Realms

The following topics describe realms and identity policies:

License Requirements for 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

Create a Proxy Sequence

A *proxy sequence* is one or more managed devices that can be used to communicate with an LDAP, Active Directory, or ISE/ISE-PIC server. It is necessary only if Security Cloud Control cannot communicate with your Active Directory or ISE/ISE-PIC server. (For example, Security Cloud Control might be in a public cloud but Active Directory or ISE/ISE-PIC might be in a private cloud.)

Although you can use one managed device as a proxy sequence, we strongly recommend you set up two or more so that, in the event one managed device cannot communicate with Active Directory or ISE/ISE-PIC, another managed device can take over.

Note To use a proxy sequence with a SAML - Azure AD realm, the managed device must run version 7.4.2 or later.

Before you begin

You must add at least two managed devices to Security Cloud Control, all of which must be able to communicate with Active Directory or ISE/ISE-PIC.

Procedure

Step 1 Log in to the Security Cloud Control if you have not already done so.

Step 2 Click **Policies** > **Firewall Threat Defense** > **Integrations** > **Other Integrations** > **Realms**.

Step 3 Click **Add Proxy Sequence**.

Step 4 In the **Name** field, enter a name to identify the proxy sequence.

Step 5 (Optional.) In the **Description** field, enter a description for the proxy sequence.

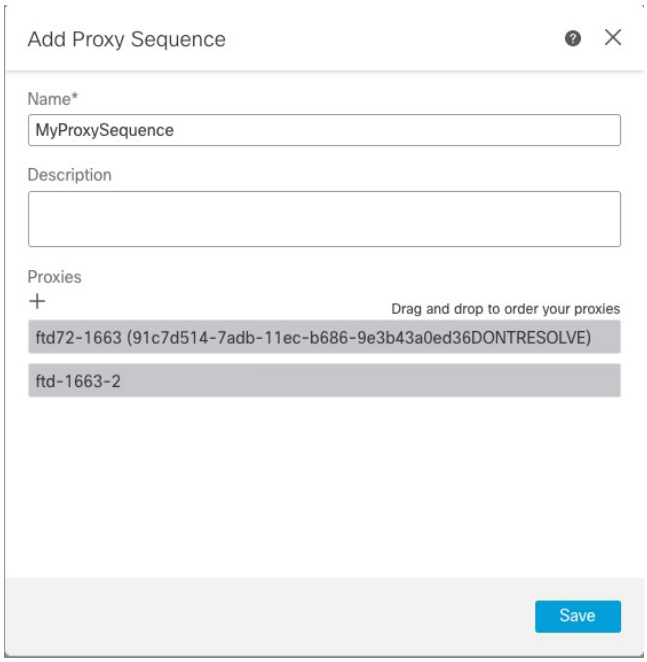
Step 6 Under Proxies, click **Add** (+).

Step 7 Click the name of each managed device to add to the sequence.

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

Step 8 Click **OK**.

Step 9 In the Add Proxy Sequence dialog box, drag and drop the proxies in the order in which you want Security Cloud Control to search for them.
The following figure shows an example of a proxy sequence consisting of two proxies. The top proxy will be searched for users before the bottom proxy. Both proxies must be able to communicate with either Active Directory or ISE/ISE-PIC.



Step 10 Click **Save**.

What to do next

See Create an Identity Policy.

Create an LDAP Realm or an Active Directory Realm and Realm Directory

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 Cloud-Delivered Firewall Management Center. For more information, see Realm Fields, on page 13.

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 20
- Find the Active Directory Server's Name, on page 19

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, see 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 13 and Realm Directory and Synchronize fields, on page 16.

A step-by-step example of setting up a realm with cross-domain trust is shown in Configure the Firewall Management Center for Cross-Domain-Trust: The Setup, on page 24.

An Active Directory Global Catalog server is *not supported* as a realm directory. For more information about the Global Catalog Server, see 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.

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 Cloud-Delivered Firewall Management Center. For more information, see Realm Fields, on page 13.

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 13.

If you are managing devices with Cisco Security Cloud Control (Security Cloud Control), create a proxy sequence first as discussed in Create a Proxy Sequence, on page 2

Important To reduce latency between the Cloud-Delivered 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 Cloud-Delivered Firewall Management Center.

For example, if your Cloud-Delivered 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.

Procedure

Step 1 Log in to the Cisco Security Cloud Control.

Step 2 Click **Policies** > **Firewall Threat Defense** > **Integrations** > **Other Integrations** > **Realms**.

Step 3 To create a new realm, choose from **Add Realm** drop-down list.

Step 4 To perform other tasks (such as enable, disable, or delete a realm), see Manage a Realm, on page 32.

Step 5 Enter realm information as discussed in Realm Fields, on page 13.

Step 6 (Optional.) From the **Proxy** list, click a managed device or proxy sequence to communicate with ISE/ISE-PIC if Security Cloud Control is unable to do so. For example, your Security Cloud Control might be in a public cloud but the ISE/ISE-PIC server might be on an internal intranet.

Step 7 In the Directory Server Configuration section, enter directory information as discussed in Realm Directory and Synchronize fields, on page 16.

Step 8 (Optional.) To configure another domain for this realm, click **Add another directory**.

Step 9 Click **Configure Groups and Users**.
Enter the following information:

Information	Description
AD Primary Domain	Domain for the Active Directory server where users should be authenticated. For additional information, see Realm Fields, on page 13. 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.
Proxy	From the list, click one or more managed devices or a proxy sequence. These devices must be able to communicate with Active Directory or ISE/ISE-PIC to retrieve user data for identity policies.
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 13.
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 excluded from user awareness and control. All other groups and users *are* available. For more information, see Realm Directory and Synchronize fields, on page 16.

Step 10 Click the **Realm Configuration** tab.

Step 11 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 16.

Step 12 If you use Kerberos authentication, click **Test**. If the test fails, wait a short time and try again.

Step 13 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 14 When you're finished configuring the realm, click **Save**.

What to do next

- Configure the Firewall Management Center for Cross-Domain-Trust: The Setup, on page 24
- Synchronize Users and Groups, on page 22
- Edit, delete, enable, or disable a realm; see Manage a Realm, on page 32.
- Compare Realms, on page 33.
- Optionally, monitor the task status; see *Viewing Task Messages* in the Cisco Secure Firewall Management Center Administration Guide.

