Windows Server 2012, 2016, and 2019	Yes	Yes	Yes
Microsoft Azure AD	Yes	No	No
OpenLDAP on Linux	No	No	Yes

An Active Directory Global Catalog server is *not supported* as a realm directory. For more information about the Global Catalog Server, refer to Global Catalog on learn.microsoft.com.

Note If the TS Agent is installed on a Microsoft Active Directory Windows Server shared with another passive authentication identity source (ISE/ISE-PIC), the Firewall Management Center prioritizes the TS Agent data. If the TS Agent and a passive identity source report activity by the same IP address, only the TS Agent data is logged to the Firewall Management Center.

Note the following about your server group configurations:

- To perform user control on user groups or on users in groups, you must configure user groups on the LDAP or Active Directory server.
- Group names cannot start with `S-` because it is used internally by LDAP.

  Neither group names nor organizational unit names can contain special characters like asterisk (*), equals (=), or backslash (\); otherwise, users in those groups or organizational units are not downloaded and are not available for identity policies.

- To configure an Active Directory realm that includes or excludes users who are members of a sub-group on your server, note that Microsoft recommends that Active Directory has no more than 5000 users per group in Windows Server 2012. For more information, see Active Directory Maximum Limits—Scalability on MSDN.

  If necessary, you can modify your Active Directory server configuration to increase this default limit and accommodate more users.

- To uniquely identify the users reported by a server in your Remote Desktop Services environment, you must configure the Cisco Terminal Services (TS) Agent. When installed and configured, the TS Agent assigns unique ports to individual users so the system can uniquely identify those users. (Microsoft changed the name *Terminal Services* to *Remote Desktop Services*.)

  For more information about the TS Agent, see the *Cisco Terminal Services (TS) Agent Guide*.

Supported server object class and attribute names

Map user metadata attributes from your LDAP servers to the correct firewall fields to ensure user information is accurately retrieved and populated in the firewall.

The servers in your realms *must* use the attribute names listed in the following table for the Secure Firewall Management Center to retrieve user metadata from the servers. If the attribute names are incorrect on your server, the Secure Firewall Management Center cannot populate its database with the information in that attribute.

Table 1: Map of attribute names to Secure Firewall Management Center fields

Metadata	Firewall Management Center Attribute	LDAP ObjectClass	Active Directory Attribute	OpenLDAP Attribute
LDAP user name	Username	• user • inetOrgPerson	samaccountname	cn uid
first name	First Name		givenname	givenname
last name	Last Name		sn	sn
email address	Email		mail userprincipalname (if mail has no value)	mail
department	Department		department distinguishedname (if department has no value)	ou
telephone number	Phone		telephonenumber	telephonenumber

Note The LDAP ObjectClass for groups is `group`, `groupOfNames`, (`group-of-names` for Active Directory) or `groupOfUniqueNames`.

For more information about ObjectClasses and attributes, see these references:

- Microsoft Active Directory:
  - ObjectClasses: All Classes on MSDN
  - Attributes: All Attributes on MSDN
- OpenLDAP: RFC 4512

License requirements for realms

This topic outlines the specific license requirements necessary to enable and manage realms.

Threat Defense License

Any

Classic License

Control

Requirements and prerequisites for realms

Model support

Any.

Supported domains

Any

User roles

- Admin
- Access Admin
- Network Admin

Prerequisites for kerberos authentication

If you're using Kerberos to authentication captive portal users, keep the following in mind.

Hostname character limit

If you're using Kerberos authentication, the managed device's host name must be less than 15 characters (it's a NetBIOS limitation set by Windows); otherwise, captive portal authentication fails. You set the managed device host name when you set up the device. For more information, see an article like this one on the Microsoft documentation site: Naming conventions in Active Directory for computers, domains, sites, and OUs.

DNS response character limit

DNS must return a response of 64KB or less to the hostname; otherwise, the AD connection test fails. This limit applies in both directions and is discussed in RFC 6891 section-6.2.5.

Realm fields

Configure a realm to manage user authentication, directory access, and session timeouts for Active Directory, LDAP, or LOCAL user repositories in the Secure Firewall Management Center. Learn how to set realm type, credentials, supported characters, and session duration for identity policies and RA-VPN configurations.

Realm configuration fields

These settings apply to all Active Directory servers or domain controllers (also referred to as *directories*) in a realm.

Name

A unique name for the realm.

- To use the realm in identity policies, the system supports alphanumeric and special characters.
- To use the realm in RA VPN configurations, the system supports alphanumeric, hyphen (-), underscore (_), and plus (+) characters.

Description

(Optional.) Enter a description of the realm.

Type

The type of realm, **AD** for Microsoft Active Directory, **LDAP** for other supported LDAP repositories, or **LOCAL**. For a list of supported LDAP repositories, see Supported servers for realms, on page 7. You can authenticate captive portal users with an LDAP repository; all others require Active Directory.

Note Only captive portal supports an LDAP realm.

The realm type **LOCAL** is used for configuring LOCAL user settings. The LOCAL realm is used in remote access user authentication.

Add the following LOCAL User Information for the LOCAL realm:

- **Username**—Name of the LOCAL user.
- **Password**—LOCAL user password.
- **Confirm Password**—Confirm the LOCAL user password.



Note **Click Add another LOCAL user** to add more users to the LOCAL realm.

You can add more users after creating the realm and update password for the LOCAL users. You can also create multiple LOCAL realms but cannot disable them.

AD Primary Domain

For Microsoft Active Directory realms only. Domain for the Active Directory server where users should be authenticated.



Note You must specify a unique **AD Primary Domain** for every Microsoft Active Directory (AD) realm. Although the system allows you to specify the same **AD Primary Domain** for different Microsoft AD realms, the system won't function properly. This happens because system assigns a unique ID to every user and group in each *realm*; therefore, the system cannot definitively identify any particular user or group. The system prevents you from specifying more than one realm with the same **AD Primary Domain** because users and groups won't be identified properly. This happens because system assigns a unique ID to every user and group in each *realm*; therefore, the system cannot definitively identify any particular user or group.

AD Join Username and AD Join Password

(Available on the **Realm Configuration** tab page when you edit a realm.)

For Microsoft Active Directory realms intended for Kerberos captive portal active authentication, the distinguished username and password of any Active Directory user with appropriate rights to create a Domain Computer account in the Active Directory domain.

Keep the following in mind:

- DNS must be able to resolve the domain name to an Active Directory domain controller's IP address.
- The user you specify must be able to join computers to the Active Directory domain.
- The user name must be fully qualified (for example, **`administrator@mydomain.com`**, *not* **`administrator`**).

If you choose **`Kerberos`** (or **`HTTP Negotiate`**, if you want Kerberos as an option) as the **Authentication Protocol** in an identity rule, the **Realm** you select must be configured with an **AD Join Username** and **AD Join Password** to perform Kerberos captive portal active authentication.



Note The SHA-1 hash algorithm is not secure for storing passwords on your Active Directory server and should not be used. For more information, consult a reference such as Migrating your Certification Authority Hashing Algorithm from SHA1 to SHA2 on Microsoft TechNet or Password Storage Cheat Sheet on the Open Web Application Security Project website.

We recommend SHA-256 for communicating with Active Directory.

Group Attribute

(Available on the **Realm Configuration** tab page.)

These group attributes are available for Microsoft Active Directory or LDAP realms.

- Member: A user attribute that indicates the groups to which a user belongs. Each user entry contains a Member attribute that lists the groups the user is part of, rather than each group listing its members.
- Unique Member: A group attribute that lists the distinguished names (DNs) of the members of the group.

Directory Username and Directory Password

The distinguished username and password for a user with appropriate access to the user information you want to retrieve.

Note the following:

- For OpenLDAP, the user's access privileges are determined by the `<level>` parameter discussed in section 8 of the OpenLDAP specification. The user's `<level>` should be `auth` or better.
- The user name must be fully qualified (for example, **`administrator@mydomain.com`**, *not* **`administrator`**).



Note The SHA-1 hash algorithm is not secure for storing passwords on your Active Directory server and should not be used. For more information, consult a reference such as Migrating your Certification Authority Hashing Algorithm from SHA1 to SHA2 on Microsoft TechNet or Password Storage Cheat Sheet on the Open Web Application Security Project website.

We recommend SHA-256 for communicating with Active Directory.

Base DN

(Optional.)The directory tree on the server where the Secure Firewall Management Center should begin searching for user data. If you don't specify a **Base DN**, the system retrieves the top-level DN provided you can connect to the server.

Typically, the base distinguished name (DN) has a basic structure indicating the company domain name and operational unit. For example, the Security organization of the Example company might have a base DN of **`ou=security,dc=example,dc=com`**.

Group DN

(Optional.)The directory tree on the server where the Secure Firewall Management Center should search for users with the group attribute. A list of supported group attributes is shown in Supported server object class and attribute names, on page 8. If you don't specify a **Group DN**, the system retrieves the top-level DN provided you can connect to the server.

Note The following is the list of characters the system *supports* in users, groups, DNS in your directory server. Using any characters other than these could result in the system failing to download users and groups.

Entity	Supported characters
User name	**a-z A-Z 0-9 ! # $ % ^ & ( ) _ - { } ' . ~ `**
Group name	**a-z A-Z 0-9 ! # $ % ^ & ( ) _ - { } ' . ~ `**
Base DN and Group DN	**a-z A-Z 0-9 ! @ $ % ^ & * ( ) _ - . ~ `**

A space is not supported anywhere in a user name, including at the end.

These fields are available when you edit an existing realm.

User Session Timeout

(Available on the **Realm Configuration** tab page when you edit a realm.)

Enter the number of minutes before user sessions time out. The default is 1440 (24 hours) after the user's login event. After the timeout is exceeded, the user's session ends; if the user continues to access the network without logging in again, the user is seen by the Secure Firewall Management Center as Unknown (except for **Failed Captive Portal Users**).

In addition, if you set up ISE/ISE-PIC without a realm and the timeout is exceeded, a workaround is required. For more information, contact Cisco TAC.

You can set timeout values for the following:

- **User Agent and ISE/ISE-PIC Users**: Timeout for users tracked by the user agent or by ISE/ISE-PIC, which are types of passive authentication.

  The timeout value you specify does *not* apply to pxGrid SXP session topic subscriptions (for example, destination SGT mappings). Instead, session topic mappings are preserved as long as there is no delete or update message for a given mapping from ISE.

  For more information about ISE/ISE-PIC, see The ISE/ISE-PIC identity source.

- **Terminal Services Agent Users**: Timeout for users tracked by the TS Agent, which is a type of passive authentication. For more information, see Terminal services agent identity source.

- **Captive Portal Users**: Timeout for users who successfully log in using the captive portal, which is a type of active authentication. For more information, see Captive portal identity source.

- **Failed Captive Portal Users**: Timeout for users who do not successfully log in using the captive portal. You can configure the **Maximum login attempts** before the user is seen by the Secure Firewall Management Center as Failed Auth User. A Failed Auth User can optionally be granted access to the network using access control policy and, if so, this timeout value applies to those users.

  For more information about failed captive portal logins, see Captive portal fields.

- **Guest Captive Portal Users**: Timeout for users who log in to the captive portal as a guest user. For more information, see Captive portal identity source.

Realm directory and synchronize fields

Configure Active Directory realm directory and user synchronization fields to enable secure authentication, user data lookup, and group management in the Secure Firewall Management Center. Learn how to specify server, encryption, domain, and group settings for optimized user awareness and access control.

Realm directory fields

These settings apply to individual servers (such as Active Directory domain controllers) in a realm.

Hostname / IP Address

Fully qualified host name of the Active Directory domain controller machine. To find the fully qualified name, see Find the active directory server's name, on page 29.

