



Realms

The following topics describe realms and identity policies:

- [About Realms and Realm Sequences, on page 1](#)
- [License Requirements for Realms, on page 8](#)
- [Requirements and Prerequisites for Realms, on page 8](#)
- [Create a Microsoft Azure AD \(SAML\) Realm, on page 8](#)
- [Create an LDAP Realm or an Active Directory Realm and Realm Directory, on page 34](#)
- [Create a Realm Sequence, on page 46](#)
- [Configure the Management Center for Cross-Domain-Trust: The Setup, on page 48](#)
- [Manage a Realm, on page 55](#)
- [Compare Realms, on page 56](#)
- [Troubleshoot Realms and User Downloads, on page 56](#)
- [History for Realms, on page 64](#)

About Realms and Realm Sequences

Realms are connections between the Secure 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.

(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.

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 management center queries the server.

To perform user awareness, you must configure a realm for any of the [Supported Servers for Realms](#). 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 the following:

- 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 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 34](#).

About User Synchronization

You can configure a realm or realm sequence to establish a connection between the 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 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 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 management center.

For example, if your 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. The maximum number of users you can store and use in access control depends on your 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 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 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 management center next updates its list of authoritative users.

Realms and Trusted Domains

When you configure a Microsoft Active Directory (AD) *realm* in the 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.



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 and trusted domains

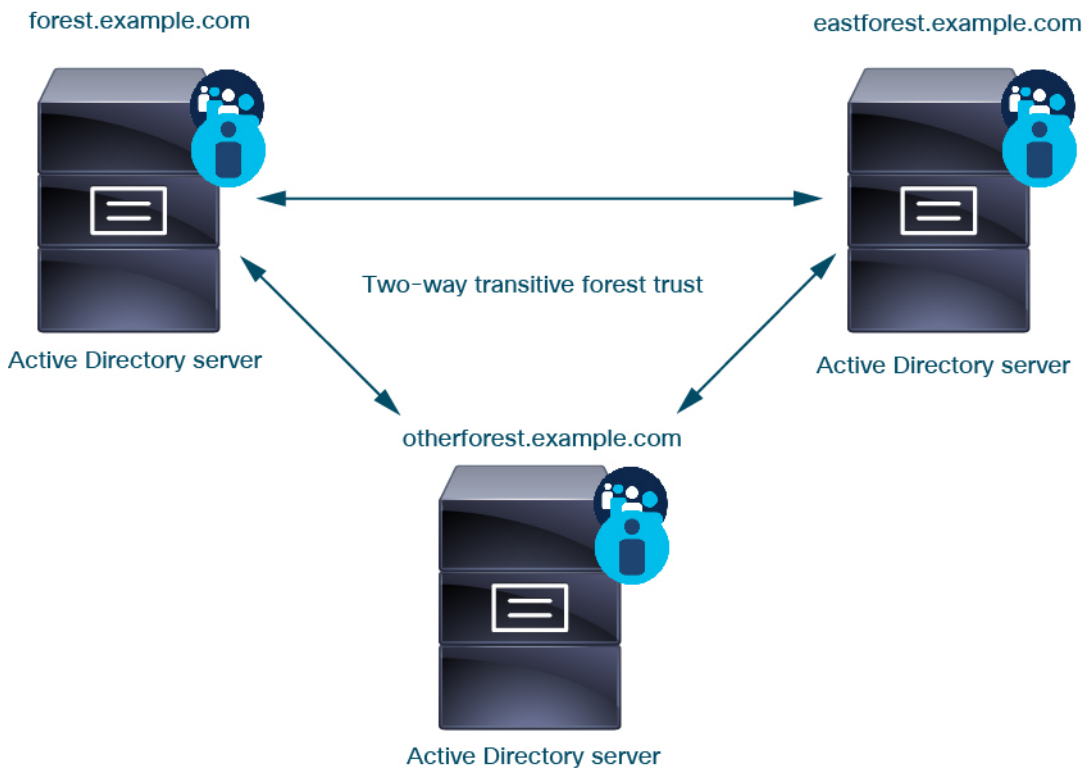
The system supports AD forests that are configured in a trust relationship. There are several types of trust relationships; this guide discusses two-way, transitive forest trust relationships. The following simple example shows two forests: **forest.example.com** and **eastforest.example.com**. Users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

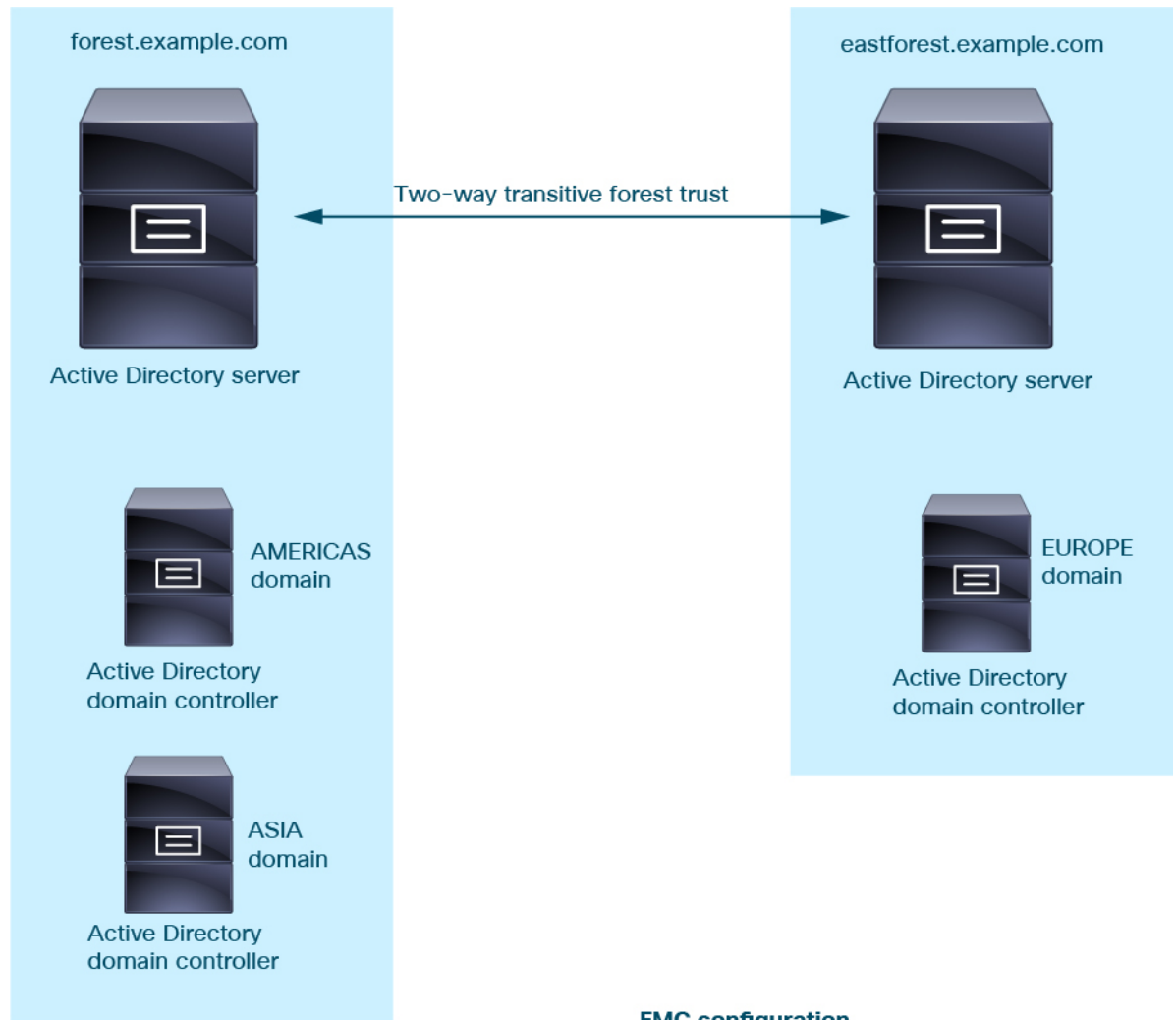


To continue the example, suppose you have three AD forests (one of which could be a subdomain or an independent forest), all set up as two-way transitive forest relationships, all users and groups are available in all three forests as well as in the system. (As in the preceding example, all three AD 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 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 management center to be able to enforce identity policies on those users and groups, you must set up each domain containing relevant users as management center realm and each domain controller as management center directory in the respective realm.

Failure to properly configure the 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.



FMC configuration



Realm: forest.example.com
Directory: AMERICAS.forest.example.com
Directory: ASIA.forest.example.com
Realm: eastforest.example.com
Directory: EUROPE.eastforest.example.com

Using the preceding example, set up the 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 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 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, 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 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 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 management center to retrieve user metadata from the servers. If the attribute names are incorrect on your server, the 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	Management Center Attribute	LDAP ObjectClass	Active Directory Attribute	OpenLDAP Attribute
LDAP user name	Username	<ul style="list-style-type: none"> • 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](#)

License Requirements for Realms

Threat Defense License

Any

Requirements and Prerequisites for Realms

Model Support

Any.

Supported Domains

Any

User Roles

- Admin
- Access Admin
- Network Admin

Create a Microsoft Azure AD (SAML) Realm

You can use a Microsoft Azure Active Directory (AD) realm for either passive authentication or active authentication.

If you enabled Change Management, you must approve all certificates used in this procedure. Open a new ticket or edit an existing one. For more information, see [Creating Change Management Tickets](#) and [Policies and Objects that Support Change Management](#)

Passive authentication

Passive authentications occur when a user authenticates with Cisco ISE.

You have the following options, depending on your choice of user and group repository:

- To use Cisco ISE as a repository for users and to perform passive authentication using Azure AD. For more information, see:
 - [About Azure AD and Cisco ISE with Resource Owned Password Credentials, on page 10](#)
 - [About Azure AD and Cisco ISE with TEAP/EAP-TLS, on page 11](#)

- To download groups from Azure AD.