About Realms and Realm Sequences

Realms are connections between the Cloud-Delivered Firewall Management Center and the user accounts on the servers you monitor. They specify the connection settings and authentication filter settings for the server. Realms can:

- Specify the users and user groups whose activity you want to monitor.
- 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.

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 Cloud-Delivered 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 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 the following:

- A realm or realm sequence for an 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.

- 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 Cloud-Delivered 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 3.

About 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 the following information and metadata about each user:

- LDAP user name
- First and last names
- Email address
- Department
- Telephone number

Important To reduce latency between the Cloud-Delivered 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 Cloud-Delivered Firewall Management Center.

For example, if your Cloud-Delivered 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.

About User Activity Data

User activity data is stored in the user activity database and user identity data is stored in the users database. 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*.

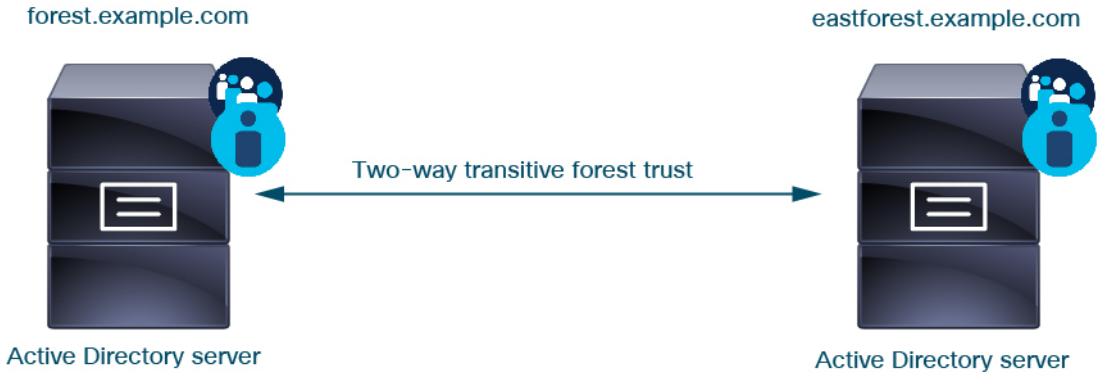
A grouping of Microsoft Active Directory (AD) domains that trust each other is commonly referred to as a *forest*. This trust relationship can enable domains to access each other's resources in different ways. For example, a user account defined in domain A can be marked as a member of a group defined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

The system and trusted domains

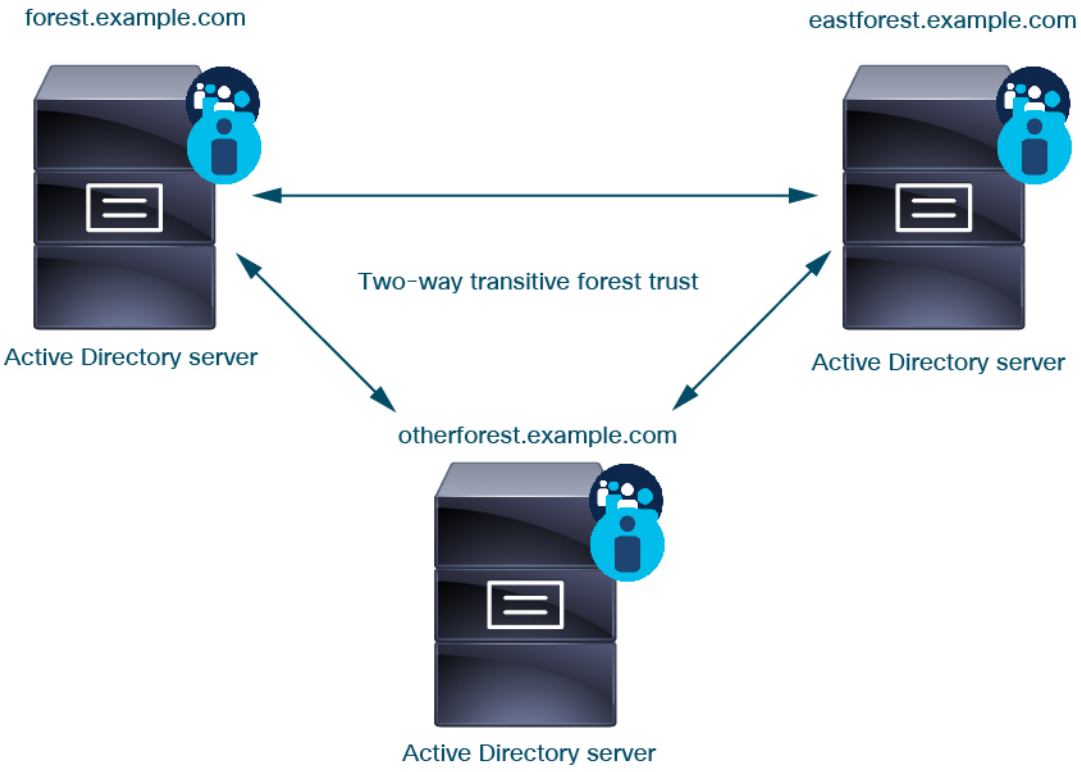
The system supports AD forests that are configured in a trust relationship. There are several types of trust relationships; this guide discusses two-way, transitive forest trust relationships. The following simple example shows two forests: **forest.example.com** and **eastforest.example.com**. Users 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.