If you're using Kerberos for authenticating captive portal, also make sure you understand these considerations:

If you're using Kerberos authentication, the managed device's host name must be less than 15 characters (it's a NetBIOS limitation set by Windows); otherwise, captive portal authentication fails. You set the managed device host name when you set up the device. For more information, see an article like this one on the Microsoft documentation site: Naming conventions in Active Directory for computers, domains, sites, and OUs.

DNS must return a response of 64KB or less to the hostname; otherwise, the AD connection test fails. This limit applies in both directions and is discussed in RFC 6891 section-6.2.5.

Port

The server's port.

Encryption

(Strongly recommended.) The encryption method to use:

- **`STARTTLS`**—encrypted LDAP connection
- **`LDAPS`**—encrypted LDAP connection
- **`None`**—unencrypted LDAP connection (unsecured traffic)

To communicate securely with an Active Directory server, see Connect securely to Active Directory or LDAP, on page 28.

CA Certificate

The TLS/SSL certificate to use for authentication to the server. You must configure **`STARTTLS`** or **`LDAPS`** as the **Encryption** type to use a TLS/SSL certificate.

If you are using a certificate to authenticate, the name of the server in the certificate must match the server **Hostname / IP Address**. For example, if you use 10.10.10.250 as the IP address but **`computer1.example.com`** in the certificate, the connection fails.

Interface used to connect to Directory server

Required only for RA VPN authentication so the Secure Firewall Threat Defense can connect securely to your Active Directory server. This interface is not used for downloading users and groups, however.

You can choose only a routed interface group. For more information, see Interfaces.

Click one of these options:

- **Resolve via route lookup**: Use routing to connect to the Active Directory server.
- **Choose an interface**: Choose a specific managed device interface group to connect to the Active Directory server.

User synchronize fields

AD Primary Domain

For Microsoft Active Directory realms only. Domain for the Active Directory server where users should be authenticated.

Note You must specify a unique **AD Primary Domain** for every Microsoft Active Directory (AD) realm. Although the system allows you to specify the same **AD Primary Domain** for different Microsoft AD realms, the system won't function properly. This happens because system assigns a unique ID to every user and group in each *realm*; therefore, the system cannot definitively identify any particular user or group. The system prevents you from specifying more than one realm with the same **AD Primary Domain** because users and groups won't be identified properly. This happens because system assigns a unique ID to every user and group in each *realm*; therefore, the system cannot definitively identify any particular user or group.

Enter query to look for users and groups

Base DN:

(Optional.) The directory tree on the server where the Firewall Management Center should begin searching for user data.

Typically, the base distinguished name (DN) has a basic structure indicating the company domain name and operational unit. For example, the Security organization of the Example company might have a base DN of `ou=security,dc=example,dc=com`.

Group DN:

(Optional.) The directory tree on the server where the Firewall Management Center should search for users with the group attribute. A list of supported group attributes is shown in Supported server object class and attribute names, on page 8.

Note Neither the group name nor the organizational unit name can contain special characters like asterisk (*), equals (=), backslash (\) because users in those groups are not downloaded and cannot be used in identity policies.

Load Groups

Enables you to download users and groups for user awareness and user control.

Available Groups, Add to Include, Add to Exclude

Limits the groups that can be used in policy.

- Groups that are displayed in the **Available Groups** field are available for policy unless you move groups to the **Included Groups and Users** or **Excluded Groups and Users** field.
- If you move groups to the **Included Groups and Users** field, only those groups and users they contain are downloaded and user data is available for user awareness and user control.
- If you move groups to the **Excluded Groups and Users** field, all groups and users they contain *except* these are downloaded and available for user awareness and user control.
- To include users from groups that are not included, enter the user name in the field below **User Inclusion** and click **Add**.
- To exclude users from groups that are not excluded, enter the user name in the field below **User Exclusion** and click **Add**.

Note The users that are downloaded to the Firewall Management Center is calculated using the formula **R = I - (E+e) + i**, where

- R is list of downloaded users
- I is included groups
- E is excluded groups
- e is excluded users
- i is included users

Synchronize Now
Click to synchronize groups and users with AD.

Begin automatic synchronization at
Enter the time and time interval at which to download users and groups from AD.

Create a Microsoft Azure AD Realm

You can use a Microsoft Azure Active Directory (AD) realm with Cisco ISE to authenticate users and get user sessions for user control. We get groups from Azure AD and logged-in user session data from Cisco ISE.

Authentication options

You have two authentication options:

- Resource owned password credentials (ROPC): Enables users to log in with a client like AnyConnect using a user name and password. ISE sends user sessions to the Secure Firewall Management Center. For more information, see How Entra ID and Cisco ISE authentication with resource owned password credentials works, on page 17.

  Additional resource: Microsoft identity platform and OAuth 2.0 Resource Owner Password Credentials on learn.microsoft.com.

- Extensible Authentication Protocol (EAP) Chaining with Tunnel-based Extensible Authentication Protocol (TEAP) and Transport Layer Security (TLS), abbreviated EAP/TEAP-TLS: TEAP is a tunnel-based EAP

method that establishes a secure tunnel and executes other EAP methods under the protection of that secured tunnel. ISE is used to validate user credentials and to send user sessions to the Secure Firewall Management Center. For more information, see How Entra ID and Cisco ISE authentication works with TEAP/EAP-TLS, on page 18.

Note Before deploying policies related to a Microsoft Azure AD realm, see User limits for microsoft azure active directory realms.

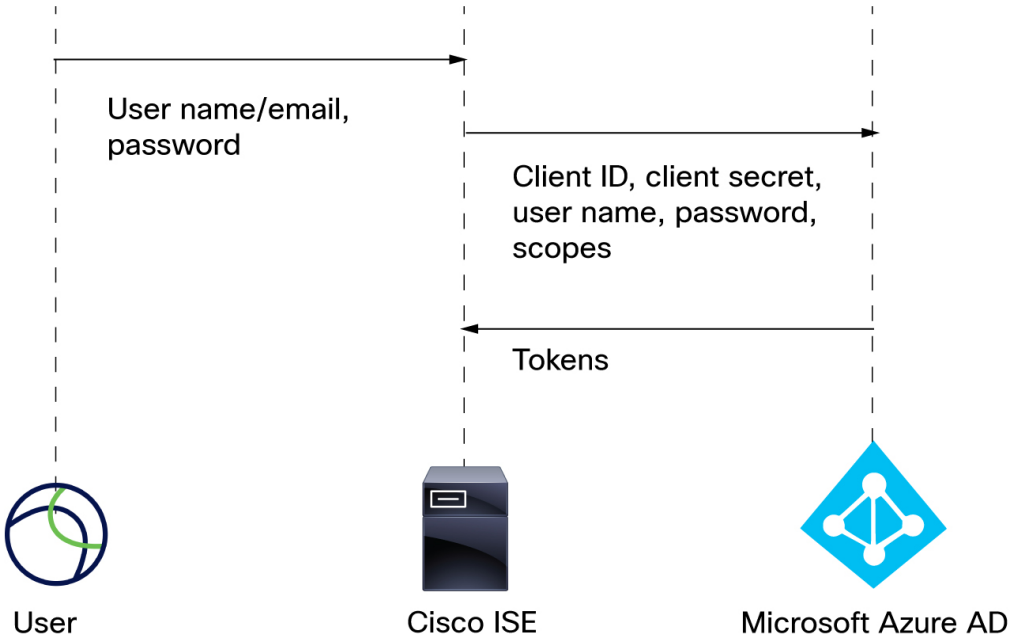
How Entra ID and Cisco ISE authentication with resource owned password credentials works

Summary

The key components involved in the Entra ID authentication with resource owned password credentials process are:

- User: Logs in with credentials using a VPN client
- Cisco Secure Client: VPN client that sends user credentials
- Entra ID (formerly Azure AD): Validates credentials and issues tokens
- Cisco ISE: Receives tokens and manages user sessions
- Secure Firewall Management Center: Receives user sessions from ISE

Workflow



These stages describe how Entra ID and Cisco ISE authentication with resource owned password credentials works:

1. The user logs in with a user name (or email address) and password using a VPN client like Cisco Secure Client.
2. The client ID, client secret, user name, password, and scopes are sent to Entra ID.
3. Tokens are sent from Entra ID to Cisco ISE, which sends user sessions to the Secure Firewall Management Center.

   For details about configuring Cisco ISE, see Configure ISE 3.0 REST ID with Azure Active Directory.

   Additional resource: Microsoft identity platform and OAuth 2.0 Resource Owner Password Credentials on learn.microsoft.com.

How Entra ID and Cisco ISE authentication works with TEAP/EAP-TLS

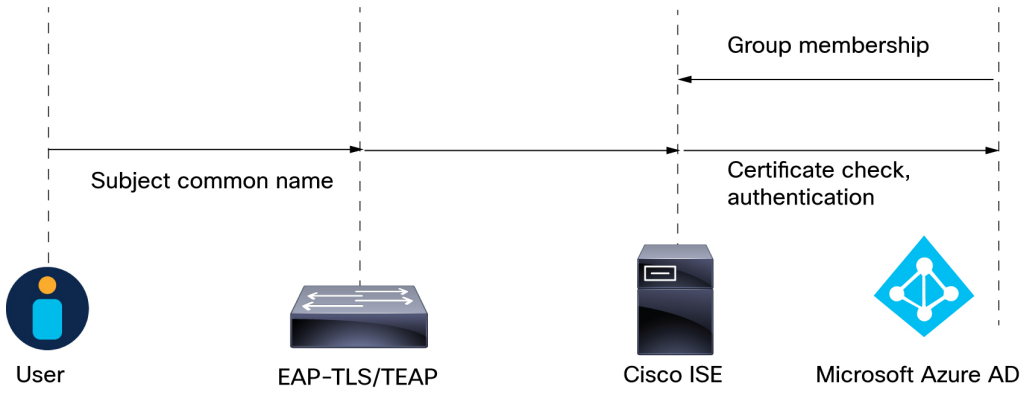
Tunnel Extensible Authentication Protocol (TEAP), defined by RFC7170, can be used with ISE and the Secure Firewall Management Center for secure authentication.

Summary

The key components involved in this authentication process are:

- User device: Provides certificate through EAP-TLS or TEAP protocol
- ISE: Validates certificate and performs user lookup through Azure Graph API
- Entra ID: Provides user attributes and group information for authorization

Workflow



These stages describe how the authentication process works and are based on Configure Cisco ISE 3.2 EAP-TLS with Microsoft Azure Active Directory:

1. The user's certificate is sent to ISE through EAP-TLS or TEAP with EAP-TLS as the inner method.
2. ISE evaluates the user's certificate (validity period, trusted certificate authority, certificate revocation list, and so on).

3. ISE takes the certificate subject name (CN) and performs a look-up to the Azure Graph API to fetch the user's groups and other attributes. This is referred to by Azure as User Principal name (UPN).
4. ISE authorization policies are evaluated against the user's attributes returned from Azure.

Create a Microsoft Azure AD realm

Create and configure a (now called *Entra ID*) realm for passive authentication use with the Secure Firewall Management Center.

This configuration enables passive authentication between Microsoft Entra ID and your firewall system through proper realm setup and access control policy integration.

Procedure

Step 1 Enable the Dynamic Attributes Connector.

The Dynamic Attributes Connector is required to use a realm. You can do it first or you can enable it when you create the realm. For more information, see Enable the dynamic attributes connector.

Step 2 Configure Microsoft Entra ID.

Several configuration tasks are required, including setting up an event hub, giving your application permission to the Microsoft Graph API, and enabling the audit log.

See Configure Microsoft Entra ID, on page 20.

Step 3 Configure Cisco ISE.

The way you configure ISE depends on how users authenticate with your system. For more information, see Configure Cisco ISE for Microsoft Azure AD, on page 21.

Step 4 Create a Cisco ISE identity source.

The identity source enables ISE to communicate with the Secure Firewall Management Center.