For more information about setting up Azure AD, see [Configure Microsoft Azure Active Directory for Passive Authentication, on page 12](#).

Active authentication

Active authentications occur when a user authenticates through preconfigured managed devices. Captive portal is another name for active authentication. Active authentication generally uses the same user repositories as passive authentication (the exceptions being ISE/ISE-PIC, TS Agent, and the Passive Identity Agent, which are passive only).

To use Microsoft Azure AD as a captive portal requires users to authenticate with Azure AD. We refer to the realm as a Security Assertion Markup Language (SAML) realm because SAML is used to establish a trust relationship between:

- A *service provider* (the Secure Firewall Threat Defense device or devices to which authentication requests are sent).
- An *identity provider* (Microsoft Azure AD).

SAML is an open standard developed by the OASIS standards body; for more information, see the [SAML Overview](#).

For more information, see [How to Create a Microsoft Azure AD \(SAML\) Realm for Active Authentication \(Captive Portal\), on page 20](#).

How to Create a Microsoft Azure AD (SAML) for Passive Authentication

This topic discusses the high-level tasks of creating a Microsoft Azure AD (SAML) realm for passive authentication use with the Secure Firewall Management Center.

Procedure

	Command or Action	Purpose
Step 1	Enable the Cisco Secure Dynamic Attributes Connector.	The Cisco Secure Dynamic Attributes Connector is required to use a Microsoft Azure AD (SAML) realm. You can do it first or you can enable it when you create the realm. For more information, see Enable the Cisco Secure Dynamic Attributes Connector .
Step 2	Configure Microsoft Azure AD.	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 Azure Active Directory for Passive Authentication, on page 12 .
Step 3	Configure Cisco ISE.	The way you configure ISE depends on how users authenticate with your system. For more

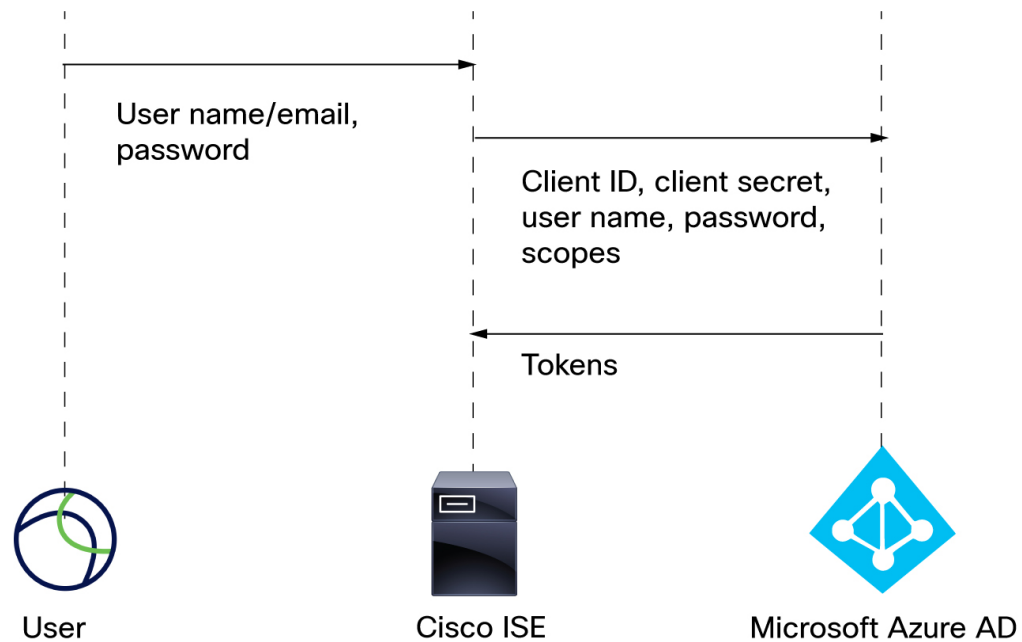
	Command or Action	Purpose
		information, see How to Configure ISE for Microsoft Azure AD (SAML) , on page 12.
Step 4	Create a Cisco ISE identity source.	The identity source enables ISE to communicate with the Secure Firewall Management Center.
Step 5	Get the information required to configure your Microsoft Azure AD (SAML) realm.	This information includes client and tenant IDs, client secret, and other information store in Microsoft Azure AD.
Step 6	Configure and verify your realm.	Test the realm's configuration before you start to use it in access control policies. Create a Microsoft Azure AD (SAML) realm as discussed in Create a Microsoft Azure AD (SAML) Realm , on page 8
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 [About Azure AD and Cisco ISE with Resource Owned Password Credentials](#), on page 10.

About Azure AD and Cisco ISE with Resource Owned Password Credentials

The following figure summarizes an Azure AD realm with Cisco ISE and resource owned password credentials (ROPC):



With ROPC,

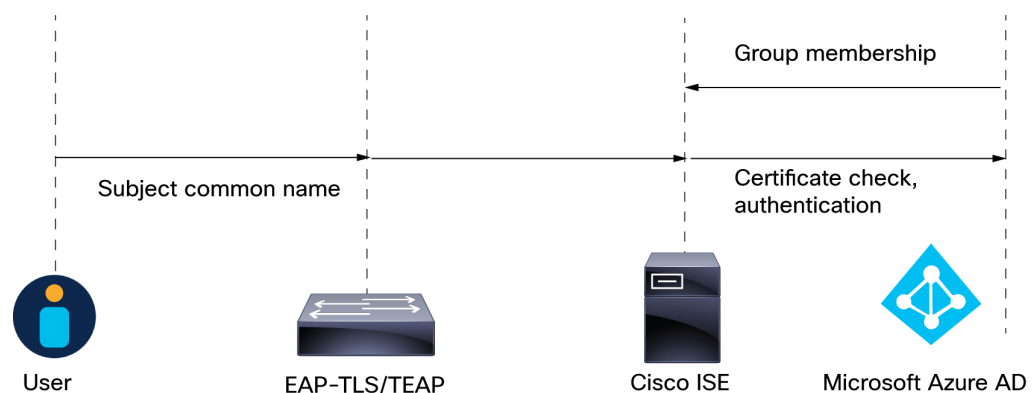
1. The user logs in with a user name (or email address) and password using a VPN client like Cisco Secure Client.
2. The client ID, client secret, user name, password, and scopes are sent to Azure AD.
3. Tokens are sent from Azure AD to Cisco ISE, which sends user sessions to the Secure Firewall Management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

About Azure AD and Cisco ISE with TEAP/EAP-TLS

Tunnel Extensible Authentication Protocol (TEAP), defined by [RFC7170](#), can be used with ISE and the Secure Firewall Management Center as follows:



The following is 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.

How to Configure ISE for Microsoft Azure AD (SAML)

In a Microsoft Azure AD (SAML) realm, it's the responsibility of ISE to send user sessions (login, logout) to the 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 AD (SAML) 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 \(SAML\) Realm, on page 14](#)

Configure Microsoft Azure Active Directory for Passive Authentication

This topic provides basic information about how to set up a 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 Azure AD; if not, consult documentation or a support resource before you get started.

Give your application the Microsoft Graph permission

Grant your Azure AD 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 Azure AD the first time.

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

- Name of the app you registered

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

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 Azure AD realm in the Secure Firewall Management Center:

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

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.

Configure Cisco ISE for Azure AD

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

What to do next

See [How to Configure ISE for Microsoft Azure AD \(SAML\)](#), on page 12.

Configure Azure AD Basic Settings

Give your application the Microsoft Graph permission

Grant your Azure AD 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 management center to download users and groups from Azure AD the first time.

Required information from this step for setting up the Azure AD realm in the management center:

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

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 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 Azure AD realm in the Secure Firewall Management Center:

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

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.

Get Required Information For Your Microsoft Azure AD (SAML) Realm

This task explains how to get the information required to set up a Microsoft Azure AD (SAML) realm in the Secure Firewall Management Center. You might have already obtained this information when you set up Microsoft Azure AD as discussed in [Configure Microsoft Azure Active Directory for Passive Authentication, on page 12](#).

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**.
 - Step 4** If necessary, filter the list of displayed apps to show the one you want to use.
 - Step 5** Click the name of your app.



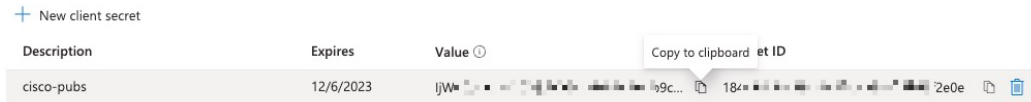
Step 6 Click **Copy** (📄) next to the following values on this page and paste those values to a text file.

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

Step 7 Click **Client Credentials**.

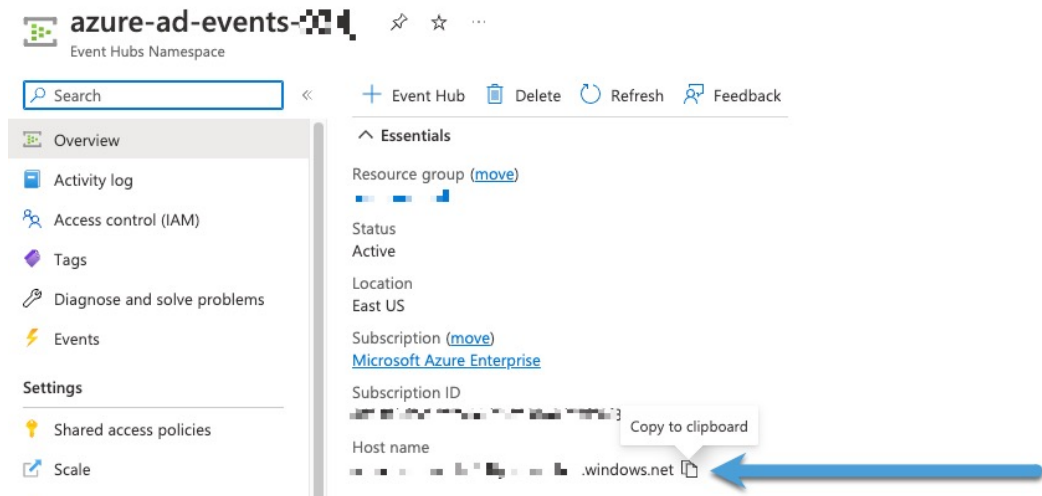
Step 8 Unless you already know the client secret *value* (as opposed to the client *secret ID*), you must create a new client secret as follows:

- a) Click **New Client Secret**.
- b) Enter the required information in the provided fields.
- c) Click **Add**.
- d) Click **Copy** (📄) next to Value as the following figure shows.