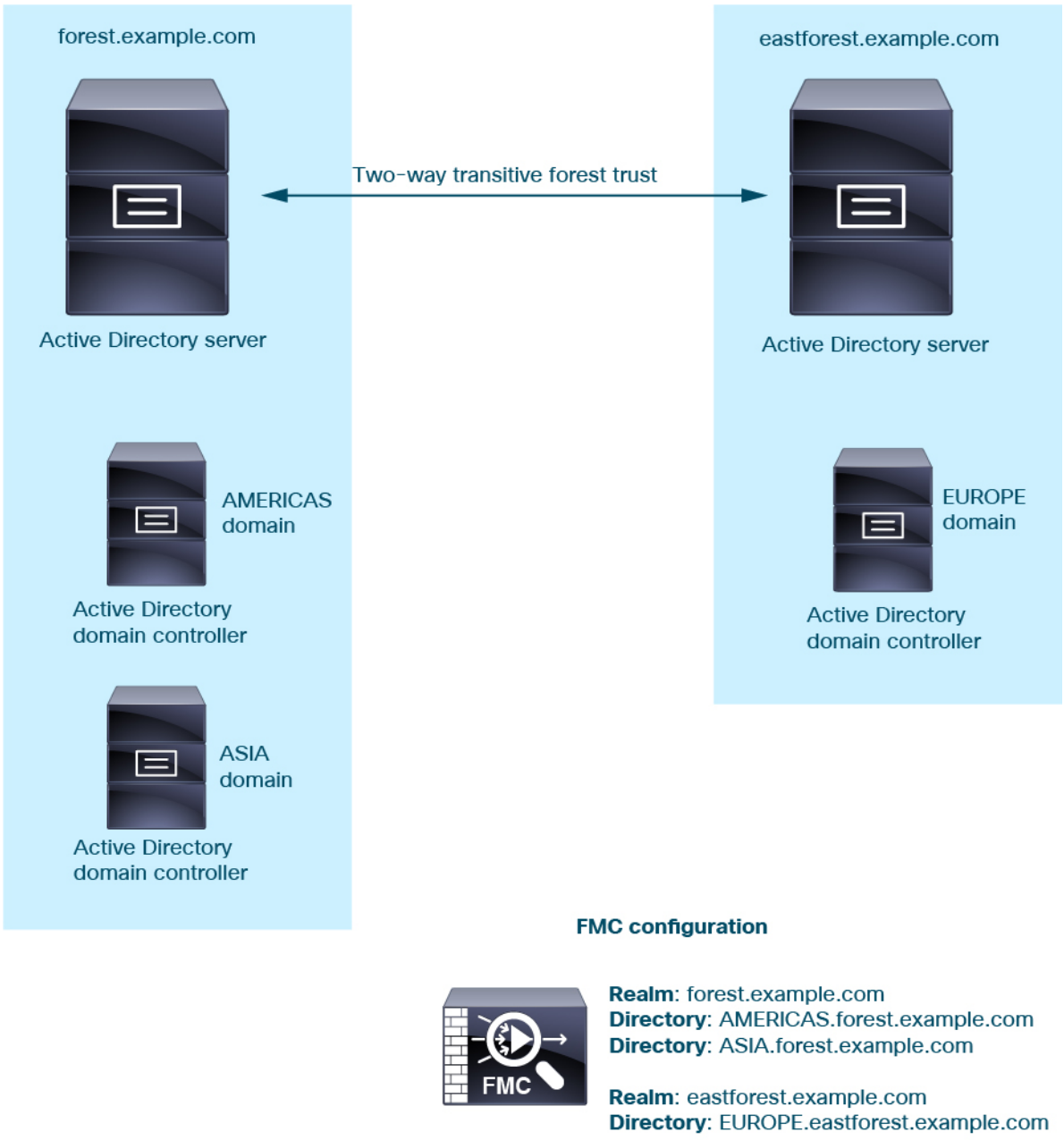


To continue the example, suppose you have three AD forests (one of which could be a subdomain or an independent forest), all set up as two-way transitive forest relationships, all users and groups are available in all three forests as well as in the system. (As in the preceding example, all three AD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



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.



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
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, see 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

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

Table 1: Map of attribute names to Cloud-Delivered 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 the following references:

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

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

The following fields are used to configure a realm.

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 11. 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.

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 Cisco Security Cloud Control 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 Cisco Security Cloud Control 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 12. If you don't specify a **Group DN**, the system retrieves the top-level DN provided you can connect to the server.

Note Following is the list of characters the system *supports* in users, groups, DNs in your directory server. Using any characters other than the following 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.

Proxy
From the list, click one or more managed devices or a proxy sequence. These devices must be able to communicate with Active Directory or ISE/ISE-PIC to retrieve user data for identity policies.

The following 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 Cisco Security Cloud Control 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 The Terminal Services (TS) 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 The 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 Cisco Security Cloud Control 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 The Captive Portal Identity Source.

Realm Directory and Synchronize fields

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 19.

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

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 19.

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 Interface.

Click one of the following:

- **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 12.

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.

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.

See one of the following tasks for more information.

Related Topics

Export the Active Directory Server's Root Certificate, on page 20
Find the Active Directory Server's Name, on page 19
Create an LDAP Realm or an Active Directory Realm and Realm Directory, on page 3

Find the Active Directory Server's Name

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.

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 3.

Related Topics

Export the Active Directory Server's Root Certificate, on page 20

Export the Active Directory Server's Root Certificate

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

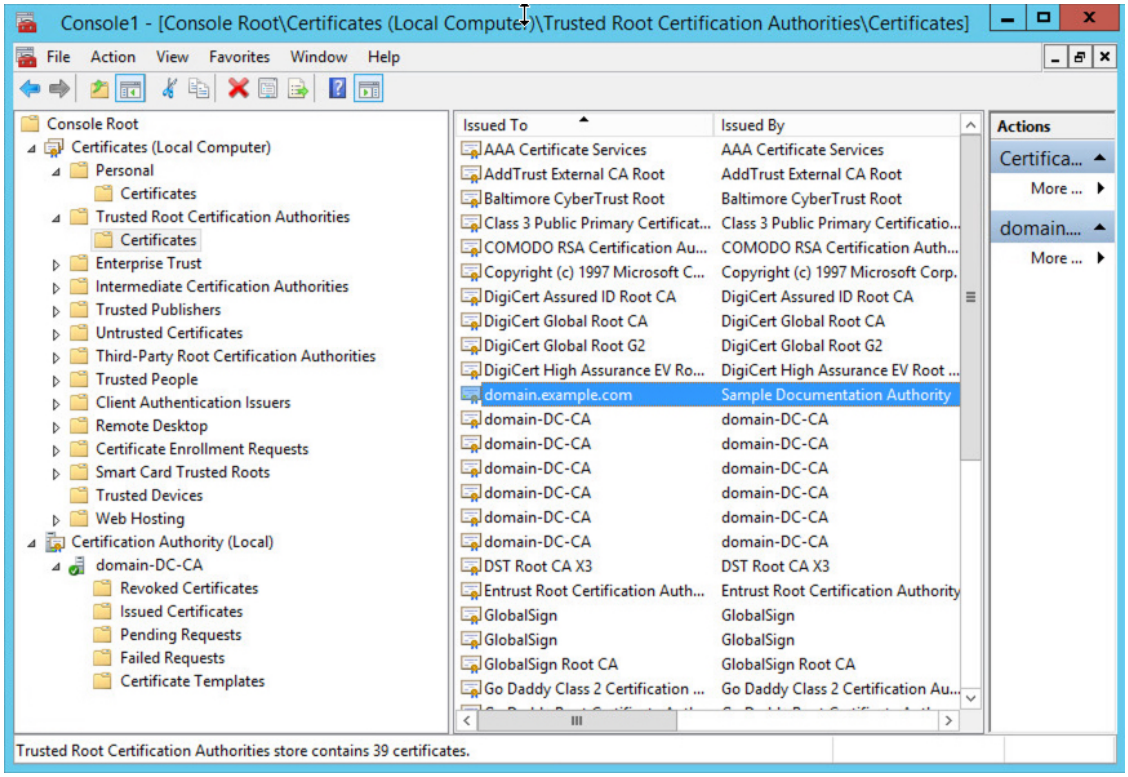
You must know the name of your Active Directory server's root certificate. The root certificate might have the same name as the domain or the certificate might have a different name. The procedure that follows shows one way you can find the name; there could be other ways, however.