Step 5 Get the information required to configure your Microsoft Azure AD realm.

This information includes client and tenant IDs, client secret, and other information store in Microsoft Entra ID.

Step 6 Configure and verify your realm.

Test the realm's configuration before you start to use it in access control policies.

Step 7 Create access control policies and rules using your Microsoft Azure AD (SAML) realm.

Unlike other types of realms, you do not need to create an identity policy or associate the identity policy with an access control policy.

See Creating a basic access control policy and Create and edit access control rules.

What to do next

See How Entra ID and Cisco ISE authentication with resource owned password credentials works, on page 17.

Configure Microsoft Entra ID

Configure Microsoft Entra ID to enable passive authentication and user group synchronization with the Secure Firewall Management Center.

This task provides basic information about how to set up a Microsoft Entra ID (formerly called *Microsoft Azure Active Directory (AD)*) as a realm you can use with the Secure Firewall Management Center. We expect you to already be familiar with Entra ID; if not, consult documentation or a support resource before you get started.

Procedure

Step 1 Grant your Entra ID application the Microsoft Graph permissions.

Grant your Entra ID application the following permissions to Microsoft Graph as discussed in Authorization and the Microsoft Graph Security API on the Microsoft site:

- Reader role
- User.Read.All permission
- Group.Read.All permission

This permission enables the Secure Firewall Management Center to download users and groups from Entra ID the first time.

Required information from this step for setting up the Entra ID realm in the Secure Firewall Management Center:

- Name of the app you registered
- **Application (client) ID**
- **Client secret**
- **Directory (tenant) ID**

Step 2 Set up an event hub.

Set up the event hub as discussed in Quickstart: Create an event hub using Azure portal on the Microsoft site. The Secure Firewall Management Center uses the event hub audit log to download periodic updates to users and groups.

More information: Features and terminology in Azure Event Hubs.

Important
You must choose the **Standard** pricing tier or better. If you choose **Basic**, the realm cannot be used.

Required information from this step for setting up the Entra ID realm in the Secure Firewall Management Center:

- Namespace **Name**
- **Connection string—primary key**
- Event Hub **Name**
- Consumer group **Name**

Step 3 Enable the audit log.

Enable the audit log as discussed in Tutorial: Stream Azure Active Directory logs to an Azure event hub on the Microsoft site.

Step 4 Configure Cisco ISE for Entra ID.

To send user session information to the Secure Firewall Management Center, configure Cisco ISE for Entra ID as discussed in Configure ISE 3.0 REST ID with Azure Active Directory.

What to do next

See Configure Cisco ISE for Microsoft Azure AD, on page 21.

Configure Cisco ISE for Microsoft Azure AD

In a Microsoft Azure AD (now called *Entra ID*) realm, it's the responsibility of ISE to send user sessions (login, logout) to the Secure Firewall Management Center. This topic discusses how to set up ISE for use with an Azure AD realm.

Resource owned password credentials authentication

To use ISE with Microsoft Azure ADMicrosoft Azure AD implemented through Representational State Transfer (REST) Identity (ID) service with the help of Resource Owner Password Credentials (ROPC), see Configure ISE 3.0 REST ID with Azure Active Directory.

TEAP/EAP-TLS

To use ISE with authorization policies based on Azure AD group membership and other user attributes with EAP-TLS or TEAP as the authentication protocols, see Configure Cisco ISE 3.2 EAP-TLS with Microsoft Azure Active Directory.

What to do next

Get required information For Your Microsoft Azure AD realm, on page 21

Get required information For Your Microsoft Azure AD realm

This task enables you to collect the necessary credentials and configuration information from Microsoft Entra ID (formerly Azure AD) and Event Hubs to establish a SAML authentication realm in your Secure Firewall Management Center.

This task explains how to get the information required to set up a Microsoft Azure AD (now called *Entra ID*) realm in the Secure Firewall Management Center. You might have already obtained this information when you set up Microsoft Entra ID as discussed in Configure Microsoft Entra ID, on page 20.

Procedure

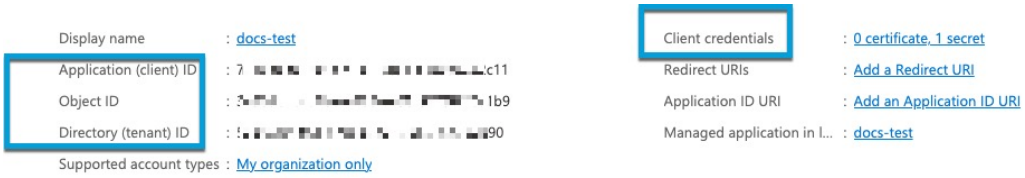
Step 1 Log in to https://portal.azure.com/ as a user with at least the Product Designer role.

Step 2 At the top of the page, click **Microsoft Entra ID**.

Step 3 In the left column, click **App Registrations**.

a) If necessary, filter the list of displayed apps to show the one you want to use.

b) Click the name of your app.



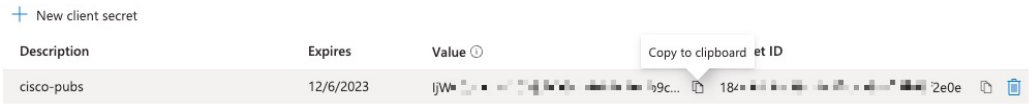
c) Click **Copy** ( ) next to the following values on this page and paste those values to a text file.

- **Application (Client) ID**
- **Directory (tenant) ID**

d) Click **Client Credentials**.

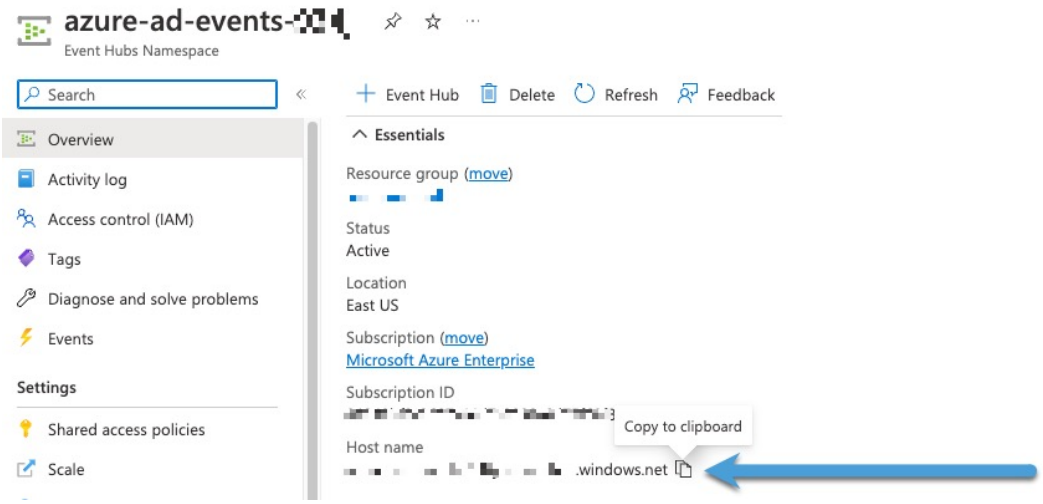
e) Unless you already know the client secret *value* (as opposed to the client *secret ID*), you must create a new client secret as follows:

1. Click **New Client Secret**.
2. Enter the required information in the provided fields.
3. Click **Add**.
4. Click **Copy** ( ) next to Value as the following figure shows.



Step 4 From https://portal.azure.com/, click **Event Hubs** > **(name of an event hub)**.

a) In the right pane, click **Copy** ( ) next to the value of **Host name** and paste the value to the clipboard. This is your event hub host name.

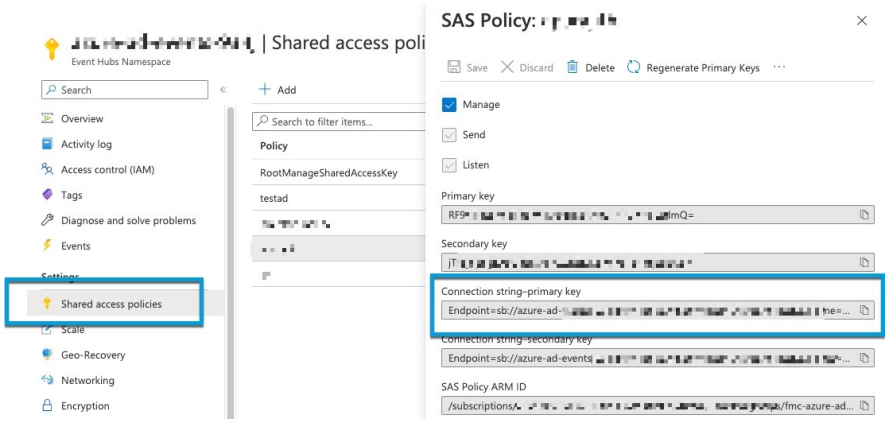


b) Write down or copy to a text file the name of the event hub (same as the **Event Hubs Namespace** at the top of the page).

c) In the left pane, under Settings, click **Shared access policies**.

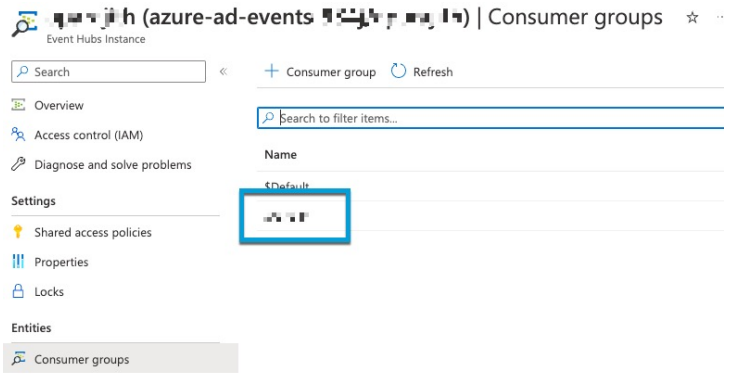
d) Click the name of a policy.

e) Click **Copy** ( ) next to **Connection string-primary key**.



Step 5 Click **Overview** > **Entities** > **Event Hubs** > **(name of an event hub)** > **Entities** > **Consumer Groups**.

Write down this value or copy it to the clipboard. This is your consumer group name.



Step 6 In the left pane, click **Overview**.

Step 7 Click **Copy** ( ) next to **Namespace**.



This is your event hubs topic name.

Create an Azure AD realm

This task creates a *realm* (a connection between the Firewall Management Center and a Microsoft Azure AD realm) to enable user and identity control through access control policies.

Note To perform user and identity control with an Azure AD realm, you need only an access control policy with an associated Azure AD realm. You do not need to create an identity policy.

Before you begin

Complete all of the following tasks:

- Configure ISE as discussed in Configure Cisco ISE for Microsoft Azure AD, on page 21
- Create an ISE identity source as discussed in ISE/ISE-PIC configuration
- Enable the Dynamic Attributes Connector as discussed in Enable the dynamic attributes connector .
- Get values required for the Azure AD realm as discussed in Get required information For Your Microsoft Azure AD realm, on page 21.
- Configure Azure AD as discussed in Configure Microsoft Entra ID, on page 20

Follow these steps to create an Azure AD realm:

Procedure

Step 1 Log in to Secure Firewall Management Center .

Step 2 Click **Integration** > **Other Integrations** > **Realms** > **Realms**.

Step 3 To create a new realm, click **Add Realm** > **Azure AD**.

Step 4 Enter the required information.

Item	Description
Name	
(Optional.) **Description**	
Client ID	Enter the information you found as discussed in Get required information For Your Microsoft Azure AD realm, on page 21.
Client Secret	
Tenant ID	
Event Hubs Host Name	
Event Hub Name	
Event Hub Connection String	
(Optional.) **Excluded User Groups**	Enter one or more groups from which to *not* download users for identity control. Users in these groups will not be available for use in access control policies. Enter one group name per line followed by a line break. Group names are case-sensitive.