Step 9 From <https://portal.azure.com/>, click **Event Hubs** > **(name of an event hub)**.

Step 10 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.

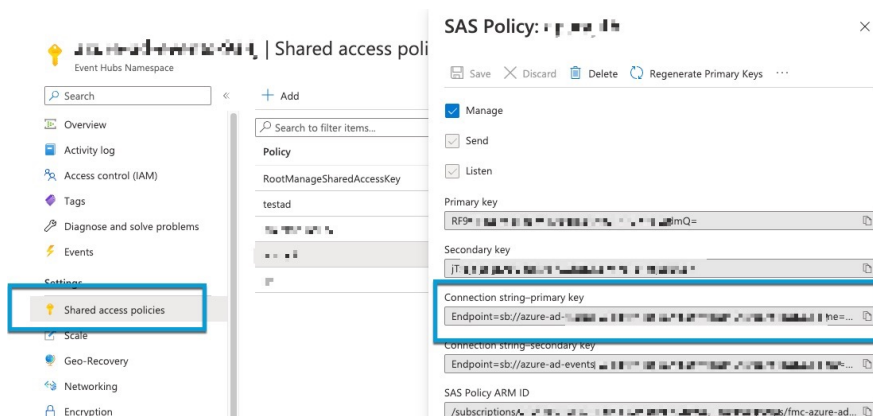


Step 11 Write down or copy to a text file the name of the event hub (same as the **Event Hubs Namespace** at the top of the page).

Step 12 In the left pane, under Settings, click **Shared access policies**.

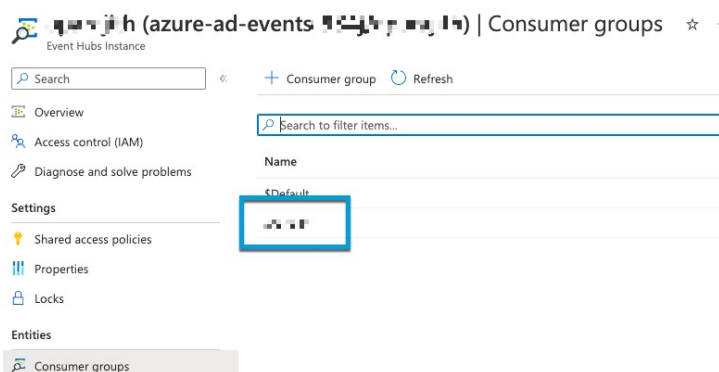
Step 13 Click the name of a policy.

Step 14 Click **Copy** next to **Connection string-primary key**.



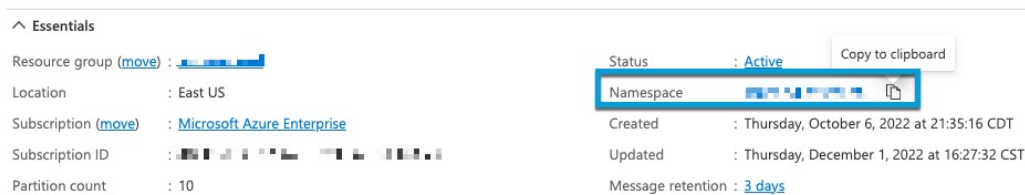
Step 15 Click **Overview > Entities > Event Hubs > (name of an event hub) > Entities > Consumer Groups**.

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



Step 16 In the left pane, click **Overview**.

Step 17 Click **Copy** next to **Namespace**.



This is your event hubs topic name.

Create a Microsoft Azure AD (SAML) Realm for Passive Authentication

The following topics discuss how to run the multi-step wizard required to create a Microsoft Azure AD (SAML) realm for passive authentication.

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.

You have the following options:

- Resource owned password credentials (ROPC): Enables users to log in with a client like Cisco Secure Client using a user name and password. ISE sends user sessions to the Secure Firewall Management Center. For more information, see [About Azure AD and Cisco ISE with Resource Owned Password Credentials, on page 10](#).

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 [About Azure AD and Cisco ISE with TEAP/EAP-TLS, on page 11](#).

To configure the realm, complete all tasks in the following order:

1. [Configure Azure AD Basic Settings, on page 13](#).
2. Get required information for your realm as discussed in [Get Required Information For Your Microsoft Azure AD \(SAML\) Realm, on page 14](#).
3. [Microsoft Azure AD \(SAML\) Realm: SAML Details, on page 17](#).

Microsoft Azure AD (SAML) Realm: SAML Details

This task discusses the first step in a multi-step wizard that creates a Microsoft Azure AD (SAML) realm. You must complete all steps in the wizard to set up your realm. The steps are different depending on whether you create the realm for active or passive authentication.

Before you begin

Complete all of the following tasks before you create your realm:

- (Passive authentication with Cisco ISE only.) If you're using Cisco ISE as the repository for users and groups, set up ISE:
 - [About Azure AD and Cisco ISE with Resource Owned Password Credentials, on page 10](#)
 - [About Azure AD and Cisco ISE with TEAP/EAP-TLS, on page 11](#)
- To use Azure AD as the repository for users and groups, see [Configure Microsoft Azure Active Directory for Passive Authentication, on page 12](#).
- Get required information for your realm as discussed in [Get Required Information For Your Microsoft Azure AD \(SAML\) Realm, on page 14](#).

Procedure

-
- Step 1** Log in to the Secure Firewall Management Center.
- Step 2** Click **Integration > Other Integrations > Realms**.
- Step 3** From the list, click **SAML - Azure AD**.
- Step 4** Enter the following information.

Item	Description
Name	Unique name to identify the realm.
Description	(Optional.) Description of the realm.
Identity Provider	Always displays Azure AD .
Configuration Type	Click one of the following: <ul style="list-style-type: none"> • Passive Authentication with ISE for passive authentication. • Passive authentication or captive portal with Azure AD for to use Azure AD as a user store for either passive authentication or active authentication (that is, captive portal).

- Step 5** Click **Next**.
-

What to do next

One of the following:

- Passive authentication: [Microsoft Azure AD \(SAML\) Realm: Azure AD Details, on page 18](#).
- Active authentication: [Microsoft Azure AD \(SAML\) Realm: SAML Service Provider \(SP\) Metadata, on page 31](#).


Microsoft Azure AD (SAML) Realm: Azure AD Details

This task discussed one page in a multi-page wizard to enable you to create a Microsoft Azure AD (SAML) realm.

Procedure

-
- Step 1** Continue from the preceding step in the wizard.
- Step 2** Enter the following information.

Item	Description
Name	Enter a unique name to identify this realm.

Item	Description
Client Secret	Enter the information you found as discussed in: <ul style="list-style-type: none"> • Passive authentication: How to Create a Microsoft Azure AD (SAML) for Passive Authentication, on page 9 • Active authentication: Get Required Information For Your Microsoft Azure AD (SAML) Realm (Active Authentication Only), on page 26
Tenant ID	
Event Hubs Host Name	
Event Hub Name	
Event Hub Connection String	
(Optional.) User Groups	Slide to Slider enabled () to specify groups to include or exclude from policy.
(Optional.) Excluded User Groups	If you enter one or more group names in this field, all groups and users they contain <i>except</i> these are downloaded and available for user awareness and user control. Enter one group name per line followed by a line break. Group names are case-sensitive.
(Optional.) Included User Groups	If you enter one or more group names in this field, only those groups and users they contain are downloaded and user data is available for user awareness and user control. Enter one group name per line followed by a line break. Group names are case-sensitive.

- Step 3** Click **Test**.
Make sure the test connection succeeds before you continue to the next step.
- Step 4** Click **Next**.

Microsoft Azure AD (SAML) Realm: User Session Timeout

This task discussed one page in a multi-page wizard to enable you to create a Microsoft Azure AD (SAML) realm.

This option sets the number of seconds before an inactive session is terminated by the system.

Procedure

- Step 1** Continue from the preceding step in the wizard.
- Step 2** Enter the following information.

Item	Description
ISE users	Default is 1440 minutes (24 hours).
Captive portal users	Default is 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 management center as Unknown (except for **Failed Captive Portal Users**).

Step 3 Click **Save**.

How to Create a Microsoft Azure AD (SAML) Realm for Active Authentication (Captive Portal)

This topic discusses the high-level tasks of creating a Microsoft Azure Active Directory (AD) realm for use with the Secure Firewall Management Center.

Before you begin

If you enabled Change Management, you must open or edit, assign, and approve a ticket for each of the following objects before you can create the realm:

- Base URL
- Service provider certificate enrollment (PKCS12 format)
- Identity provider certificate enrollment (manual format)
- The realm itself (create and assign the ticket until realm creation is complete, then approve it)

For more information, see [Opening a Ticket for Configuration Changes](#) and [Policies and Objects that Support Change Management](#).

Procedure

	Command or Action	Purpose
Step 1	Create a fully-qualified host name (FQDN) using your DNS server and upload the Threat Defense's internal certificate to the Secure Firewall Management Center. You can consult a resource such as this one if you've never done it before. Specify the IP address of a routed interface on one of the devices managed by your Secure Firewall Management Center.	Consult a DNS server reference.
Step 2	Enable the Cisco Secure Dynamic Attributes Connector.	The Cisco Secure Dynamic Attributes Connector is required to use a Microsoft Azure AD realm. You can do it first or you can enable it when you create the realm. For more information, see Enable the Cisco Secure Dynamic Attributes Connector .
Step 3	Create a network object with an associated internal certificate.	See Creating Network Objects .