Procedure

Step 1 Following 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's 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 Adding a Trusted CA Object.

Related Topics

Find the Active Directory Server's Name, on page 19

Synchronize Users and Groups

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 8.

Before you begin

Create a Cloud-Delivered 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 3.

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 Cloud-Delivered 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 3.

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.

Procedure

Step 1 Log in to the Cisco Security Cloud Control.

Step 2 Click **Policies** > **Firewall Threat Defense** > **Integrations** > **Other Integrations** > **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.
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 36.

Create a Realm Sequence

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 3.

Procedure

Step 1 Log in to the Cisco Security Cloud Control.

Step 2 Click **Policies** > **Firewall Threat Defense** > **Integrations** > **Other Integrations** > **Realms**.

Step 3 Click the **Realm Sequences** tab.

Step 4 Click **Add Sequence**.

Step 5 In the **Name** field, enter a name to identify the realm sequence.

Step 6 (Optional.) In the **Description** field, enter a description for the realm sequence.

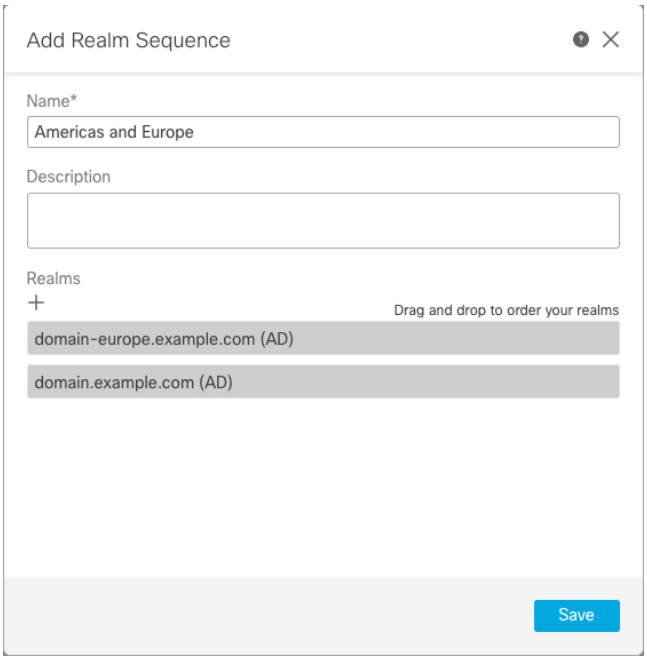
Step 7 Under Realms, click **Add** (+).

Step 8 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.

Step 9 Click **OK**.

Step 10 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 11 Click **Save**.

What to do next

See Create an Identity Policy.

Configure the Firewall Management Center for Cross-Domain-Trust: The Setup

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

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.

Following is the example setup used in this example.

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

- 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 the Cisco Security Cloud Control for Cross-Domain-Trust Step 1: Configure Realms and Directories, on page 25

Configure the Cisco Security Cloud Control for Cross-Domain-Trust Step 1: Configure Realms and Directories

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 Configure the Firewall Management Center for Cross-Domain-Trust: The Setup, on page 24.

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 8 for more information.

If you authenticate users with LDAP, you *cannot* use this procedure.

