



## Create and Manage Realms

---

The following topics discuss how to create and manage *realms*, which are user stores for user awareness and control:

- [About Realms and Realm Sequences, on page 1](#)
- [License Requirements for Realms, on page 5](#)
- [Requirements and Prerequisites for Realms, on page 6](#)
- [Create a Realm, on page 6](#)
- [Create a Realm Sequence, on page 18](#)
- [Manage a Realm, on page 19](#)
- [Compare Realms, on page 20](#)
- [Troubleshoot Realms and User Downloads, on page 20](#)
- [History for Realms, on page 25](#)

## About Realms and Realm Sequences

*Realms* are connections between the Firepower 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.

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 Firepower 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 Firepower 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, 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 AD server or for ISE/ISE-PIC




---

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

---

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

A realm sequence is not supported for LDAP.

### About User Download

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

- LDAP and 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.

You configure LDAP server or Active Directory domain controller connections as a directory in a realm. You must check **Download users and user groups for access control** to download a realm's user and user group data for user awareness and user control.

The Firepower Management Center obtains the following information and metadata about each user:

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

### 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 Firepower 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 Firepower 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 Firepower Threat Defense Command Reference*.



**Note** If you remove a user that has been detected by the system from your user repository, the Firepower 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 Firepower Management Center next updates its list of authoritative users.

Video  [YouTube video on creating a realm.](#)

## Realms and Trusted Domains

When you configure a *realm* in the Firepower Management Center, it is associated with an Active Directory or LDAP *domain*.

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

### The Firepower System and trusted domains

The Firepower System does not support trusted AD domains. This means that the Firepower System does not track which configured domains trust each other, and does not know which domains are parent or child domains of each other. The Firepower System also has not been tested to assure support for environments that use cross-domain trust, even when the trust relationship is exercised outside of the Firepower System.

## Supported Servers for Realms

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

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



---

**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 Firepower 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 Firepower 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 Firepower 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 Firepower Management Center to retrieve user metadata from the servers. If the attribute names are incorrect on your server, the Firepower Management Center cannot populate its database with the information in that attribute.

Table 1: Map of attribute names to Firepower Management Center fields

Metadata	FMC Attribute	LDAP ObjectClass	Active Directory Attribute	OpenLDAP Attribute
LDAP user name	Username	<ul style="list-style-type: none"> <li>• user</li> <li>• inetOrgPerson</li> </ul>	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

### FTD License

Any

### Classic License

Control

# Requirements and Prerequisites for Realms

## Model Support

Any.

## Supported Domains

Any

## User Roles

- Admin
- Access Admin
- Network Admin

## Create a Realm

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

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

- [Export the Active Directory Server's Root Certificate, on page 14](#)
- [Find the Active Directory Server's Name, on page 13](#)

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 8](#) and [Realm Directory and Download fields, on page 11](#).



---

**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 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 Firepower Management Center. For more information, see [Realm Fields, on page 8](#).

### Procedure

---

- Step 1** Log in to the Firepower Management Center.
- Step 2** Click **System** > **Integration**.
- Step 3** Click **Realms**.
- Step 4** To create a new realm, click **Add Realm**.
- Step 5** To perform other tasks (such as enable, disable, or delete a realm), see [Manage a Realm, on page 19](#).
- Step 6** Enter realm information as discussed in [Realm Fields, on page 8](#).
- Step 7** (Optional.) Click **Test AD Join** to test the connection to the realm.
- Note** For a Microsoft Active Directory realm test to succeed, you must enter values in both the **AD Join Username** and **AD Join Password** fields and the user must have sufficient privileges to add computers to the domain. For more information, see [Realm Fields, on page 8](#).
- Step 8** Click **OK**.
- Step 9** Configure at least one directory as discussed in [Configure a Realm Directory, on page 15](#).
- Step 10** Configure user and user group download (required for access control) as discussed in [Download Users and Groups, on page 17](#).
- Step 11** Click **Realm Configuration**.
- Step 12** Enter user session timeout values, in minutes, for **ISE/ISE-PIC Users**, **TS 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 a Realm Directory, on page 15](#)
- Edit, delete, enable, or disable a realm; see [Manage a Realm, on page 19](#).
- [Compare Realms, on page 20](#).
- Optionally, monitor the task status; see [Viewing Task Messages](#).

## 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, testing the connection the AD connection 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 or **LDAP** for other supported LDAP repositories. For a list of supported LDAP repositories, see [Supported Servers for Realms, on page 3](#). You can authenticate captive portal users with an LDAP repository; all others require Active Directory.




---

**Note** Only captive portal supports an LDAP realm.

---

**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 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

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.

---

### 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 Microsoft Active Directory, the user does not need elevated privileges. You can specify any user in the domain.
- 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.

---

### Base DN

The directory tree on the server where the Firepower 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

The directory tree on the server where the Firepower 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 4](#).



**Note** Following is the list of characters the Firepower System *supports* in users, groups, DNs in your directory server. Using any characters other than the following could result in the Firepower System failing to download users and groups.