	Command or Action	Purpose
Step 4	Get a signed certificate and upload it to the Secure Firewall Threat Defense to which Azure AD authentication requests will be sent.	<p>The certificate should be signed by a trusted Certificate Authority (CA) and delivered to you in .p12 format (also referred to as PKCS#12; see also this article on ssl.com).</p> <p>For background, see the section on public key infrastructure in Cisco Secure Firewall Management Center Device Configuration Guide or stackoverflow.com.</p> <p>To upload the signed certificate, see Installing a Certificate Using a PKCS12 File.</p>
Step 5	Configure Microsoft Azure AD basic settings.	<p>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.</p> <p>See Configure Azure AD Basic Settings, on page 13.</p>
Step 6	Create a single sign-on (SSO) app in Azure AD.	<p>The SSO app enables users that request access to a protected network resource to authenticate with Azure AD. The SSO app has both the federation XML that you can use to simplify realm creation as well as the identity provider certificate the Secure Firewall Threat Defense requires to security authenticate with Azure AD.</p> <p>See Configure a Single Sign-On (SSO) App in Azure AD, on page 23.</p>
Step 7	Get the information required to configure your Microsoft Azure AD realm.	<p>This information includes client and tenant IDs, client secret, and other information store in Microsoft Azure AD.</p> <p>See Get Required Information For Your Microsoft Azure AD (SAML) Realm, on page 14.</p>
Step 8	Configure a decryption policy with a Decrypt - Resign rule for the Azure Authentication Service so users can access web pages using the HTTPS protocol.	<p>The Microsoft Azure AD realm can authenticate users only if the HTTPS traffic is decrypted before the traffic is sent to the realm. The Microsoft Azure AD realm itself is seen by the system as the Azure Authentication Service application.</p> <p>Create a Decryption Rule with Decrypt - Resign Action, on page 25.</p>

	Command or Action	Purpose
Step 9	Create identity policy with an active authentication rule.	The identity policy enables selected users in your realm access resources after authenticating with the SAML realm. For more information, see Create an Identity Policy .
Step 10	Create access control policies and rules using your Microsoft Azure AD 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 .
Step 11	Associate the identity and decryption policies with the access control policy from step 3.	This final step enables the system to authenticate users with the Microsoft Azure AD realm. For more information, see Associating Other Policies with Access Control .

What to do next

See [Configure Azure AD Basic Settings, on page 13](#).

Configure Azure AD Basic Settings**Give your application the Microsoft Graph permission**

Grant your Azure AD 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 management center to download users and groups from Azure AD the first time.

Required information from this step for setting up the Azure AD realm in the management center:

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

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 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 Azure AD realm in the Secure Firewall Management Center:

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

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.

Configure a Single Sign-On (SSO) App in Azure AD

This topic discusses how to create an app in Microsoft Azure AD to handle single sign-on (SSO) from Azure AD when a network user attempts to access a protected network.

Create the app

In the Microsoft Azure AD portal, click **Enterprise Applications** on the home page and follow the instructions in [Configure Microsoft Entra SSO](#) on learn.microsoft.com.

The following figure shows part of the SSO app configuration. You must provide some of the information on this page when you configure the Microsoft Azure AD (SAML) realm. For more information, see [Get Required Information For Your Microsoft Azure AD \(SAML\) Realm \(Active Authentication Only\)](#), on page 26.

Set up Single Sign-On with SAML

An SSO implementation based on federation protocols improves security, reliability, and end user experiences and is easier to implement. Choose SAML single sign-on whenever possible for existing applications that do not use OpenID Connect or OAuth. [Learn more.](#)

Read the [configuration guide](#) for help integrating `aparajith_azure_saml`.

1 Basic SAML Configuration [Edit](#)

Identifier (Entity ID)	https://[redacted]/saml/sp/metadata/Azure
Reply URL (Assertion Consumer Service URL)	https://[redacted]/+CSCO+/saml/sp/acs?tgname=[redacted]
Sign on URL	https://samltoolkit.azurewebsites.net/
Relay State (Optional)	Optional
Logout Url (Optional)	Optional

2 Attributes & Claims [Edit](#)

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname

3 SAML Certificates [Edit](#)

Token signing certificate	
Status	Active
Thumbprint	DEB37E[redacted]B5A7

(Optional.) Upload the service provider metadata

If you already configured the Microsoft Azure AD (SAML) realm, click Upload metadata file at the top of the page to quickly provide configuration values for the SSO app.

The following figure shows an example.

aparajith_azure_saml | SAML-based Sign-on ...

Enterprise Application

[Upload metadata file](#) [Change single sign-on mode](#) [Test this application](#) [Got feedback?](#)

Set up Single Sign-On with SAML

An SSO implementation based on federation protocols improves security, reliability, and end user experiences and is easier to implement. Choose SAML single sign-on whenever possible for existing applications that do not use OpenID Connect or OAuth. [Learn more.](#)

Read the [configuration guide](#) for help integrating `aparajith_azure_saml`.

1 Basic SAML Configuration [Edit](#)

Identifier (Entity ID)	https://inside.ntd-test.cisco.com/saml/sp/metadata/Azure
Reply URL (Assertion Consumer Service URL)	https://inside.ntd-test.cisco.com/+CSCO+/saml/sp/acs?tgname=[redacted]

Add users and groups to the SSO app

Add users and groups to your app as discussed in [Add a user account to an enterprise application](#) on learn.microsoft.com

What to do next

See [Get Required Information For Your Microsoft Azure AD \(SAML\) Realm \(Active Authentication Only\)](#), on page 26.

Create a Decryption Rule with Decrypt - Resign Action

This part of the procedure discusses how to create a decryption policy to decrypt and resign traffic before the traffic reaches the SAML realm. The realm can authenticate traffic only after it has been decrypted.

Before you begin

Procedure

- Step 1** If you haven't done so already, log in to the Secure Firewall Management Center.
- Step 2** If you haven't done so already, create an internal certificate authority object to decrypt TLS/SSL traffic as discussed in [PKI](#).
- Step 3** Click **Policies > Access Control > Decryption**.
- Step 4** Click **New Policy**.
- Step 5** Enter a **Name** and choose a **Default Action** for the policy. Default actions are discussed in [Decryption Policy Default Actions](#).
- Step 6** Click **Save**.
- Step 7** Click **Add Rule**.
- Step 8** Enter a **Name** for the rule.
- Step 9** From the **Action** list, choose **Decrypt - Resign**.
- Step 10** From the **with** list, choose your service provider certificate object.
- Step 11** Click the **Applications** tab page.
- Step 12** In the Available Applications section, enter **Azure Authentication Service** in the search field.
- Step 13** Click **Azure Authentication** and click **Add to Rule**.
The following figure shows an example.

The screenshot displays the 'Add Rule' configuration interface. At the top, the 'Name' field is 'Rule for Azure AD Decryption', and the 'Insert' dropdown is set to 'below rule'. The 'Action' is 'Decrypt - Resign', and the 'with' field is 'IntCADecryption'. Below this, there are tabs for 'Zones', 'Networks', 'VLAN Tags', 'Users', 'Applications', 'Ports', 'Category', 'Certificate', 'DN', 'Cert Status', 'Cipher Suite', 'Version', and 'Logging'. The 'Applications' tab is active, showing a search for 'azure authentication ser' and a list of 'Available Applications (1)' containing 'Azure Authentication Service'. The 'Selected Applications and Filters (1)' list also contains 'Azure Authentication Service'. At the bottom right, there are 'Cancel' and 'Add' buttons.

- Step 14** (Optional.) Set other options as discussed in [Decryption Rule Conditions](#).
- Step 15** Click **Add**.

Step 16 At the top of the page, click **Save**.

What to do next

Get Required Information For Your Microsoft Azure AD (SAML) Realm (Active Authentication Only)

This task explains how to get the information required to set up a Microsoft Azure AD (SAML) realm in the management center.

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**.

Step 4 If necessary, filter the list of displayed apps to show the one you want to use.

Step 5 Click the name of your app.

Display name : docs-test

Application (client) ID : 7 [redacted]c11

Object ID : [redacted]1b9

Directory (tenant) ID : [redacted]90

Supported account types : [My organization only](#)

Client credentials : 0 certificate_1 secret

Redirect URIs : [Add a Redirect URI](#)

Application ID URI : [Add an Application ID URI](#)

Managed application in I... : docs-test

Step 6 Click **Copy** (📄) next to the following values on this page and paste those values to a text file.

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

Step 7 Click **Client Credentials**.

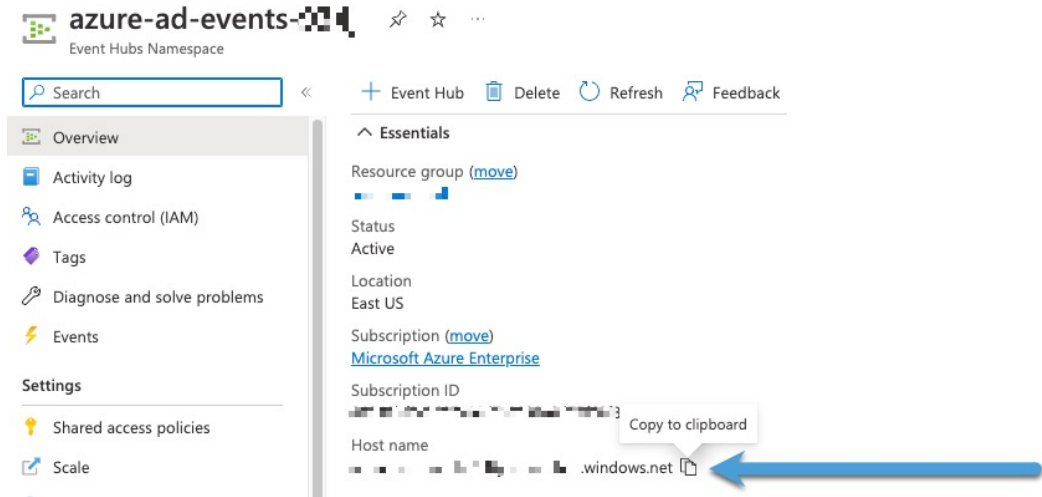
Step 8 Unless you already know the client secret *value* (as opposed to the client *secret ID*), you must create a new client secret as follows:

- a) Click **New Client Secret**.
- b) Enter the required information in the provided fields.
- c) Click **Add**.
- d) Click **Copy** (📄) next to Value as the following figure shows.