Step 5 Enter the values you found as discussed in Get required information For Your Microsoft Azure AD realm, on page 21.

Step 6 Click **Test**.

Step 7 Fix any errors that are displayed in the test.

Step 8 Click **Save**.

What to do next

Create an access control policy and rule as discussed in Creating a basic access control policy.

Note Before deploying policies related to a Microsoft Azure AD realm, see User limits for microsoft azure active directory realms.

Azure AD user session timeout

Set the Entra ID user session timeout for ISE or ISE-PIC to define how long users stay authenticated, ensuring network access control after timeout via the User Session Timeout page when editing an Entra ID realm.

The Azure AD user session timeout for ISE/ISE-PIC is available on the **User Session Timeout** page when you edit an Azure AD realm.

The default value 1440 minutes (24 hours). After the timeout is exceeded, the user's session ends; if the user continues to access the network without logging in again, the user is seen by the Firewall Management Center as Unknown (except for **Failed Captive Portal Users**).

Create an LDAP realm or an Active Directory realm and realm directory

Before you begin

If you're using Kerberos authentication for captive portal, see the following section before you begin: Prerequisites for kerberos authentication, on page 9 .

Note Microsoft Azure Active Directory is not supported for captive portal.

Important To reduce latency between the Firewall Management Center and your Active Directory domain controller, we strongly recommend you configure a realm directory (that is, domain controller) that is as close as possible geographically to the Firewall Management Center.

For example, if your Firewall Management Center is in North America, configure a realm directory that is also in North America. Failure to do so can cause problems such as timeout downloading users and groups.

If you're setting up ISE/ISE-PIC without a realm, be aware there is a user session timeout that affects how users are seen by the Firewall Management Center. For more information, see Realm fields, on page 10.

The following procedure enables you to create a *realm* (a connection between the Firewall Management Center and an Active Directory realm) and a *directory* (a connection between the Firewall Management Center and an LDAP server or an Active Directory domain controller).

(Recommended.) To connect securely from the Firewall Management Center to your Active Directory server, first perform the following tasks:

- Export the active directory server's root certificate, on page 29
- Find the active directory server's name, on page 29

Microsoft has announced that Active Directory servers will start enforcing LDAP binding and LDAP signing in 2020. Microsoft is making these a requirement because when using default settings, an elevation of privilege vulnerability exists in Microsoft Windows that could allow a man-in-the-middle attacker to successfully forward an authentication request to a Windows LDAP server. For more information, refer to 2020 LDAP channel binding and LDAP signing requirement for Windows on the Microsoft support site.

For more information about realm and directory configuration fields, see Realm fields, on page 10 and Realm directory and synchronize fields, on page 14 .

A step-by-step example of setting up a realm with cross-domain trust is shown in Cross-domain trust setups with Firewall Management Center, on page 34 .

An Active Directory Global Catalog server is *not supported* as a realm directory. For more information about the Global Catalog Server, refer to Global Catalog on learn.microsoft.com.

Note You must specify a unique **AD Primary Domain** for every Microsoft Active Directory (AD) realm. Although the system allows you to specify the same **AD Primary Domain** for different Microsoft AD realms, the system won't function properly. This happens because system assigns a unique ID to every user and group in each *realm*; therefore, the system cannot definitively identify any particular user or group. The system prevents you from specifying more than one realm with the same **AD Primary Domain** because users and groups won't be identified properly. This happens because system assigns a unique ID to every user and group in each *realm*; therefore, the system cannot definitively identify any particular user or group.

Procedure

Step 1 Log in to the Secure Firewall Management Center. Click **Integration** > **Other Integrations** > **Realms** > **Realms**

Step 2 To create a new realm, choose from **Add Realm** drop-down list.

Step 3 To perform other tasks (such as enable, disable, or delete a realm), see Manage a realm, on page 42 .

Step 4 Enter realm information as discussed in Realm fields, on page 10 .

Step 5 In the Directory Server Configuration section, enter directory information as discussed in Realm directory and synchronize fields, on page 14 .

Step 6 (Optional.) To configure another domain for this realm, click **Add another directory** .

Step 7 Click **Configure Groups and Users** .

Information	Description
AD Primary Domain	Domain for the Active Directory server where users should be authenticated. For additional information, see Realm fields, on page 10 . You must create the realm with the original domain name of the domain and not any alternative user principal name (UPN) suffixes of the domain. Otherwise, users and groups fail to download and identity policies will not be enforced. For example, if the original domain is `domain.example.com` and the alternative UPN name is`domain2.mydomain.com`, you must configure the realm to use `domain.example.com`. For more information about configuring an alternative UPN suffix, see a resource like Configuring Alternate Login ID on learn.microsoft.com.
Base DN	The directory tree on the server where the Firewall Management Center should begin searching for user data.
Group DN	The directory tree on the server where the Firewall Management Center should begin searching for group data.

Information	Description
Load Groups	Click to load groups from the Active Directory server. If no groups are displayed, enter or edit information in the **AD Primary Domain** , **Base DN** , and **Group DN** fields and click **Load Groups** . For more information about those fields, see Realm fields, on page 10 .
Available Groups section	Limit the groups to use in policy by moving them to either the **Included Groups and Users** or **Excluded Groups and Users** list. Moving one group to the **Included Groups and Users** list, for example, allows that group only to be used in policy but excludes all other groups. Groups in the **Excluded Groups and Users** and the users they contain are excluded from user awareness and control. All other groups and users *are* available. For more information, see Realm directory and synchronize fields, on page 14 .

Configure the Realm

Before you begin

You must have created a new realm and its groups and users, as described in the prior procedure.

Procedure

Step 1 Click the **Realm Configuration** tab.

Step 2 Enter **Group Attribute** , and (if you use Kerberos authentication for captive portal) enter **AD Join Username** and **AD Join Password** . For more information, see Realm directory and synchronize fields, on page 14 .

Step 3 If you use Kerberos authentication, click **Test** . If the test fails, wait a short time and try again.

Step 4 Enter user session timeout values, in minutes, for **ISE/ISE-PIC Users** , **Terminal Server Agent Users** , **Captive Portal Users** , **Failed Captive Portal Users** , and **Guest Captive Portal Users** .

Step 5 When you're finished configuring the realm, click **Save** .

Connect securely to Active Directory or LDAP

To create a secure connection between an Active Directory or LDAP server and the Secure Firewall Management Center (which we strongly recommend), you must perform all of the following tasks:

- Export the server's *root* certificate.
- Import the root certificate into the Secure Firewall Management Center as a trusted CA certificate (**Objects** > **Object Management** > **PKI** > **Trusted CAs**).
- Find the server's fully qualified name.

- Create the realm directory.

Related Topics

Export the active directory server's root certificate, on page 29
Find the active directory server's name, on page 29
Create an LDAP realm or an Active Directory realm and realm directory, on page 26

Find the active directory server's name

Find the fully qualified server name in Microsoft Active Directory that you need to configure a realm directory.

To configure a realm directory in the Firewall Management Center, you must know the fully qualified server name, which you can find as discussed in the procedure that follows.

These tasks apply to Microsoft Active Directory only. If you use LDAP, consult an appropriate reference for the procedure.

Before you begin

You must log in to the Active Directory server as a user with sufficient privileges to view the computer's name.

Follow these steps to find the Active Directory server's name:

Procedure

Step 1 Log in to the Active Directory server.

Step 2 Click **Start**.

Step 3 Right-click **This PC**.

Step 4 Click **Properties**.

Step 5 Click **Advanced System Settings**.

Step 6 Click the **Computer Name** tab.

Step 7 Note the value of **Full computer name**.
You must enter this exact name when you configure the realm directory in the Firewall Management Center.

What to do next

Create an LDAP realm or an Active Directory realm and realm directory, on page 26.

Related Topics

Export the active directory server's root certificate, on page 29

Export the active directory server's root certificate

Export the Active Directory server's root certificate to enable secure connection to the Firewall Management Center for obtaining user identity information and authentication purposes.

The task that follows discusses how to export the Active Directory server's root certificate, which is required to connect securely to the Firewall Management Center to obtain user identity information.

These tasks apply to Microsoft Active Directory only. If you use LDAP, consult an appropriate reference for the procedure.

Before you begin

You must know the name of your Active Directory server's root certificate. The root certificate might have the same name as the domain or the certificate might have a different name. The procedure that follows shows one way you can find the name; there could be other ways, however.

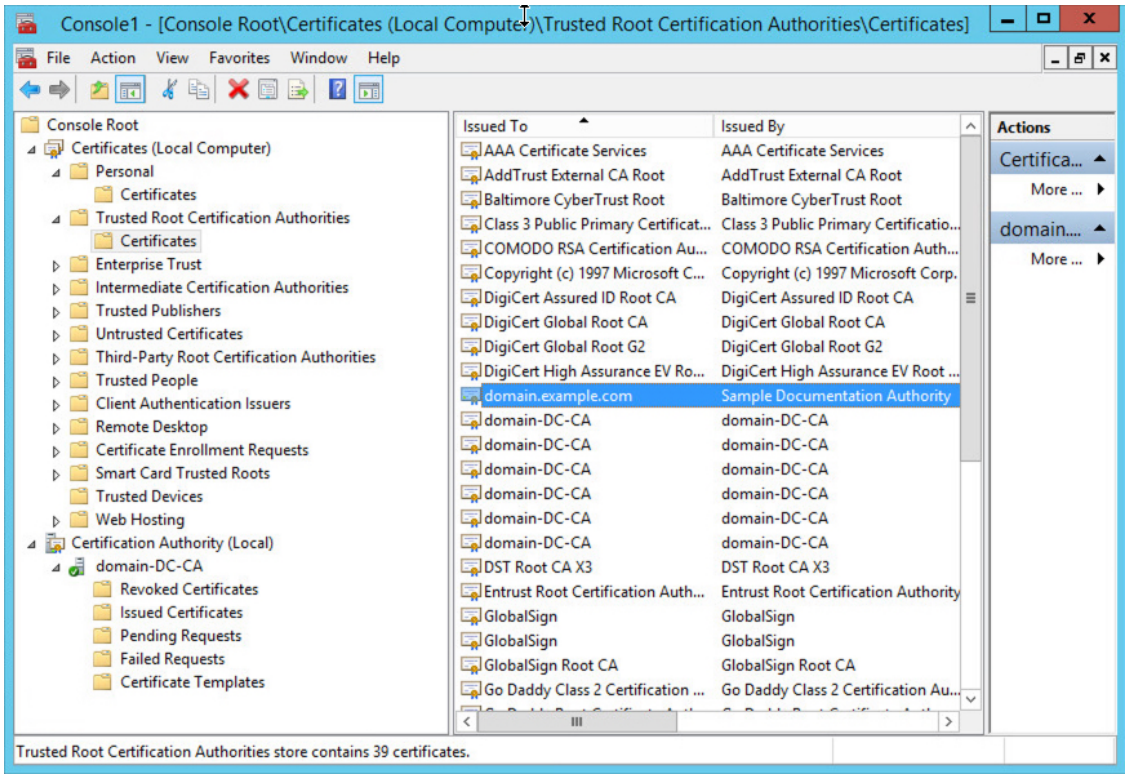
Follow these steps to export the Active Directory server's root certificate:

Procedure

Step 1 Find the name of the Active Directory Server's root certificate using the Microsoft Management Console.