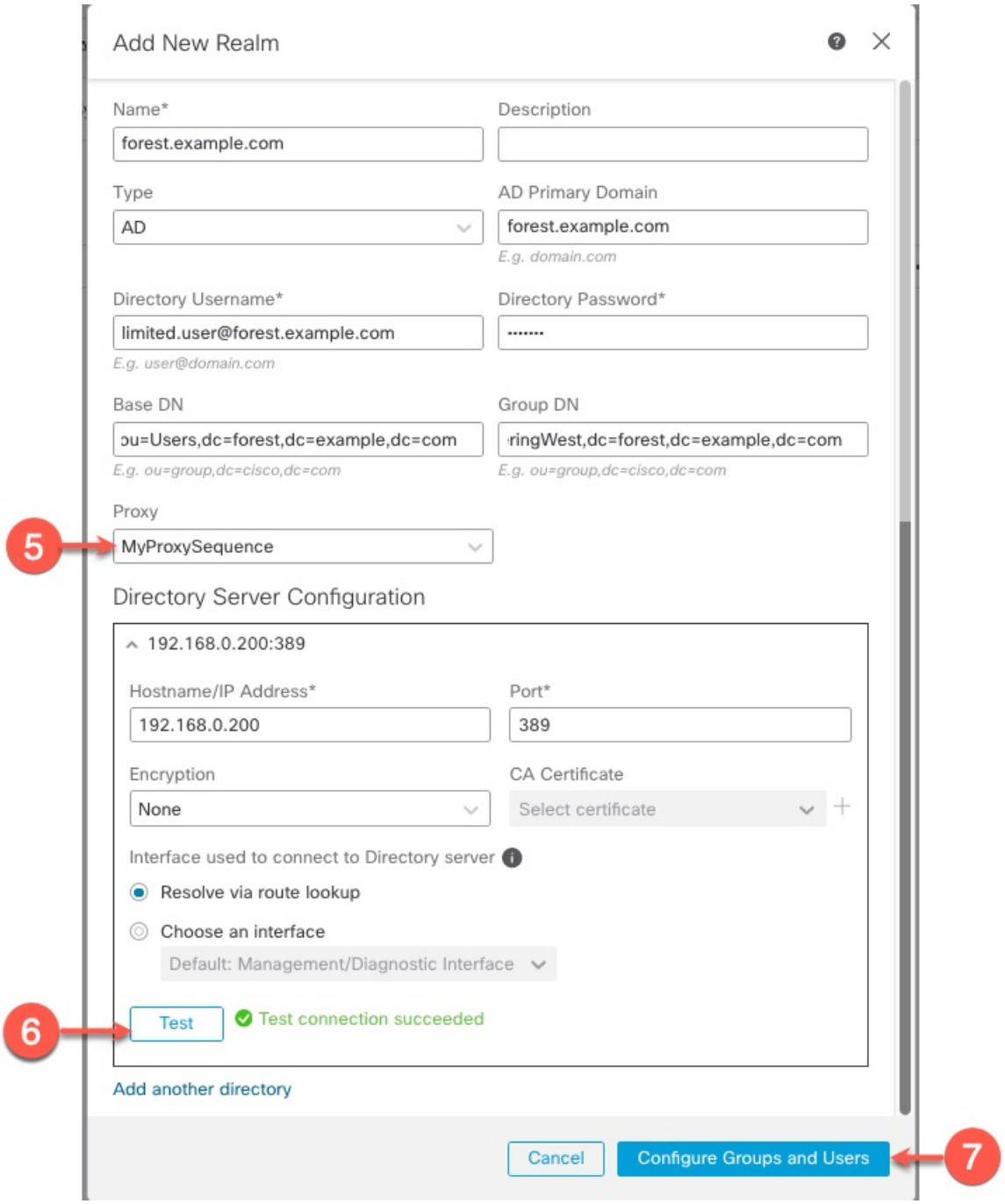
Procedure

Step 1 Log in to the Cisco Security Cloud Control.

Step 2 Click **Policies** > **Firewall Threat Defense** > **Integrations** > **Other Integrations** > **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.

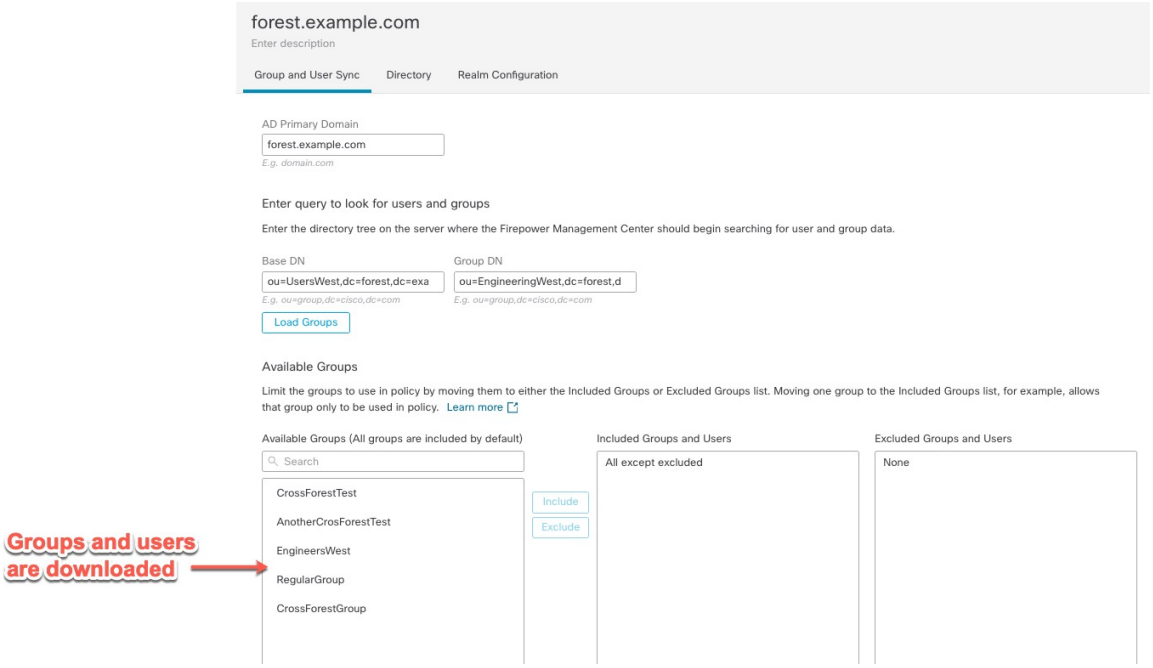
The **Interface used to connect to Directory server** can be any interface that can connect to the Active Directory server.

Step 5 **Proxy** is an optional managed device or proxy sequence to communicate with ISE/ISE-PIC if Security Cloud Control is unable to do so. For example, your Security Cloud Control might be in a public cloud but the ISE/ISE-PIC server might be on an internal intranet.

Step 6 Click **Test** and make sure the test succeeds before you continue.

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

Step 8 If your configuration was successful, 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**.