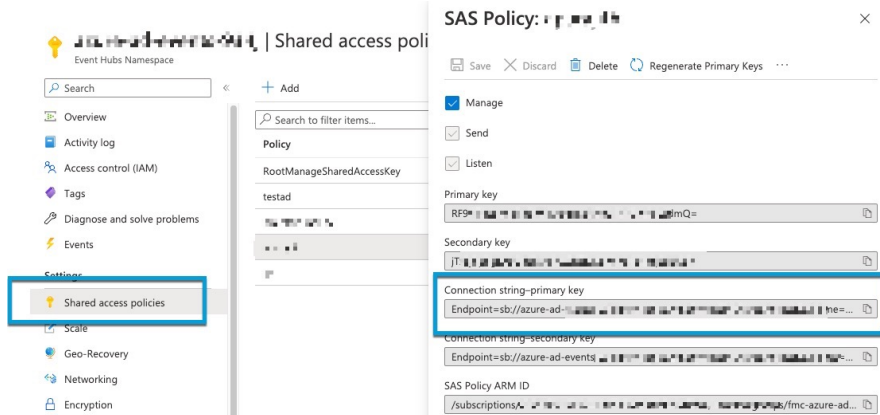
Description	Expires	Value
cisco-pubs	12/6/2023	[redacted] 18z# [redacted] 2e0e

Step 9 From <https://portal.azure.com/>, click **Event Hubs > (name of an event hub)**.

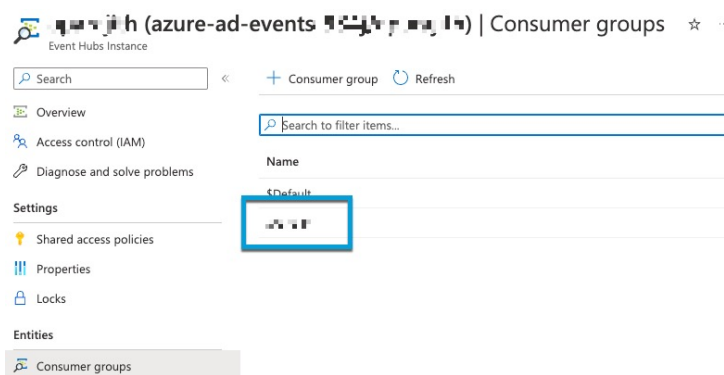
Step 10 In the right pane, click **Copy** (📄) next to the value of **Host name** and paste the value to the clipboard. This is your event hub host name.



- Step 11** 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).
- Step 12** In the left pane, under Settings, click **Shared access policies**.
- Step 13** Click the name of a policy.
- Step 14** Click **Copy** (📄) next to **Connection string-primary key**.

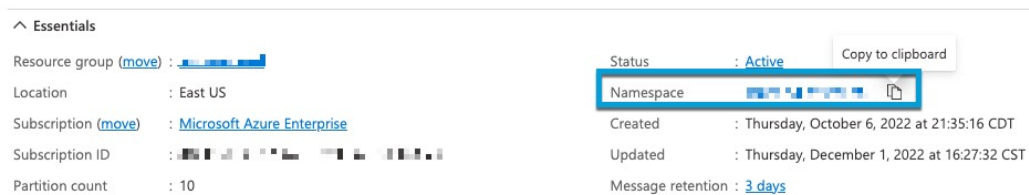


- Step 15** Click **Overview > Entities > Event Hubs > (name of an event hub) > Entities > Consumer Groups**. Write down the following value or copy it to the clipboard. This is your consumer group name.



Step 16 In the left pane, click **Overview**.

Step 17 Click **Copy** (📄) next to **Namespace**.



This is your event hubs topic name.

Step 18 Return to the home page and log in if necessary: <https://portal.azure.com/#home>.

Step 19 Click **Microsoft Entra ID**.

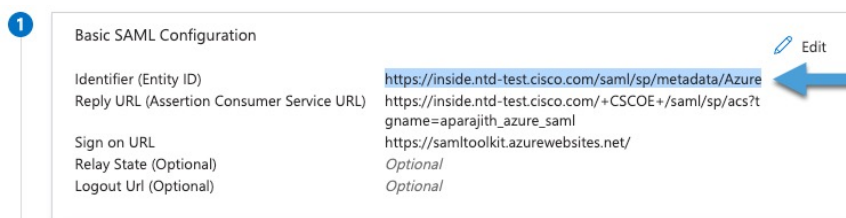
Step 20 In the left pane, click **Enterprise Applications**.

Step 21 If necessary, filter the list of applications to locate yours.

Step 22 Click the name of your enterprise application.

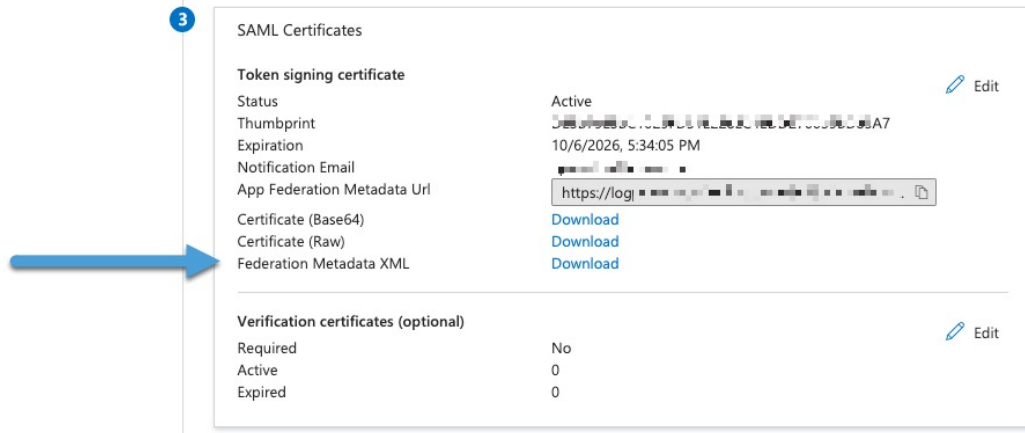
Step 23 Click **Get Started** under Set up single sign on.

Step 24 On your SSO app page, copy the value of Identifier (Entity ID) to the clipboard. The following figure shows an example.




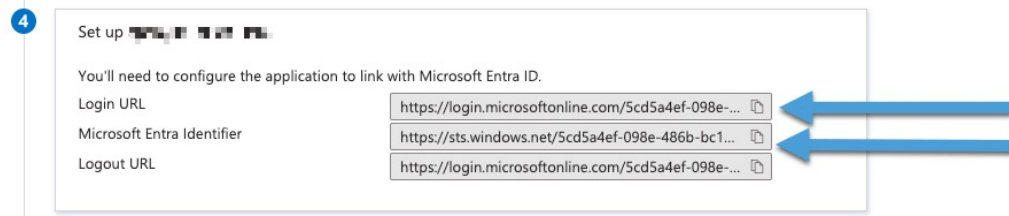
Step 25 On your SSO app page, click the **Download** link next to Federation Metadata XML, as the following figure shows.

The following figure shows an example.



Step 26 If you've already set up your SSO app, *you can stop here*. The Federation Metadata XML contains all the information required to configure the identity provider in the Secure Firewall Management Center.

Step 27 (Optional if you already downloaded the federation XML.) Click **Copy** () next to both of the following values and save them to a text file. The following figure shows an example.



What to do next

See [Create a Decryption Rule with Decrypt - Resign Action, on page 25](#).

Create a Microsoft Azure AD (SAML) Realm for Active Authentication (Captive Portal)

The following topics discuss how to run the multi-step wizard required to create a Microsoft Azure AD (SAML) realm for active authentication.

In active authentication (also referred to as *captive portal*), Microsoft Azure AD is the user store. When a user tries to access a protected resource as defined in access control rules, the user must authenticate with Microsoft Azure AD first.

To configure the realm, complete all tasks in the following order:

1. [Configure Azure AD Basic Settings, on page 13](#).
2. [Configure a Single Sign-On \(SSO\) App in Azure AD, on page 23](#).
3. [Get Required Information For Your Microsoft Azure AD \(SAML\) Realm \(Active Authentication Only\), on page 26](#)

Microsoft Azure AD (SAML) Realm: SAML Details

This task discusses the first step in a multi-step wizard that creates a Microsoft Azure AD (SAML) realm. You must complete all steps in the wizard to set up your realm. The steps are different depending on whether you create the realm for active or passive authentication.

Before you begin

Complete all of the following tasks before you create your realm:

- (Passive authentication with Cisco ISE only.) If you're using Cisco ISE as the repository for users and groups, set up ISE:
 - [About Azure AD and Cisco ISE with Resource Owned Password Credentials](#), on page 10
 - [About Azure AD and Cisco ISE with TEAP/EAP-TLS](#), on page 11
- To use Azure AD as the repository for users and groups, see [Configure Microsoft Azure Active Directory for Passive Authentication](#), on page 12.
- Get required information for your realm as discussed in [Get Required Information For Your Microsoft Azure AD \(SAML\) Realm](#), on page 14.