This is one way to find the name of the Active Directory Server's root certificate; consult Microsoft documentation for more information:

a) Log in to the Active Directory server as a user with privileges to run the Microsoft Management Console.
b) Click **Start** and enter **mmc**.
c) Click **File** > **Add/Remove Snap-in**
d) From the Available Snap-ins list in the left pane, click **Certificates (local)**.
e) Click **Add**.
f) At the Certificates snap-in dialog box, click **Computer Account** and click **Next**.
g) At the Select Computer dialog box, click **Local Computer** and click **Finish**.
h) *Windows Server 2012 only*. Repeat the preceding steps to add the Certification Authority snap-in.
i) Click **Console Root** > **Trusted Certification Authorities** > **Certificates**.
The server's trusted certificates are displayed in the right pane. The following figure is only an example for Windows Server 2012; yours will probably look different.



Step 2 Export the certificate using the **certutil** command.

This is only one way to export the certificate. It is a convenient way to export the certificate, especially if you can run a web browser and connect to the Firewall Management Center from the Active Directory server.

a) Click **Start** and enter **cmd**.
b) Enter the command **certutil -CA.cert** *certificate-name*.
The server's certificate is displayed on the screen.
c) Copy the entire certificate to the clipboard, starting with **-----BEGIN CERTIFICATE-----** and ending with **-----END CERTIFICATE-----** (including those strings).

What to do next

Import the Active Directory server's certificate into the Firewall Management Center as a trusted CA certificate as discussed in Add a trusted CA object.

Related Topics

Find the active directory server's name, on page 29

Synchronize users and groups

This task synchronizes users and groups from Active Directory domains to enable their use in identity policies.

Synchronizing users and groups means the Firewall Management Center queries the realms and directories you configured for groups and users in those groups. All users the Firewall Management Center finds can be used in identity policies.

If issues are found, you most likely need to add a realm that contains users and groups the Firewall Management Center cannot load. For details, see Realms and trusted domains, on page 3.

Before you begin

Create a Secure Firewall Management Center *realm* for each Active Directory domain and a Firewall Management Center *directory* for each Active Director domain controller in each forest. See Create an LDAP realm or an Active Directory realm and realm directory, on page 26.

Note Synchronizing users and groups is not necessary for Microsoft Azure AD realms.

You must create a realm only for domains that have users you want to use in user control.

You can nest Microsoft AD groups and the Firewall Management Center downloads those groups and the users they contain. You can optionally restrict which groups and users get downloaded as discussed in Create an LDAP realm or an Active Directory realm and realm directory, on page 26.

You must create the realm with the original domain name of the domain and not any alternative user principal name (UPN) suffixes of the domain. Otherwise, users and groups fail to download and identity policies will not be enforced. For example, if the original domain is `domain.example.com` and the alternative UPN name is`domain2.mydomain.com`, you must configure the realm to use `domain.example.com`. For more information about configuring an alternative UPN suffix, see a resource like Configuring Alternate Login ID on learn.microsoft.com.

Follow these steps to synchronize users and groups:

Procedure

Step 1 Log in to the Secure Firewall Management Center if you have not already done so.

Step 2 Click **Integration** > **Other Integrations** > **Realms** > **Realms**.

Step 3 Next to each realm, click **Download** ( ).

Step 4 To see the results, click the **Sync Results** tab.
The Realms column indicates whether or not there were issues synchronizing users and groups in Active Directory forests. Look for the following indicators next to each realm.

Indicator in Realms column	Meaning
(nothing)	All users and groups synchronized without error. No action is necessary.

Indicator in Realms column	Meaning
Yellow Triangle ( )	There were issues synchronizing users and groups. Make sure you added a realm for each Active Directory domain and a directory for each Active Directory domain controller. For more details, see Troubleshoot cross-domain trust, on page 48.

Create a realm sequence

Creating a realm sequence provides an ordered list of realms the system searches when it applies identity policy, allowing you to specify the priority order for user authentication across multiple Active Directory servers.

The following procedure enables you to create a realm sequence, which is an ordered list of realms the system searches when it applies identity policy. You add a realm sequence to an identity rule exactly the same way as you add a realm; the difference is that the system searches all the realms in the order specified in the realm sequence when applying an identity policy.

Before you begin

You must create and enable at least two realms, each corresponding to a connection with an Active Directory server. You cannot create realm sequences for LDAP realms.

Create a realm as discussed in Create an LDAP realm or an Active Directory realm and realm directory, on page 26.

Follow these steps to create a realm sequence:

Procedure

Step 1 Log in to the Secure Firewall Management Center if you have not already done so and click **Integration** > **Other Integrations** > **Realms** > **Realm Sequences**.

Step 2 Under the **Realm Sequences** tab, click **Add Sequence**.

Step 3 In the **Name** field, enter a name to identify the realm sequence.

Step 4 (Optional.) In the **Description** field, enter a description for the realm sequence.

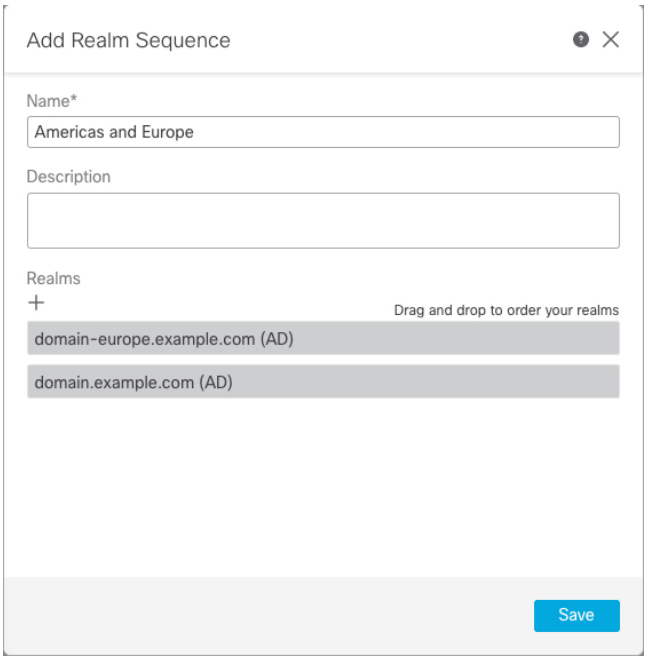
Step 5 Under Realms, click **Add** ( ).

Step 6 Click the name of each realm to add to the sequence.

To narrow your search, enter all or part of a realm name in **Filter** field.

Click **OK**.

Step 7 In the Add Realm Sequence dialog box, drag and drop the realms in the order in which you want the system to search for them.
The following figure shows an example of a realm sequence consisting of two realms. The **domain-europe.example.com** realm will be searched for users before the **domain.example.com** realm.



Step 8 Click **Save**.

What to do next

See Create an identity policy.

Cross-domain trust setups with Firewall Management Center

A cross-domain trust setup allows discovery and use of users and groups from multiple domains in access control policies.

This is an introduction to several topics that walk you through configuring the Firewall Management Center with two realms having cross-domain trust.

Example setup configuration

This step-by-step example involves two forests: **forest.example.com** and **eastforest.example.com**. The forests are configured so that certain users and groups in each forest can be authenticated by Microsoft AD in the other forest.

Note This topic applies to Microsoft AD realms only. It does *not* apply to Microsoft Azure AD realms.

The example setup uses this configuration:



Using this example, you would set up the Firewall Management Center with these components:

- Realm and directory for any domain in **forest.example.com** that contains users you want to control with access control policy
- Realm and directory for any domain in **eastforest.example.com** that contains users you want to control with access control policy

Each realm in the example has one domain controller, which is configured in the Firewall Management Center as a directory. The directories in this example are configured as follows:

- **forest.example.com**
  - Base distinguished name (DN) for users: **ou=UsersWest,dc=forest,dc=example,dc=com**
  - Base DN for groups: **ou=EngineringWest,dc=forest,dc=example,dc=com**
- **eastforest.example.com**
  - Base DN for users: **ou=EastUsers,dc=eastforest,dc=example,dc=com**
  - Base DN for groups: **ou=EastEngineering,dc=eastforest,dc=example,dc=com**

Related Topics

Configure Secure Firewall Management Center for cross-domain-trust step 1: Configure realms and directories, on page 35

Configure Secure Firewall Management Center for cross-domain-trust step 1: Configure realms and directories

This task configures the Firewall Management Center to recognize Active Directory servers in a cross-domain trust relationship, enabling the discovery and use of users and groups from multiple domains in access control policies.

This is the first task in a step-by-step procedure that explains how to configure the Firewall Management Center to recognize Active Directory servers configured in a cross-domain trust relationship, which is an increasingly common configuration for enterprise organizations. For an overview of this sample configuration, see Cross-domain trust setups with Firewall Management Center, on page 34.

If you set up the system with one realm for each domain and one directory for each domain controller, the system can discover up to 100,000 foreign security principals (users and groups). If these foreign security principals match a user downloaded in another realm, then they can be used in access control policy.

Before you begin

You must configure Microsoft Active Directory servers in a cross-domain trust relationship; see Realms and trusted domains, on page 3 for more information.

If you authenticate users with LDAP or Microsoft Azure AD, you *cannot* use this procedure.

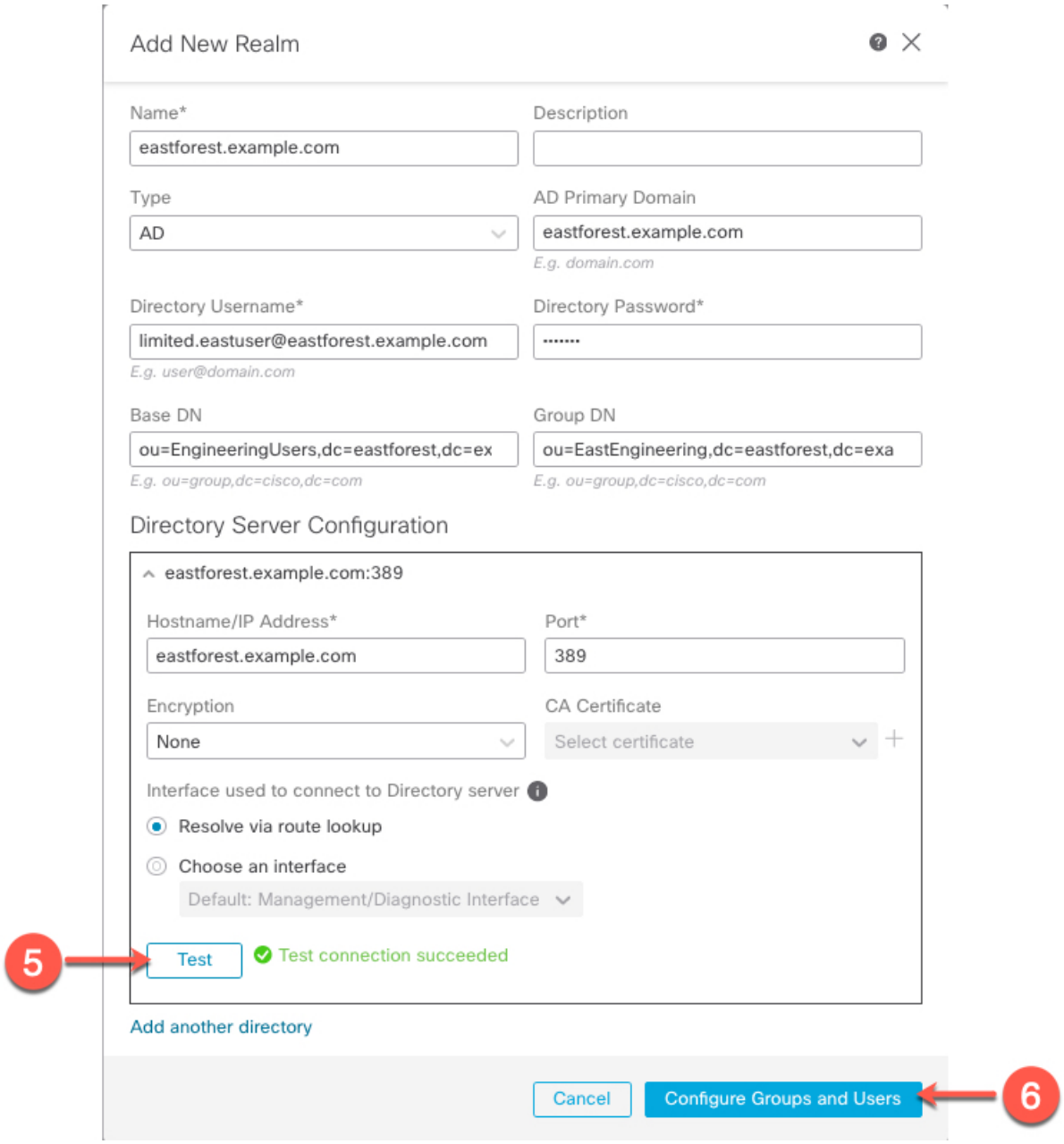
Procedure

Step 1 Log in to the Secure Firewall Management Center if you have not already done so.