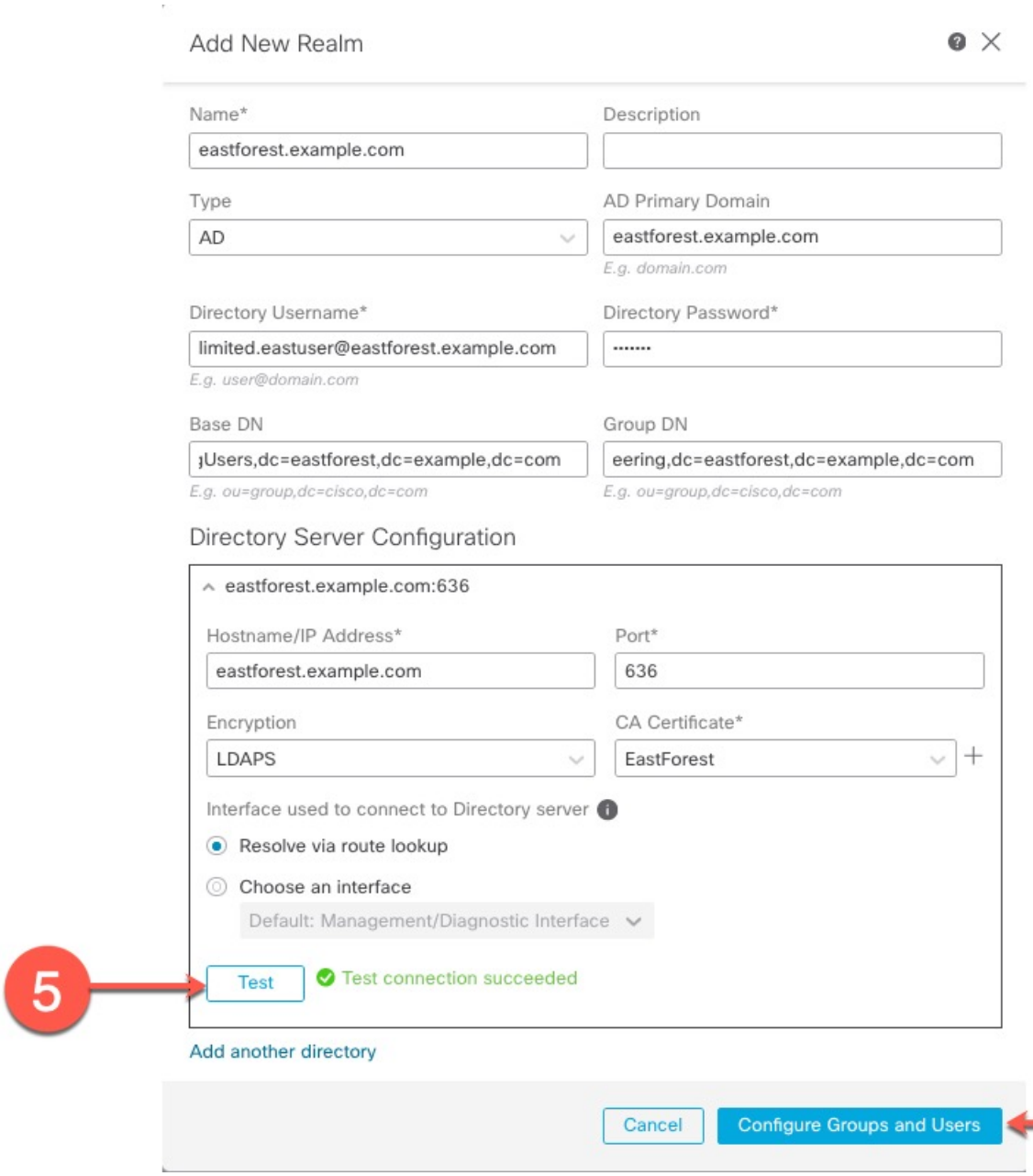
There are other optional configurations available on this page; for more information about them, see Realm Fields, on page 13 and Realm Directory and Synchronize fields, on page 16.

Step 9 If you made changes on this page or tab pages, click **Save**.

Step 10 Click **Integration** > **Other Integrations** > **Realms** > **Realms**.

Step 11 Click **Add Realm**.

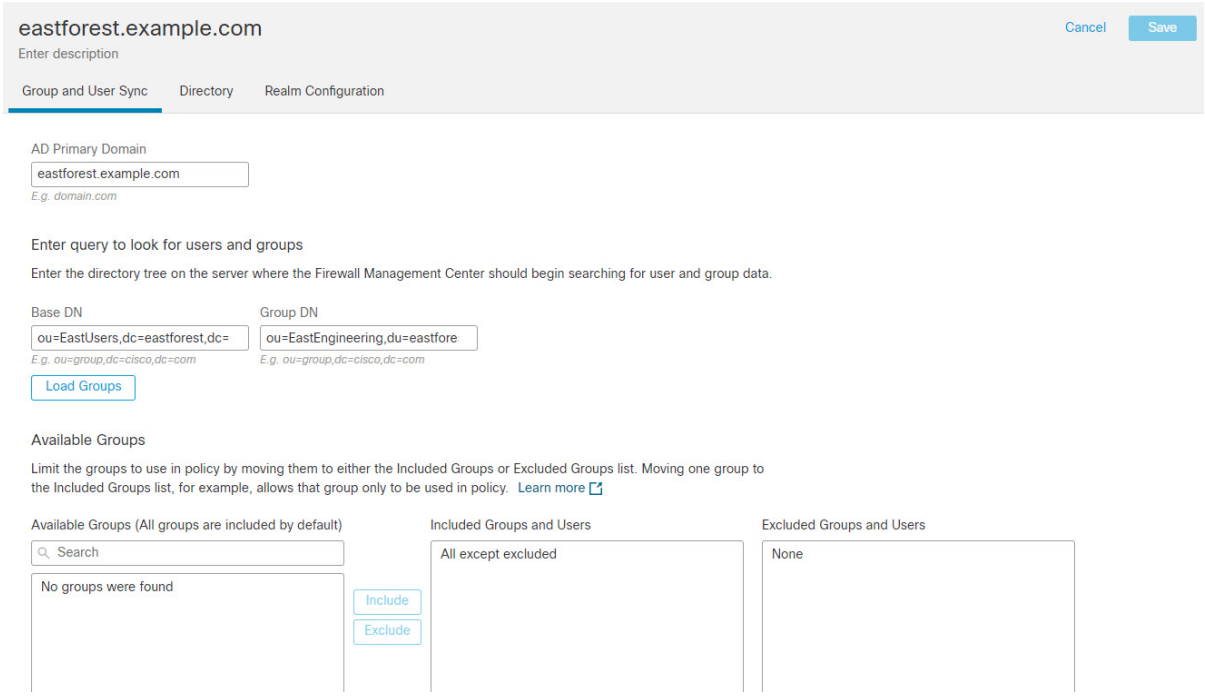
Step 12 Enter the following information to configure **eastforest.example.com**.



Step 13 Click **Test** and make sure the test succeeds before you continue.

Step 14 Click **Configure Groups and Users**.

Step 15 If your configuration was successful, the next page is displayed similar to the following.