Procedure

- Step 1** Log in to the Secure Firewall Management Center.
- Step 2** Click **Integration > Other Integrations > Realms**.
- Step 3** From the list, click **SAML - Azure AD**.
- Step 4** Enter the following information.

Item	Description
Name	Unique name to identify the realm.
Description	(Optional.) Description of the realm.
Identity Provider	Always displays Azure AD .
Configuration Type	Click one of the following: <ul style="list-style-type: none"> • Passive Authentication with ISE for passive authentication. • Passive authentication or captive portal with Azure AD for to use Azure AD as a user store for either passive authentication or active authentication (that is, captive portal).

- Step 5** Click **Next**.

What to do next

One of the following:

- Passive authentication: [Microsoft Azure AD \(SAML\) Realm: Azure AD Details, on page 18.](#)
- Active authentication: [Microsoft Azure AD \(SAML\) Realm: SAML Service Provider \(SP\) Metadata, on page 31.](#)

Microsoft Azure AD (SAML) Realm: SAML Service Provider (SP) Metadata

This task discussed one page in a multi-page wizard to enable you to create a Microsoft Azure AD (SAML) realm.

Before you begin

Complete the tasks discussed in [Microsoft Azure AD \(SAML\) Realm: SAML Details, on page 17](#)

Procedure

Step 1 Continue from [Microsoft Azure AD \(SAML\) Realm: SAML Details, on page 17.](#)

Step 2 Enter the following information.

Item	Description
Base URL	From the list, click the network object you previously created. Network users are directed to this URL when they try to access protected network resources. You can also click Add (+) to create an object now.
Entity ID	Your SSO app's entity ID.
Assertion Consumer Services (ACS) URL	Automatically generated from the preceding values.
Service Provider Certificate	From the list, click the certificate to use to decrypt requests to the Secure Firewall Threat Defense. You can also click Add (+) to create an object now.
Download Service Provider Metadata	(Optional.) Download the metadata associated with the service provider (that is, managed device) to simplify configuring your Microsoft Azure AD SSO app.

Step 3 Click **Next**.

What to do next

[Microsoft Azure AD \(SAML\) Realm: SAML Identity Provider \(IdP\) Metadata, on page 32.](#)

Microsoft Azure AD (SAML) Realm: SAML Identity Provider (IdP) Metadata

This task discussed one page in a multi-page wizard to enable you to create a Microsoft Azure AD (SAML) realm.

Before you begin

Complete the tasks discussed in [Microsoft Azure AD \(SAML\) Realm: SAML Service Provider \(SP\) Metadata, on page 31](#).

Procedure

-
- Step 1** Continue from [Microsoft Azure AD \(SAML\) Realm: SAML Service Provider \(SP\) Metadata, on page 31](#).
- Step 2** If you previously downloaded the Azure AD SSO app's federation XML, click **Upload XML** and upload it now. You can then skip the next step.
- Step 3** Enter the following information.

Item	Description
Entity ID	Enter your identity provider's entity ID.
Single Sign on (SSO) URL	Enter the app's SSO URL.
IdP Certificate	From the list, click the certificate to use to authenticate with Microsoft Azure AD. You can also click Add (+) to create an object now.

- Step 4** Click **Next**.
-

What to do next

[Microsoft Azure AD \(SAML\) Realm: SAML Details, on page 17](#).


Microsoft Azure AD (SAML) Realm: Azure AD Details

This task discussed one page in a multi-page wizard to enable you to create a Microsoft Azure AD (SAML) realm.

Procedure

-
- Step 1** Continue from the preceding step in the wizard.
- Step 2** Enter the following information.

Item	Description
Name	Enter a unique name to identify this realm.

Item	Description
Client Secret	Enter the information you found as discussed in: <ul style="list-style-type: none"> Passive authentication: How to Create a Microsoft Azure AD (SAML) for Passive Authentication, on page 9 Active authentication: Get Required Information For Your Microsoft Azure AD (SAML) Realm (Active Authentication Only), on page 26
Tenant ID	
Event Hubs Host Name	
Event Hub Name	
Event Hub Connection String	
(Optional.) User Groups	Slide to Slider enabled () to specify groups to include or exclude from policy.
(Optional.) Excluded User Groups	If you enter one or more group names in this field, all groups and users they contain <i>except</i> these are downloaded and available for user awareness and user control. Enter one group name per line followed by a line break. Group names are case-sensitive.
(Optional.) Included User Groups	If you enter one or more group names in this field, only those groups and users they contain are downloaded and user data is available for user awareness and user control. Enter one group name per line followed by a line break. Group names are case-sensitive.

- Step 3** Click **Test**.
Make sure the test connection succeeds before you continue to the next step.
- Step 4** Click **Next**.

Microsoft Azure AD (SAML) Realm: User Session Timeout

This task discussed one page in a multi-page wizard to enable you to create a Microsoft Azure AD (SAML) realm.

This option sets the number of seconds before an inactive session is terminated by the system.

Procedure

- Step 1** Continue from the preceding step in the wizard.
- Step 2** Enter the following information.

Item	Description
ISE users	Default is 1440 minutes (24 hours).
Captive portal users	Default is 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 management center as Unknown (except for **Failed Captive Portal Users**).

Step 3 Click **Save**.

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 management center. For more information, see [Realm Fields, on page 37](#).

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

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

- [Export the Active Directory Server's Root Certificate, on page 44](#)
- [Find the Active Directory Server's Name, on page 43](#)

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 37](#) and [Realm Directory and Synchronize fields, on page 40](#).

A step-by-step example of setting up a realm with cross-domain trust is shown in [Configure the Management Center for Cross-Domain-Trust: The Setup, on page 48](#).

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 management center. For more information, see [Realm Fields, on page 37](#).

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 36](#).

If you enabled Change Management, you must open or edit, assign, and approve a ticket for each of the following objects before you can create the realm:

- If you're connecting securely to Microsoft AD or LDAP, the server's trusted certificate authority
- The realm itself

For more information, see [Opening a Ticket for Configuration Changes](#) and [Policies and Objects that Support Change Management](#).



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



Important To reduce latency between the 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 management center.

For example, if your 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 Secure Firewall Management Center.
- Step 2** Click **Integration** > **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 55](#).
- Step 5** Enter realm information as discussed in [Realm Fields, on page 37](#).
- Step 6** In the Directory Server Configuration section, enter directory information as discussed in [Realm Directory and Synchronize fields, on page 40](#).
- Step 7** (Optional.) To configure another domain for this realm, click **Add another directory**.
- Step 8** 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 37 .
Base DN	The directory tree on the server where the management center should begin searching for user data.

Information	Description
Group DN	The directory tree on the server where the management center should begin searching for group data.
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 37 .
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 <i>are</i> available. For more information, see Realm Directory and Synchronize fields, on page 40 .

Step 9 Click the **Realm Configuration** tab.

Step 10 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 40](#).

Step 11 If you use Kerberos authentication, click **Test**. If the test fails, wait a short time and try again.

Step 12 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 13 When you're finished configuring the realm, click **Save**.

What to do next

- [Configure the Management Center for Cross-Domain-Trust: The Setup, on page 48](#)
- [Synchronize Users and Groups, on page 45](#)
- Edit, delete, enable, or disable a realm; see [Manage a Realm, on page 55](#).
- [Compare Realms, on page 56](#).
- Optionally, monitor the task status; see *Viewing Task Messages* in the [Cisco Secure Firewall Management Center Administration Guide](#).

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 6](#). 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 some versions of Microsoft Active Directory, specific permissions might be required to read users and groups. Consult the documentation provided with Microsoft Active Directory for details.
- 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 7](#). 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.

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 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 [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 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 [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 43](#).

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](#), on page 43.

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 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 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 7.



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 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

To create a secure connection between an Active Directory server and the management center (which we strongly recommend), you must perform all of the following tasks:

- Export the Active Directory server's root certificate.
- Import the root certificate into the management center as a trusted CA certificate **Objects > Object Management > PKI > Trusted CAs**).
- Find the Active Directory 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 44

[Find the Active Directory Server's Name](#), on page 43

[Create an LDAP Realm or an Active Directory Realm and Realm Directory](#), on page 34

Find the Active Directory Server's Name

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

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 management center. |
-

What to do next

[Create an LDAP Realm or an Active Directory Realm and Realm Directory](#), on page 34.

Related Topics

[Export the Active Directory Server's Root Certificate](#), on page 44

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 management center to obtain user identity information.