Step 2 Click **Integration** > **Other Integrations** > **Realms** > **Realms**.

Step 3 Click **Add Realm** > **Active Directory/LDAP**.

Step 4 Enter the following information to configure **forest.example.com**.



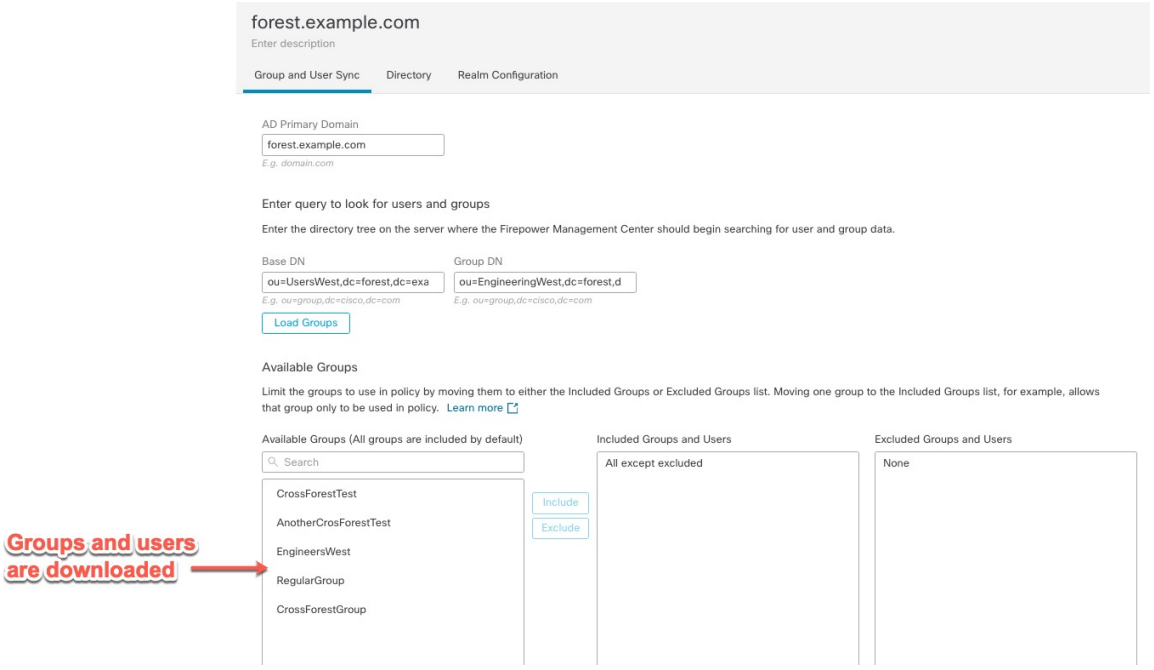
Note
The **Directory Username** can be any user in the Active Directory domain; no special permissions are required.

The **Interface used to connect to Directory server** can be any interface that can connect to the Active Directory server.

Step 5 Click **Test** and make sure the test succeeds before you continue.

Step 6 Click **Configure Groups and Users**.

Step 7 Verify your configuration was successful by checking that the next page is displayed similar to the following.



Note
If groups and users were not downloaded, verify the values in the **Base DN** and **Groups DN** fields and click **Load Groups**.

There are other optional configurations available on this page; for more information about them, see Realm fields, on page 10 and Realm directory and synchronize fields, on page 14.

Step 8 If you made changes on this page or tab pages, click **Save**.

Create another realm

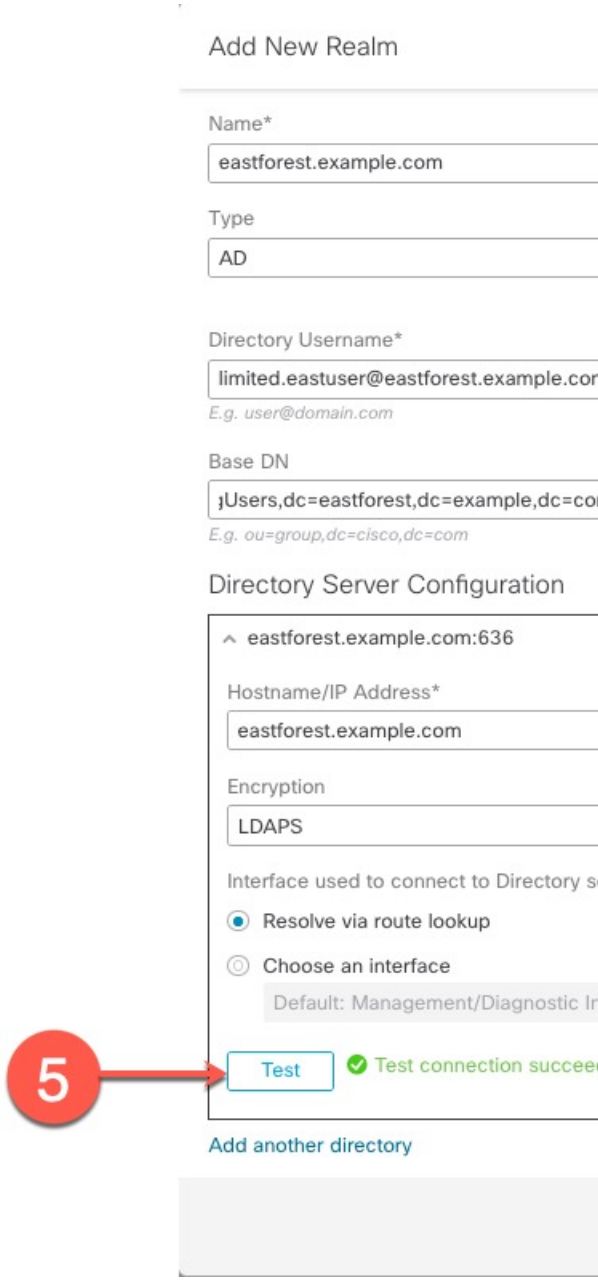
Before you begin

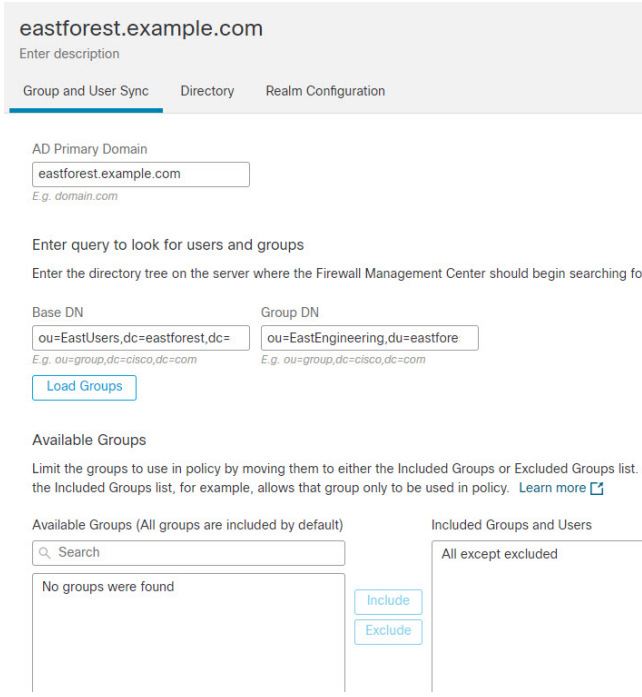
Complete the configuration of your first realm as in the prior task.

Follow these steps to create another realm.

Procedure

	Command or Action	Purpose
Step 1	Click **Integration** > **Other Integrations** > **Realms** > **Realms**.	
Step 2	Click **Add Realm**.	

	Command or Action	Purpose
Step 3	Enter the following information to configure **eastforest.example.com**.	
Step 4	Click **Test** and make sure the test succeeds before you continue.	
Step 5	Click **Configure Groups and Users**.	

	Command or Action	Purpose
Step 6	Verify your configuration was successful by checking that the next page is displayed similar to the following.	

You have successfully configured two realms (**forest.example.com** and **eastforest.example.com**) with their respective directories.

Configure the Secure Firewall Management Center for cross-domain trust Step 2: Synchronize users and groups

This task allows you to download users and groups from Active Directory servers with cross-domain trust relationships to synchronize identity data in the Secure Firewall Management Center and resolve download issues by verifying directory setup and device communication.

After you configure two or more Active Directory servers that have a cross-domain trust relationship, you must download users and groups. That process exposes possible issues with the Active Directory configuration (for example, groups or users downloaded for one Active Directory domain but not the other).

Before you begin

Make sure you have performed the tasks discussed in Configure Secure Firewall Management Center for cross-domain-trust step 1: Configure realms and directories, on page 35.

Procedure

Step 1 Log in to the Secure Firewall Management Center if you have not already done so.

Step 2 Click **Integration** > **Other Integrations** > **Realms** > **Realms**.

Step 3 At the end of the row of any realm in the cross-domain trust, click **Download Now**( ), then click **Yes**.

Step 4 Click **Check Mark** ( ) (Notifications) > **Tasks**.

If groups and users fail to download, try again. If subsequent attempts fail, review your realm and directory setup as discussed in Realm fields, on page 10 and Realm directory and synchronize fields, on page 14.

Step 5 Click **Integration** > **Other Integrations** > **Realms** > **Sync Results**.

Related Topics

Configure the Secure Firewall Management Center for cross-domain trust step 3: Resolve issues, on page 41

Configure the Secure Firewall Management Center for cross-domain trust step 3: Resolve issues

This task enables you to make sure users and groups are downloaded without errors during cross-domain trust setup.

The final step in setting up cross-domain trust in the Firewall Management Center is to make sure users and groups are downloaded without errors. A typical reason why users and groups do not download properly is that the realms to which they belong have not been downloaded to the Firewall Management Center.

This topic discusses how to diagnose that a group referred in one forest to cannot be downloaded because the realm is not configured to find the group in the domain controller hierarchy.

Procedure

Step 1 Log in to the Secure Firewall Management Center if you have not already done so.

Step 2 Click **Integration** > **Other Integrations** > **Realms** > **Realms**.

In the Realms column, if **Yellow Triangle** ( ) is displayed next to the name of a realm, you have issues that must be resolved. If not, your results are configured properly and you can quit.

Step 3 Download users and groups again from the realms that display issues.

a) Click the **Realms** tab.

b) Click (Download Now), then click **Yes**.