Related Topics

Configure the Cisco Security Cloud Control for Cross-Domain-Trust Step 2: Synchronize Users and Groups, on page 30

Configure the Cisco Security Cloud Control for Cross-Domain-Trust Step 2: Synchronize Users and Groups

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 the Cisco Security Cloud Control for Cross-Domain-Trust Step 1: Configure Realms and Directories, on page 25.

Procedure

Step 1 Log in to the Cisco Security Cloud Control.

Step 2 Click **Policies** > **Firewall Threat Defense** > **Integrations** > **Other Integrations** > **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 13 and Realm Directory and Synchronize fields, on page 16.

If you're using a proxy or proxy sequence, make sure all managed devices can communicate with Active Directory or ISE/ISE-PIC. If more than one managed device can communicate with ISE/ISE-PIC, we strongly recommend you set up a proxy sequence for the realm as discussed in Create a Proxy Sequence, on page 2

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

Related Topics

Configure the Cisco Security Cloud Control for Cross-Domain-Trust Step 3: Resolve Issues, on page 31

Configure the Cisco Security Cloud Control for Cross-Domain-Trust Step 3: Resolve Issues

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.

Before you begin

Procedure

Step 1 Log in to the Cisco Security Cloud Control.

Step 2 Click **Policies** > **Firewall Threat Defense** > **Integrations** > **Other Integrations** > **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**.

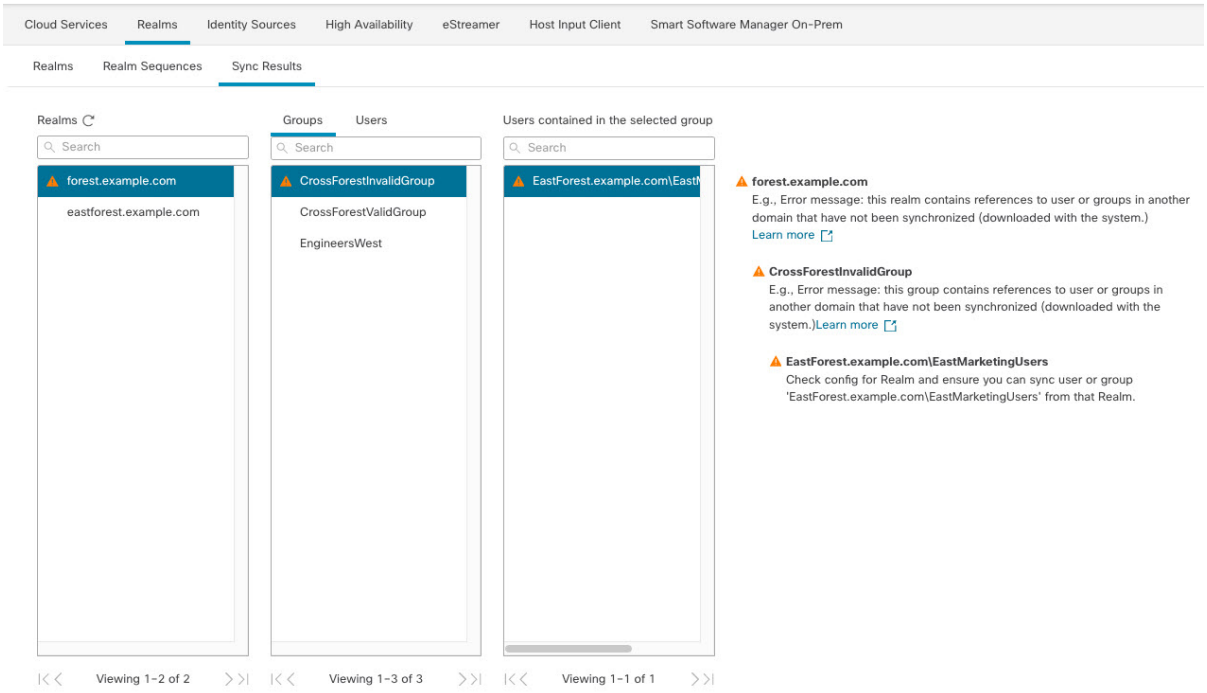
Step 4 Click the **Sync Results** tab page.

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

Procedure

Step 1 Log in to the Cisco Security Cloud Control.

Step 2 Click **Policies** > **Firewall Threat Defense** > **Integrations** > **Other Integrations** > **Realms**.

Step 3 To delete a realm, click **Delete** ( ).

Step 4 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 3.

Step 5 To enable a realm, slide **State** to the right; to disable a realm, slide it to the left.

Step 6 To download users and user groups, click **Download** ( ).

Step 7 To copy a realm, click **Copy** ( ).

Step 8 To compare realms, see Compare Realms, on page 33.

Compare Realms

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

Procedure

Step 1 Log in to the Cisco Security Cloud Control.

Step 2 Click **Policies** > **Firewall Threat Defense** > **Integrations** > **Other Integrations** > **Realms**.

Step 3 Click **Compare Realms**.

Step 4 Choose **Compare Realm** from the **Compare Against** list.

Step 5 Choose the realms you want to compare from the **Realm A** and **Realm B** lists.

Step 6 Click **OK**.

Step 7 To navigate individually through changes, click **Previous** or **Next** above the title bar.

Step 8 (Optional.) Click **Comparison Report** to generate the realm comparison report.

Step 9 (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 the ISE/ISE-PIC or Cisco TrustSec Issues
- Troubleshoot the TS Agent Identity Source
- Troubleshoot the Captive Portal Identity Source
- Troubleshoot the Remote Access VPN Identity Source
- Troubleshoot User Control

Symptom: Users are not downloaded

Possible causes follow:

- 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 Cloud-Delivered 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 Cloud-Delivered Firewall Management Center.

For example, if your Cloud-Delivered 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.

Symptom: Not all users in a realm are downloaded

Possible causes follow:

- 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 Cloud-Delivered Firewall Management Center model.
- Every user must be a member of a group. Users that are members of no groups do not get downloaded.

Symptom: 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 the following 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 Cloud-Delivered Firewall Management Center doesn't track membership in the external domain. For example, consider the following 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 Cloud-Delivered 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.

Symptom: 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 the following 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`.

Symptom: 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 the following:

- 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 the following:

- 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 Cloud-Delivered Firewall Management Center to the domain as a Domain Computer.

Symptom: 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 Cloud-Delivered 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 Cloud-Delivered Firewall Management Center. If the appliances are not synchronized, the system may perform user timeouts at unexpected intervals.