Before you begin

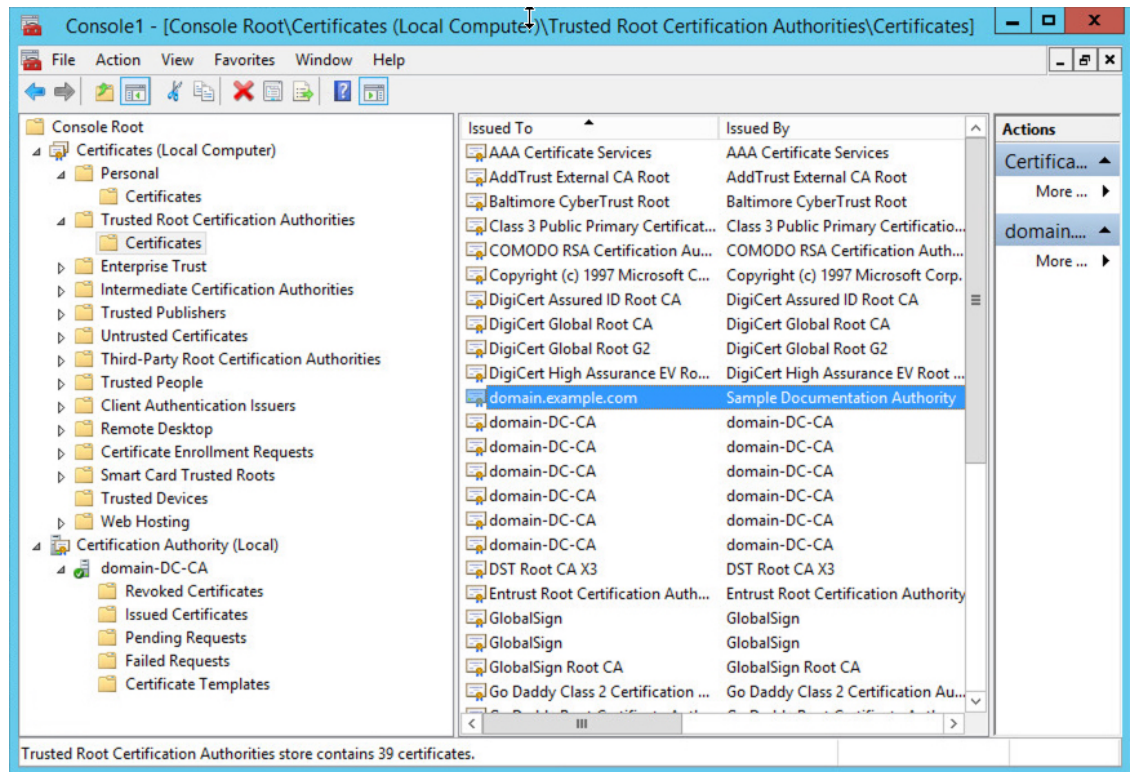
You must know the name of your Active Directory server's root certificate. The root certificate might have the same name as the domain or the certificate might have a different name. The procedure that follows shows one way you can find the name; there could be other ways, however.

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 management center from the Active Directory server.

- Click **Start** and enter **cmd**.
- Enter the command **certutil -ca.cert certificate-name**.
The server's certificate is displayed on the screen.
- 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 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 43

Synchronize Users and Groups

Synchronizing users and groups means the management center queries the realms and directories you configured for groups and users in those groups. All users the 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 management center cannot load. For details, see [Realms and Trusted Domains](#), on page 3.

Before you begin

Create a management center *realm* for each Active Directory domain and a management center *directory* for each Active Directory domain controller in each forest. See [Create an LDAP Realm or an Active Directory Realm and Realm Directory](#), on page 34.



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 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 34.

Procedure

Step 1 If you haven't done so already, log in to the management center.

Step 2 Click **Integration > 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 61.

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.

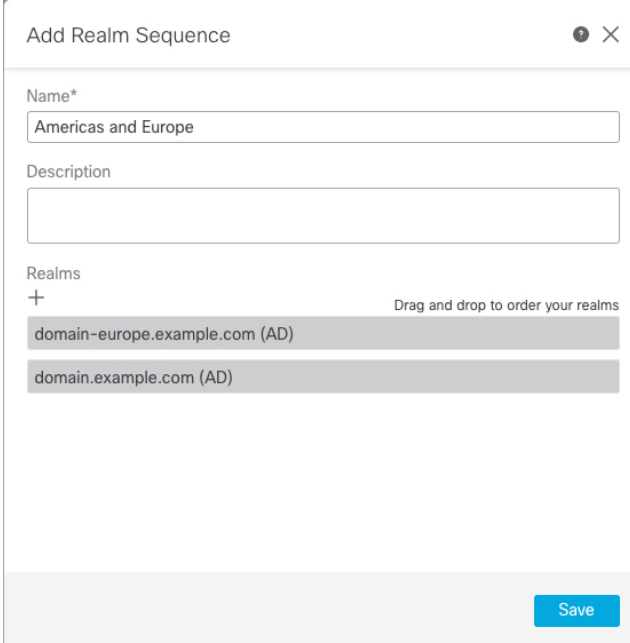
Before you begin

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 34.

Procedure

- Step 1** Log in to the management center if you have not already done so.
- Step 2** Click **Integration > Other Integrations > Realms > Realm Sequences**.
- Step 3** Click **Add Sequence**.
- Step 4** In the **Name** field, enter a name to identify the realm sequence.
- Step 5** (Optional.) In the **Description** field, enter a description for the realm sequence.
- Step 6** Under Realms, click **Add (+)**.
- Step 7** 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 8** Click **OK**.
- Step 9** 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.



Add Realm Sequence

Name*
Americas and Europe

Description

Realms
+ Drag and drop to order your realms

domain-europe.example.com (AD)

domain.example.com (AD)

Save

- Step 10** Click **Save**.

What to do next

See [Create an Identity Policy](#).

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

This is an introduction to several topics that walk you through configuring the 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.



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

Following is the example setup used in this example.



Using the preceding example, you would set up the 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 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=EngineeringWest,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 Secure Firewall Management Center for Cross-Domain-Trust Step 1: Configure Realms and Directories](#), on page 49

Configure the Secure Firewall Management Center 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 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 Management Center for Cross-Domain-Trust: The Setup](#), on page 48.

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 management center.
- Step 2** Click **Integration** > **Other Integrations** > **Realms**.
- Step 3** Choose from **Add Realm** drop-down list. .
- Step 4** Enter the following information to configure **forest.example.com**.

Add New Realm

Name* Description

Type AD Primary Domain
E.g. domain.com

Directory Username* Directory Password*
E.g. user@domain.com

Base DN Group DN
E.g. ou=group,dc=cisco,dc=com

Directory Server Configuration

eastforest.example.com:389

Hostname/IP Address* Port*

Encryption CA Certificate

Interface used to connect to Directory server ⓘ

Resolve via route lookup

Choose an interface

Default: Management/Diagnostic Interface

5 ✓ Test connection succeeded

[Add another directory](#)

6

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

forest.example.com
Enter description

Group and User Sync | Directory | Realm Configuration

AD Primary Domain
forest.example.com
E.g. domain.com

Enter query to look for users and groups
Enter the directory tree on the server where the Firepower Management Center should begin searching for user and group data.

Base DN
ou=UsersWest,dc=forest,dc=exa
E.g. ou=group,dc=cisco,dc=com

Group DN
ou=EngineeringWest,dc=forest,d
E.g. ou=group,dc=cisco,dc=com

Load Groups

Available Groups
Limit the groups to use in policy by moving them to either the Included Groups or Excluded Groups list. Moving one group to the Included Groups list, for example, allows that group only to be used in policy. [Learn more](#)

Available Groups (All groups are included by default)

Included Groups and Users
All except excluded

Excluded Groups and Users
None

Search

CrossForestTest
AnotherCrosForestTest
EngineersWest
RegularGroup
CrossForestGroup

Include
Exclude

Groups and users are downloaded →

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 37](#) and [Realm Directory and Synchronize fields, on page 40](#).

- Step 8** If you made changes on this page or tab pages, click **Save**.
- Step 9** Click **Integration > Other Integrations > Realms**.
- Step 10** Click **Add Realm**.
- Step 11** Enter the following information to configure **eastforest.example.com**.

Add New Realm
?
✕

<p>Name*</p> <input type="text" value="eastforest.example.com"/>	<p>Description</p> <input type="text"/>
<p>Type</p> <input type="text" value="AD"/>	<p>AD Primary Domain</p> <input type="text" value="eastforest.example.com"/> <p><small>E.g. domain.com</small></p>
<p>Directory Username*</p> <input type="text" value="limited.eastuser@eastforest.example.com"/> <p><small>E.g. user@domain.com</small></p>	<p>Directory Password*</p> <input type="password" value="....."/>
<p>Base DN</p> <input type="text" value="jUsers,dc=eastforest,dc=example,dc=com"/> <p><small>E.g. ou=group,dc=cisco,dc=com</small></p>	<p>Group DN</p> <input type="text" value="eering,dc=eastforest,dc=example,dc=com"/> <p><small>E.g. ou=group,dc=cisco,dc=com</small></p>

Directory Server Configuration

^ eastforest.example.com:636

<p>Hostname/IP Address*</p> <input type="text" value="eastforest.example.com"/>	<p>Port*</p> <input type="text" value="636"/>
<p>Encryption</p> <input type="text" value="LDAPS"/>	<p>CA Certificate*</p> <input type="text" value="EastForest"/>

Interface used to connect to Directory server ⓘ

Resolve via route lookup

Choose an interface

Default: Management/Diagnostic Interface ▾

Test
✔ Test connection succeeded

[Add another directory](#)

Cancel
Configure Groups and Users

Step 12 Click **Test** and make sure the test succeeds before you continue.

Step 13 Click **Configure Groups and Users**.

Step 14 If your configuration was successful, the next page is displayed similar to the following.

eastforest.example.com
Cancel Save

Enter description

Group and User Sync
Directory
Realm Configuration

AD Primary Domain

eastforest.example.com

E.g. domain.com

Enter query to look for users and groups

Enter the directory tree on the server where the Firewall Management Center should begin searching for user and group data.

Base DN

ou=EastUsers,dc=eastforest,dc=

E.g. ou=group,dc=cisco,dc=com

Group DN

ou=EastEngineering,du=eastfore

E.g. ou=group,dc=cisco,dc=com

Load Groups

Available Groups

Limit the groups to use in policy by moving them to either the Included Groups or Excluded Groups list. Moving one group to the Included Groups list, for example, allows that group only to be used in policy. [Learn more](#)

Available Groups (All groups are included by default)

No groups were found

Include

Exclude

Included Groups and Users

All except excluded

Excluded Groups and Users

None

Related Topics

[Configure the management center for Cross-Domain-Trust Step 2: Synchronize Users and Groups](#), on page 53



Configure the management center 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 Secure Firewall Management Center for Cross-Domain-Trust Step 1: Configure Realms and Directories](#), on page 49.

Procedure

- Step 1** Log in to the management center.
- Step 2** Click **Integration** > **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 37](#) and [Realm Directory and Synchronize fields, on page 40](#).

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

Related Topics

[Configure the management center for Cross-Domain-Trust Step 3: Resolve Issues](#), on page 54

Configure the management center for Cross-Domain-Trust Step 3: Resolve Issues


The final step in setting up cross-domain trust in the 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 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 management center if you have not already done so.