Entity	Supported characters
User name	<code>a-z A-Z 0-9 ! # \$ % ^ &amp; ( ) _ - { } ' . ~ `</code>
Group name	<code>a-z A-Z 0-9 ! # \$ % ^ &amp; ( ) _ - { } ' . ~ `</code>
Base DN and Group DN	<code>a-z A-Z 0-9 ! @ \$ % ^ &amp; * ( ) _ - . ~ ` [ ]</code>

### Group Attribute

(Optional.) The group attribute for the server, **Member** or **Unique Member**.

The following fields are available when you edit an existing realm.

### User Session Timeout

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 Firepower Management Center as Unknown (except for **Failed Captive Portal Users**).

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](#).

- **TS 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 Firepower 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 Download 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 13](#).

#### Port

The port to use for the Firepower Management Center-controller connection.

#### Encryption

(Strongly recommended.) The encryption method to use for the Firepower Management Center-server connection:

- **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 13](#).

#### SSL Certificate

The SSL certificate to use for authentication to the server. You must configure **STARTTLS** or **LDAPS** as the **Encryption** type in order to use an 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.

### User Download 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 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.

---

#### **Download users and groups (required for user access control)**

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

#### **Begin automatic download at, Repeat every**

Specifies the frequency of the automatic downloads.

#### **Download Now**

Click to synchronize groups and users with AD.

#### **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 **Add to Include** or **Add to Exclude** field.
- If you move groups to the **Add to Include** field, only those groups are downloaded and user data is available for user awareness and user control.
- If you move groups to the **Add to Exclude** field, all groups *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 **Groups to Include** and click **Add**.
- To exclude users from groups that are not excluded, enter the user name in the field below **Groups to Exclude** and click **Add**.




---

**Note** The users that are downloaded to the Firepower 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
- 

#### **Begin automatic download 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 FMC (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 FMC as a trusted CA certificate.
- 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 14

[Find the Active Directory Server's Name](#), on page 13

[Configure a Realm Directory](#), on page 15

## Find the Active Directory Server's Name

To configure a realm directory in the FMC, 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

- 
- |               |  |
|---------------|--|
| <b>Step 1</b> | Log in to the Active Directory server.   |
| <b>Step 2</b> | Click <b>Start</b> .   |
| <b>Step 3</b> | Right-click <b>This PC</b> .   |
| <b>Step 4</b> | Click <b>Properties</b> .  |
| <b>Step 5</b> | Click <b>Advanced System Settings</b> .  |
| <b>Step 6</b> | Click the <b>Computer Name</b> tab.  |
| <b>Step 7</b> | Note the value of <b>Full computer name</b> .<br>You must enter this exact name when you configure the realm directory in the FMC. |
- 

### What to do next

Create a realm directory.