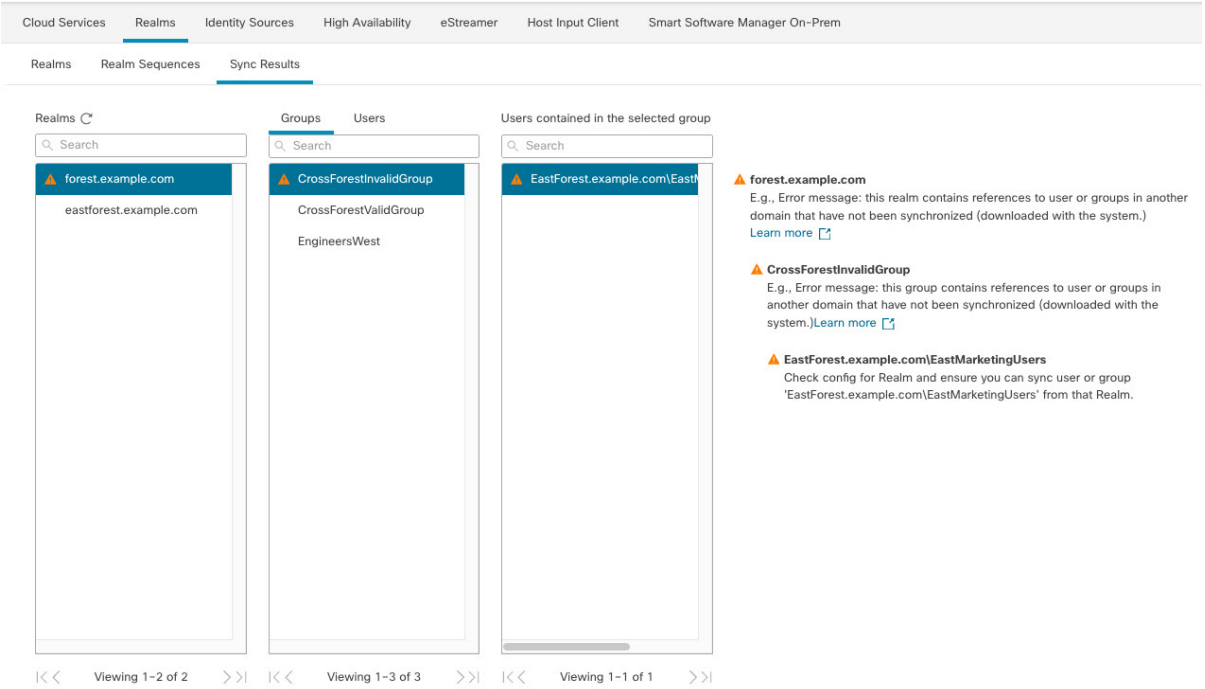
Step 4 Click the **Sync Results** tab page.

If the **Yellow Triangle** ( ) is displayed in the Realms column, click **Yellow Triangle** ( ) next to the realm that has issues.

Step 5 In the middle column, click either **Groups** or **Users** to find more information.

Step 6 In the Groups or Users tab page, click **Yellow Triangle** ( ) to display more information.

The right column should display enough information you can isolate the source of the issue.



In the preceding example, **forest.example.com** includes a cross-domain group **CrossForestInvalidGroup** that contains another group **EastMarketingUsers** that was not downloaded by the Firewall Management Center. If, after synchronizing the **eastforest.example.com** realm again, the error does not resolve, it likely means that the Active Directory domain controller does not include **EastMarketingUsers**.

To resolve this issue, you can:

- Remove the **EastMarketingUsers** from **CrossForestInvalidGroup**, synchronize the **forest.example.com** realm again, and recheck.
- Remove the **ou=EastEngineering** value from the **Group DN** of the **eastforest.example.com** realm, which causes the Firewall Management Center to retrieve groups from the highest level in the Active Directory hierarchy, synchronize **eastforest.example.com**, and recheck.

Manage a realm

This task enables you to perform various maintenance operations on realms to manage authentication and user access control.

This section discusses how to perform various maintenance tasks for a realm using controls on the Realms page:

If the controls are dimmed, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.. If **View** ( ) appears instead, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.

Procedure

Step 1 Log in to the Secure Firewall Management Center if you have not already done so. Click **Integration** > **Other Integrations** > **Realms** > **Realms**.

Step 2 To delete a realm, click **Delete** ( ).

Step 3 To edit a realm, click **Edit** ( ) next to the realm and make changes as described in Create an LDAP realm or an Active Directory realm and realm directory, on page 26.

Step 4 To enable a realm, slide **State** to the right; to disable a realm, slide it to the left.

Step 5 To download users and user groups, click **Download** ( ).

Step 6 To copy a realm, click **Copy** ( ).

Step 7 To compare realms, see Compare realms, on page 43.

Compare realms

Use this task to compare identity realms in the Secure Firewall Management Center to review differences between selected realms, generate comparison reports, and analyze changes to support identity integration management.

You must be an Admin, Access Admin, Network Admin, or Security Approver to perform this task.

Procedure

Step 1 Log in to the Secure Firewall Management Center if you have not already done so. Click **Integration** > **Other Integrations** > **Realms** > **Realms**.

Step 2 Click **Compare Realms**.

Step 3 Choose **Compare Realm** from the **Compare Against** list.

Step 4 Choose the realms you want to compare from the **Realm A** and **Realm B** lists.

Step 5 Click **OK**.

Step 6 To navigate individually through changes, click **Previous** or **Next** above the title bar.

Step 7 (Optional.) Click **Comparison Report** to generate the realm comparison report.

Step 8 (Optional.) Click **New Comparison** to generate a new realm comparison view.

Troubleshoot realms and user downloads

If you notice unexpected server connection behavior, consider tuning your realm configuration, device settings, or server settings. For other related troubleshooting information, see:

- Troubleshoot Cisco ISE/ISE-PIC or Cisco TrustSec issues
- Troubleshoot the TS agent identity source
- Troubleshoot the captive portal identity source
- Troubleshooting guidelines for remote access VPN identity source
- Troubleshoot user control

Realms and groups reported but not downloaded

The Secure Firewall Management Center's health monitor informs you of user or realm mismatches, which are defined as:

- User mismatch: A user is reported to the Secure Firewall Management Center without being downloaded.

  A typical reason for a user mismatch is that the user belongs to a group you have excluded from being downloaded to the Secure Firewall Management Center. Review the information discussed in *Cisco Secure Firewall Management Center Device Configuration Guide*.

- Realm mismatch: A user logs into a domain that corresponds to a realm not known to the Firewall Management Center.

For example, if you defined a realm that corresponds to a domain named **domain.example.com** in the Firewall Management Center but a login is reported from a domain named **another-domain.example.com**, this is a *realm mismatch*. Users in this domain are identified by the Firewall Management Center as Unknown.

You set the mismatch threshold as a percentage, above which a health warning is triggered. Examples:

- If you use the default mismatch threshold of 50%, and there are two mismatched realms in eight incoming sessions, the mismatch percentage is 25% and no warning is triggered.
- If you set the mismatch threshold to 30% and there are three mismatched realms in five incoming sessions, the mismatch percentage is 60% and a warning is triggered.

Unknown users that do not match identity rules have no policies applied to them. (Although you can set up identity rules for Unknown users, we recommend keeping the number of rules to a minimum by identifying users and realms correctly.)

For more information, see Detect realm or user mismatches, on page 47.

Users are not downloaded

Possible causes include:

- If you have the realm **Type** configured incorrectly, users and groups cannot be downloaded because of a mismatch between the attribute the system expects and what the repository provides. For example, if you configure **Type** as **LDAP** for a Microsoft Active Directory realm, the system expects the `uid` attribute, which is set to `none` on Active Directory. (Active Directory repositories use `sAMAccountName` for the user ID.)

  Solution: Set the realm **Type** field appropriately: **AD** for Microsoft Active Directory or **LDAP** for another supported LDAP repository.

- Users in Active Directory groups that have special characters in the group or organizational unit name might not be available for identity policy rules. For example, if a group or organizational unit name

contains the characters asterisk (*), equals (=), or backslash (\), users in those groups are not downloaded and can't be used for identity policies.

Solution: Remove special characters from the group or organizational unit name.



Important To reduce latency between the Firewall Management Center and your Active Directory domain controller, we strongly recommend you configure a realm directory (that is, domain controller) that is as close as possible geographically to the Firewall Management Center.

For example, if your Firewall Management Center is in North America, configure a realm directory that is also in North America. Failure to do so can cause problems such as timeout downloading users and groups.

Not all users in a realm are downloaded

Possible causes include:

- If you attempt to download more than the maximum number of users in any one realm, the download stops at the maximum number of users and a health alert is displayed. User download limits are set per Secure Firewall Management Center model. For more information, see User limits for microsoft active directory.
- Every user must be a member of a group. Users that are members of no groups do not get downloaded.

Access control policy doesn't match group membership

This solution applies to an AD domain that is in a trust relationship with other AD domains. In this discussion, *external domain* means a domain other than the one to which the user logs in.

If a user belongs to a group defined in a trusted external domain, the Secure Firewall Management Center doesn't track membership in the external domain. For example, consider this scenario:

- Domain controllers 1 and 2 trust each other
- Group A is defined on domain controller 2
- User `mparvinder` in controller 1 is a member of Group A

Even though user `mparvinder` is in Group A, the Secure Firewall Management Center access control policy rules specifying membership Group A don't match.

Solution: Create a similar group in domain controller 1 that contains has all domain 1 accounts that belong to group A. Change the access control policy rule to match any member of Group A or Group B.

Access control policy doesn't match child domain membership

If a user belongs to a domain that is child of parent domain, Firepower doesn't track the parent/child relationships between domains. For example, consider this scenario:

- Domain `child.parent.com` is child of domain `parent.com`
- User `mparvinder` is defined in `child.parent.com`

Even though user `mparvinder` is in a child domain, the Firepower access control policy matching the `parent.com` don't match `mparvinder` in the `child.parent.com` domain.

Solution: Change the access control policy rule to match membership in either `parent.com` or `child.parent.com`.

Realm or realm directory test fails

The **Test** button on the directory page sends an LDAP query to the hostname or IP address you entered. If it fails, check these items:

- The **Hostname** you entered resolves to the IP address of an LDAP server or Active Directory domain controller.
- The **IP Address** you entered is valid.

The **Test AD Join** button on the realm configuration page verifies these items:

- DNS resolves the **AD Primary Domain** to an LDAP server or Active Directory domain controller's IP address.
- The **AD Join Username** and **AD Join Password** are correct.

  AD Join Username must be fully qualified (for example, **`administrator@mydomain.com`**, *not* **`administrator`**).
- The user has sufficient privileges to create a computer in the domain and join the Secure Firewall Management Center to the domain as a Domain Computer.

User timeouts are occurring at unexpected times

If you notice the system performing user timeouts at unexpected intervals, confirm that the time on your ISE/ISE-PIC server is synchronized with the time on the Secure Firewall Management Center. If the appliances are not synchronized, the system may perform user timeouts at unexpected intervals.

If you notice the system performing user timeouts at unexpected intervals, confirm that the time on your ISE/ISE-PIC, or TS Agent server is synchronized with the time on the Secure Firewall Management Center. If the appliances are not synchronized, the system may perform user timeouts at unexpected intervals.

User data for previously-unseen ISE/ISE-PIC users is not displaying in the web interface

After the system detects activity from an ISE/ISE-PIC or TS Agent user whose data is not yet in the database, the system retrieves information about them from the server. In some cases, the system requires additional time to successfully retrieve this information from Microsoft Windows servers. Until the data retrieval succeeds, activity seen by the ISE/ISE-PIC, or TS Agent user is *not* displayed in the web interface.

Note that this can also prevent the system from handling the user's traffic using access control rules.

User data in events is unexpected

If you notice user or user activity events contain unexpected IP addresses, check your realms. The system does not support configuring multiple realms with the same **AD Primary Domain** value.

Users originating from terminal server logins are not uniquely identified by the system

If your deployment includes a terminal server and you have a realm configured for one or more servers connected to the terminal server, you must deploy the Cisco Terminal Services (TS) Agent to accurately report user logins in terminal server environments. When installed and configured, the TS Agent assigns unique ports to individual users so the system can uniquely identify those users in the web interface.