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



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 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 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:

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 management center if you haven't already done so.
 - Step 2** Click **Integration > 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 34](#).
 - 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 56](#).
-

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 management center.
 - Step 2** Click **Integration > 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: Realms and groups reported but not downloaded

The management center's health monitor informs you of user or realm mismatches, which are defined as:

- **User mismatch:** A user is reported to the 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 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 management center.

For example, if you defined a realm that corresponds to a domain named **domain.example.com** in the 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 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 60](#).

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 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 management center.

For example, if your 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 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.

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 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 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 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 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.

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*.

Detect Realm or User Mismatches

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

- **User mismatch:** A user is reported to the 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 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 management center.

For additional details, see [Troubleshoot Realms and User Downloads, on page 56](#).

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 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 56](#).
- 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 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.

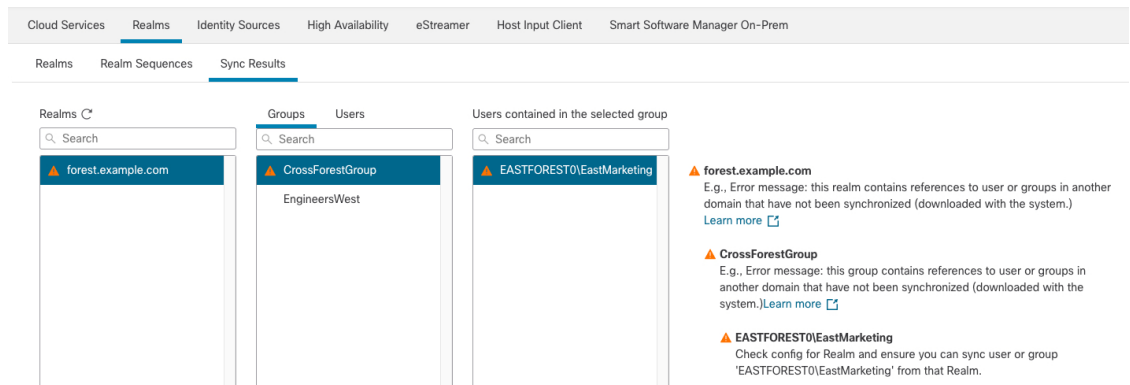
Troubleshoot Cross-Domain Trust

Typical issues with troubleshooting the 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 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	<p>Displays all realms configured in the system. Click Refresh (🔄) to update the list of realms.</p> <p>Yellow Triangle (▲) is displayed to indicate issues in the realm.</p> <p>Nothing is displayed next to a realm if all users and groups synchronized successfully.</p>
Groups	<p>Click Groups to display all groups in the realm. As with realms, Yellow Triangle (▲) is displayed to indicate issues.</p> <p>Click Yellow Triangle (▲) to see more detail about the issue.</p>
Users	<p>Click Users to display all users, sorted by group.</p>
Users contained in the selected group	<p>Displays all users in the group you selected in the Groups column. Clicking Yellow Triangle (▲) displays more information to the right of the table.</p>

Column	Meaning
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).	<p>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:</p> <ul style="list-style-type: none"> • Problem: The forest containing the groups and users do not have corresponding realms configured in the management center. <p>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 34.</p> <ul style="list-style-type: none"> • Problem: You excluded groups from being downloaded to the management center. <p>Solution: Click the Realms tab page, click Edit (✎), then move the indicated group or user from the Excluded Groups and Users list.</p>

Try downloading users and groups again

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

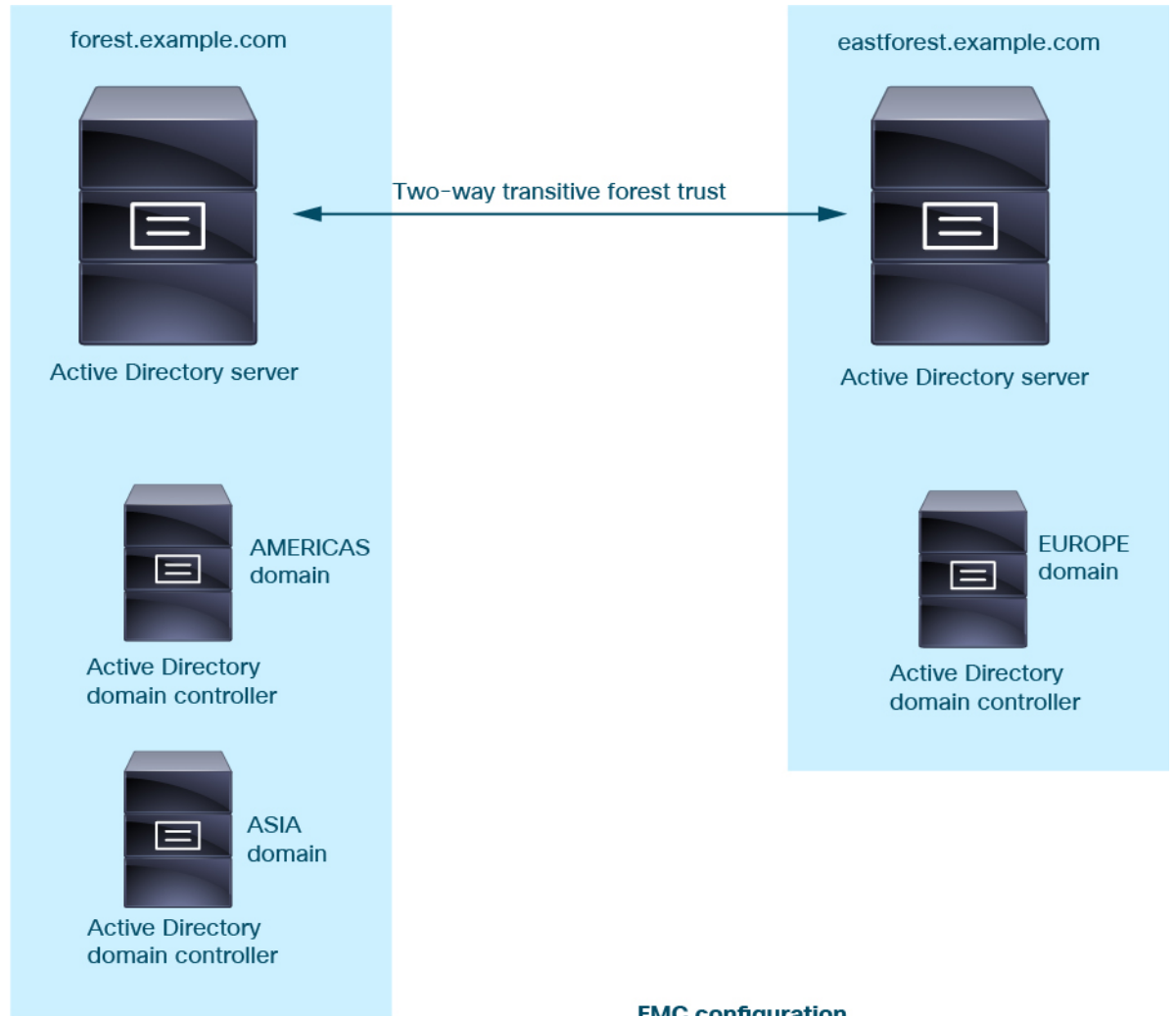
1. If you haven't done so already, log in to the management center.
2. Click **Integration > Other Integrations > Realms**.
3. Click **Download** (↓).
4. Click the **Sync Results** tab page.
5. If no indicator is displayed for entries in the Realms column, the issues have been resolved.

Add a realm for all forests

Make sure you configured:

- management center realm for each forest that has users you want to use in identity policies.
- management center directory for each domain controller in that forest with users you want to use in identity policies.

The following figure shows an example.



FMC configuration



- Realm:** forest.example.com
- Directory:** AMERICAS.forest.example.com
- Directory:** ASIA.forest.example.com

- Realm:** eastforest.example.com
- Directory:** EUROPE.eastforest.example.com

History for Realms

Feature	Minimum Management Center	Minimum Threat Defense	Details
Microsoft Azure Active Directory (SAML) realms.	7.6.0	7.4.0	<p>You can now use Microsoft Azure Active Directory (AD) realms for active and passive authentication:</p> <ul style="list-style-type: none"> • Active authentication using Azure AD: Use Azure AD as a captive portal. • Passive authentication using Cisco ISE (introduced in Version 7.4.0): The management center gets groups from Azure AD and logged-in user session data from ISE. <p>We use SAML (Security Assertion Markup Language) to establish a trust relationship between a service provider (the devices that handle authentication requests) and an identity provider (Azure AD).</p> <p>Upgrade impact. If you had a Microsoft Azure AD realm configured before the upgrade, it is displayed as a SAML - Azure AD realm configured for passive authentication. All previous user session data is preserved.</p> <p>New/modified screens: Integration > Other Integrations > Realms > Add Realm > SAML - Azure AD</p> <p>New/modified CLI commands: none</p>
Microsoft Azure Active Directory (AD) realms.	7.4.0	7.4.0	<p>You can use a Microsoft Azure Active Directory (AD) realm with ISE to authenticate users and get user sessions for user control.</p> <p>New/modified screens: System (⚙️) > Integration > Realms > Add Realm > Azure AD</p>
Cross-domain trust for Active Directory domains.	7.2.0	7.0.0	<p>A grouping of Microsoft Active Directory (AD) domains that trust each other is commonly referred to as a <i>forest</i>. 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.</p> <p>The management center can get users from Active Directory forests for identity rules.</p>
Realm sequences.	7.2.0	6.7.0	<p>A <i>realm sequence</i> 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.</p> <p>New/modified screens: Integration > Other Integrations > Realms > Realm Sequences</p>
Realms for user control.	7.2.0	Any	<p>A realm is a connection between the management center either an Active Directory or LDAP user repository.</p>