Symptom: 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.

Symptom: 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.

Symptom: 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*.

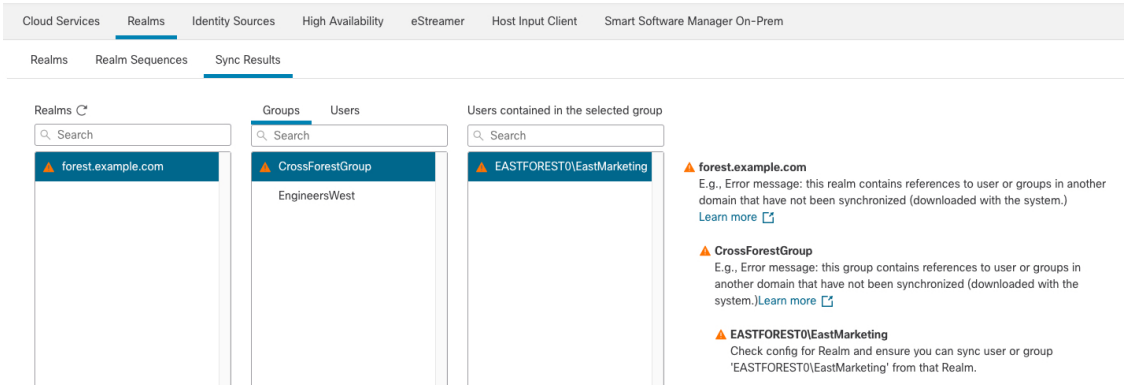
Troubleshoot Cross-Domain Trust

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

- 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 the following.



The following 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 3. • **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.

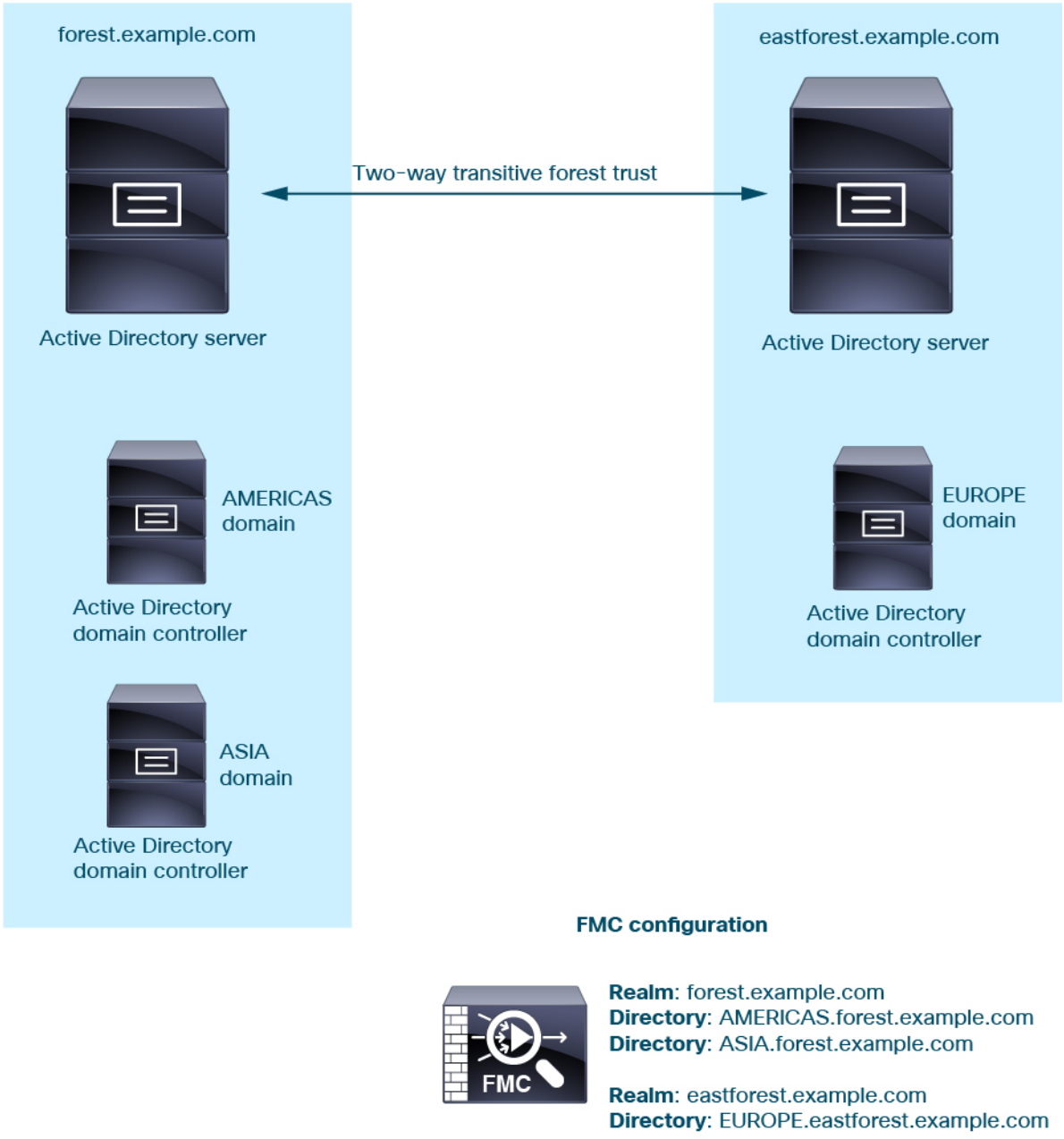
1. If you haven't done so already, log in to the Firewall Management Center.
2. Click **Integration** > **Other Integrations** > **Realms** > **Realms**.
3. Click **Download** ( ).
4. Click the **Sync Results** tab page.
5. If no indicator is displayed for entries in the Realms column, the issues have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

The following figure shows an example.



History for Realms

Table 2:

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Microsoft Azure Active Directory (AD) realms.	January 18, 2023	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.	Any	7.2.0	Similar to a realm sequence, a proxy sequence is one or more managed devices that can communicate with Cisco Security Cloud Control in the event Cisco 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.	Any	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.	Any	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.	Any	Any	A realm is a connection between the Firewall Management Center either an Active Directory or LDAP user repository.