For more information about the TS Agent, see the *Cisco Terminal Services (TS) Agent Guide*.

Detect realm or user mismatches

Detection of realm or user mismatches helps ensure accurate user identification and proper policy application in the Cisco Secure Firewall Management Center.

This section discusses how to detect realm or user *mismatches*, which are defined as:

- User mismatch: A user is reported to the Secure Firewall Management Center without being downloaded.

  A typical reason for a user mismatch is that the user belongs to a group you have excluded from being downloaded to the Secure Firewall Management Center. Review the information discussed in *Cisco Secure Firewall Management Center Device Configuration Guide*.

- Realm mismatch: A user logs into a domain that corresponds to a realm not known to the Firewall Management Center.

For additional details, see Troubleshoot realms and user downloads, on page 43.

Unknown users that do not match identity rules have no policies applied to them. (Although you can set up identity rules for Unknown users, we recommend keeping the number of rules to a minimum by identifying users and realms correctly.)

Procedure

Step 1 Enable detection of realm or user mismatches:

a. Log in to the Firewall Management Center if you have not already done so.

b. Click **System** (⚙) > **Health** > **Policy**.

c. Create a new health policy or edit an existing one.

d. On the Editing Policy page, set a **Policy Runtime Interval**.

This is the frequency at which all health monitor tasks run.

e. In the left pane, click **Realm**.

f. Enter the following information:

- **Enabled**: Click **On**
- **Warning Users match threshold %**: The percentage of either realm mismatches or user mismatches that triggers a warning in the Health Monitor. For more information, see Troubleshoot realms and user downloads, on page 43.

g. At the bottom of the page, click **Save Policy & Exit**.

h. Apply the health policy to managed devices as discussed in *Applying Health Policies* in the *Cisco Secure Firewall Management Center Administration Guide*.

Step 2 View user and realm mismatches in any of the following ways:

- If the warning threshold is exceeded, click **Warning** > **Health** in the top navigation of the Firewall Management Center. This opens the Health Monitor.
- Click **System** (⚙) > **Health** > **Monitor**.

Step 3 On the Health Monitor page, in the Display column, expand **Realm: Domain** or **Realm: User** to view details about the mismatch.

Troubleshoot cross-domain trust

Troubleshoot user and group synchronization issues in the Secure Firewall Management Center configuration for cross-domain trust. This reference provides information on typical issues, error interpretation, and resolution steps for Active Directory forest synchronization problems.

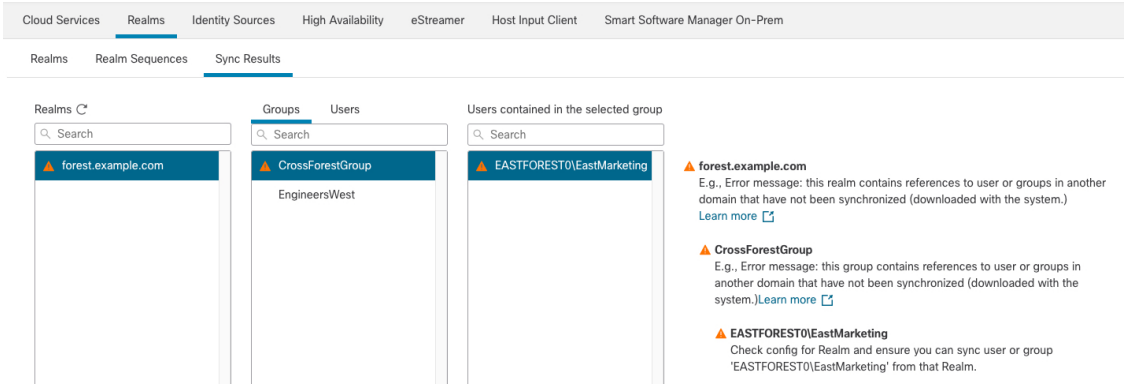
Typical issues

Typical issues with troubleshooting the Secure Firewall Management Center configuration for cross-domain trust include these items:

- Not adding realms or directories for all forests that have shared groups.
- Configure a realm to exclude users from being downloaded and those users are referenced in a group in a different realm.
- Certain temporary issues.

Understand the issues

If there are issues with the Firewall Management Center being able to synchronize users and groups with your Active Directory forests, the Sync Results tab page is displayed similar to this.



This table explains how to interpret the information.

Column	Meaning
Realms	Displays all realms configured in the system. Click **Refresh** ( ) to update the list of realms. **Yellow Triangle** ( ) is displayed to indicate issues in the realm. Nothing is displayed next to a realm if all users and groups synchronized successfully.
Groups	Click **Groups** to display all groups in the realm. As with realms, **Yellow Triangle** ( ) is displayed to indicate issues. Click **Yellow Triangle** ( ) to see more detail about the issue.
Users	Click **Users** to display all users, sorted by group.
Users contained in the selected group	Displays all users in the group you selected in the Groups column. Clicking **Yellow Triangle** ( ) displays more information to the right of the table.
Groups that contain selected user	Displays all groups the selected user belongs to. Clicking **Yellow Triangle** ( ) displays more information to the right of the table.
Error detail information (displayed to the right of the table).	The system displays the NetBIOS forest name and group name it could not synchronize. Typical reasons the system cannot synchronize these users and groups follow: • **Problem**: The forest containing the groups and users do not have corresponding realms configured in the Firewall Management Center. **Solution**: Add a realm for the forest that contains the group as discussed in Create an LDAP realm or an Active Directory realm and realm directory, on page 26. • **Problem**: You excluded groups from being downloaded to the Firewall Management Center. **Solution**: Click the **Realms** tab page, click **Edit** ( ), then move the indicated group or user from the **Excluded Groups and Users** list.

Try downloading users and groups again

If there is a possibility the issues are temporary, download users and groups for all realms.

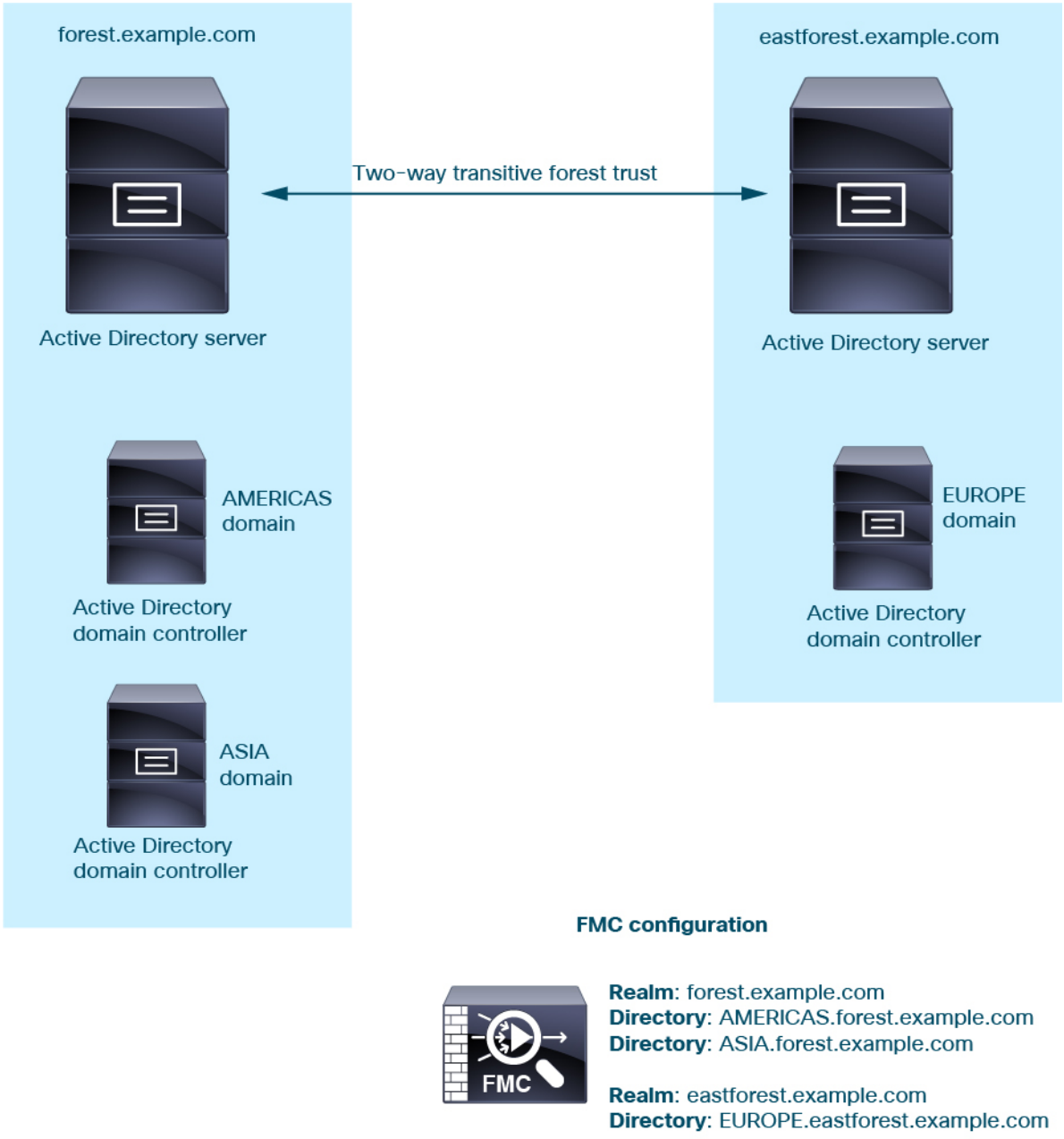
1. If you haven't done so already, log in to the Firewall Management Center.
2. Click **Integration** > **Other Integrations** > **Realms** > **Realms**.
3. Click **Download** ( ).
4. Click the **Sync Results** tab page.
5. If no indicator is displayed for entries in the Realms column, the issues have been resolved.

Add a realm for all forests

Make sure you configured:

- Firewall Management Center realm for each forest that has users you want to use in identity policies.
- Firewall Management Center directory for each domain controller in that forest with users you want to use in identity polices.

This figure shows an example.



History for realms

This reference provides the version history and implementation details for realm-related features across different versions of the Cisco security platform.

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Microsoft Azure Active Directory (AD) realms.	7.4.0	7.4.0	You can use a Microsoft Azure Active Directory (AD) realm with ISE to authenticate users and get user sessions for user control. New/modified screens: **System** > **Integration** > **Realms** > **Add Realm** > **Azure AD**
Proxy sequences.	7.2.0	7.2.0	Similar to a realm sequence, a proxy sequence is one or more managed devices that can communicate with Security Cloud Control in the event Security Cloud Control cannot communicate with the LDAP or Active Directory server. New/modified screens: **Integration** > **Other Integrations** > **Realms** > **Proxy Sequence**
Cross-domain trust for Active Directory domains.	7.2.0	7.0.0	A grouping of Microsoft Active Directory (AD) domains that trust each other is commonly referred to as a *forest*. This trust relationship can enable domains to access each other's resources in different ways. For example, a user account defined in domain A can be marked as a member of a group defined in domain B. The Firewall Management Center can get users from Active Directory forests for identity rules.
Realm sequences.	7.2.0	6.7.0	A *realm sequence* is an ordered list of two or more realms to which to apply identity rules. When you associate a realm sequence with an identity policy, the Firepower System searches the Active Directory domains in order from first to last as specified in the realm sequence. New/modified screens: **Integration** > **Other Integrations** > **Realms** > **Realm SequencesSystem** > **Integration** > **Realms** > **Realm Sequences**
Realms for user control.	7.2.0	Any	A realm is a connection between the Firewall Management Center either an Active Directory or LDAP user repository.