### Related Topics

[Export the Active Directory Server's Root Certificate](#), on page 14

## 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 FMC 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

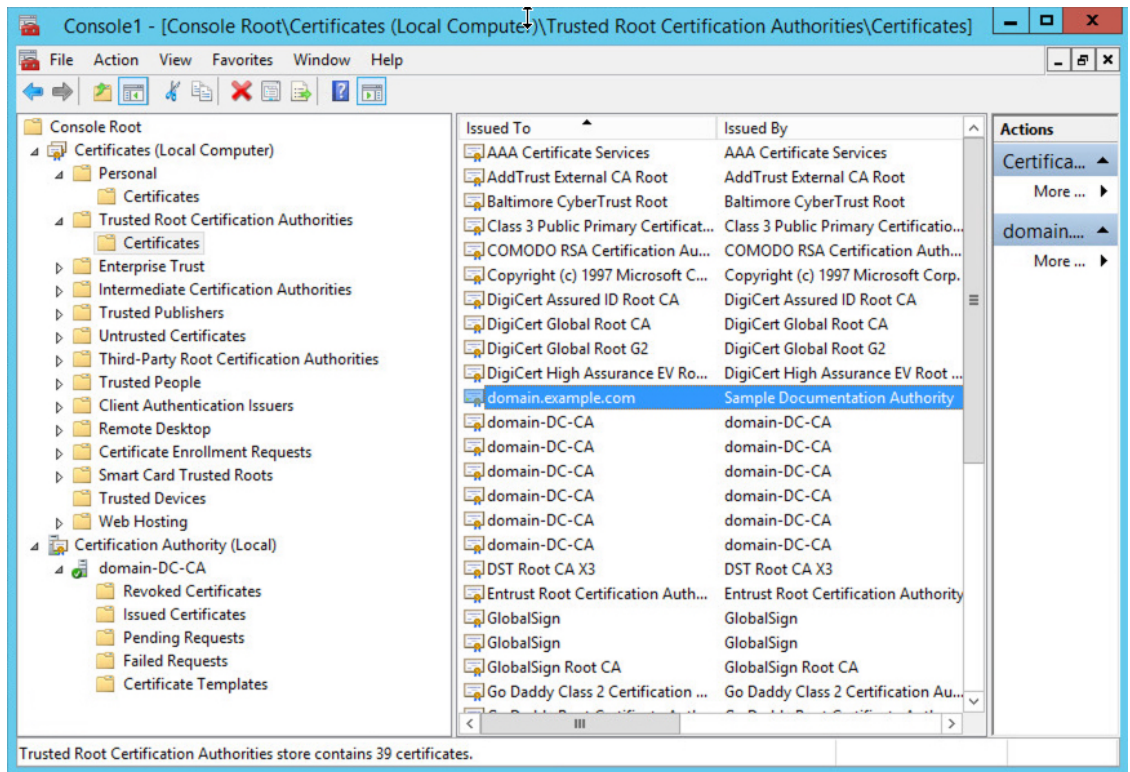
---

#### 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 FMC 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 FMC as a Trusted CA Certificate as discussed in [Adding a Trusted CA Object](#).

### Related Topics

[Find the Active Directory Server's Name](#), on page 13

## Configure a Realm Directory

This procedure enables you to create a realm directory, which corresponds to an LDAP server or a Microsoft Active Directory domain controller. An Active Directory server can have multiple domain controllers, each of which is capable of authenticating different users and groups.

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.

If you have not done so already, we recommend you start using TLS/SSL encryption to authenticate with an Active Directory server.

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.

For more information about realm directory configuration fields, see [Realm Fields, on page 8](#).

### Before you begin

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

- [Export the Active Directory Server's Root Certificate, on page 14](#)
- [Find the Active Directory Server's Name, on page 13](#)

### Procedure

- 
- Step 1** If you haven't done so already, log in to the Firepower Management Center and click **System > Integration > Realms**.
- Step 2** On Realms page, click the name of the realm for which to configure a directory.
- Step 3** On Directory page, click **Add Directory**.
- Step 4** Enter the **Hostname / IP Address** and **Port** for the LDAP server or Active Directory domain controller. The system sends an LDAP query to the hostname or IP address you specify. If the host name resolves to the IP address of an LDAP server or Active Directory domain controller, the **Test** succeeds.
- Step 5** Select an **Encryption Mode**.
- Step 6** Choose an **SSL Certificate** from the list or click **Add (+)** to add a certificate.
- Step 7** To test the connection, click **Test**.
- Step 8** Click **OK**.
- Step 9** Click **Save**. You are returned to Realms page
- Step 10** If you haven't already enabled the realm, on Realms page, slide **State** to enabled.
- 

### What to do next

- [Download Users and Groups, on page 17](#).

### Related Topics

- [Export the Active Directory Server's Root Certificate, on page 14](#)
- [Find the Active Directory Server's Name, on page 13](#)
- [Create a Realm Sequence, on page 18](#)



## Download Users and Groups

Smart License	Classic License	Supported Devices	Supported Domains	Access
Any	Control	Any	Any	Administrator, Access Admin, Network Admin

This section discusses how to download users and groups from your Active Directory server to the Firepower Management Center. If you do not specify any groups to include, the system retrieves user data for all the groups that match the parameters you provided. For performance reasons, Cisco recommends that you explicitly include only the groups that represent the users you want to use in access control.

The maximum number of users the Firepower Management Center can retrieve from the server depends on your Firepower Management Center model. If the download parameters in your realm are too broad, the Firepower Management Center obtains information on as many users as it can and reports the number of users it failed to retrieve in Task of the Message Center.

For more information about realm configuration fields, see [Realm Fields, on page 8](#).

### Procedure

- 
- Step 1** Log in to the Firepower Management Center.
- Step 2** Click **System > Integration > Realms**.
- Step 3** To download users and groups manually, click **Download** (↓) next to the realm to download users and user groups. If the controls are dimmed, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration. You can skip the remainder of this procedure.
- Step 4** To configure the realm for automatic user and group download, click **Edit** (✎) next to the realm to configure for automatic user and group download.
- Step 5** On User Access Control page, check **Download users and groups (required for user access control)**.
- Step 6** Select a time to **Begin automatic download at** from the lists.
- Step 7** Select a download interval from the **Repeat Every** list.
- Step 8** To include or exclude user groups from the download, choose user groups from the **Available Groups** column and click **Add to Include** or **Add to Exclude**.

Separate multiple users with commas. You can also use an asterisk (\*) as a wildcard character in this field.

**Note** You must **Add to Include** if you want to perform user control on users in that group.

Use the following guidelines:

- If you leave a group in the **Available Groups** box, the group is not downloaded.
- If you move a group to the **Add to Include** box, the group is downloaded and user data is available for user awareness and user control.
- If you move a group to the **Add to Exclude** box, the group is downloaded and user data is available for user awareness, but not for user control.
- To include users from groups that are not included, enter the user name in the field below **Groups to Include** and click **Add**.

- To exclude users from groups that are not excluded, enter the user name in the field below **Groups to Exclude** and click **Add**.

---

## Create a Realm Sequence

The following procedure enables you to create a realm sequence, which is an ordered list of realms the Firepower 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 Firepower System searches all the realms in the order specified in the realm sequence when applying an identity policy.

### Before you begin

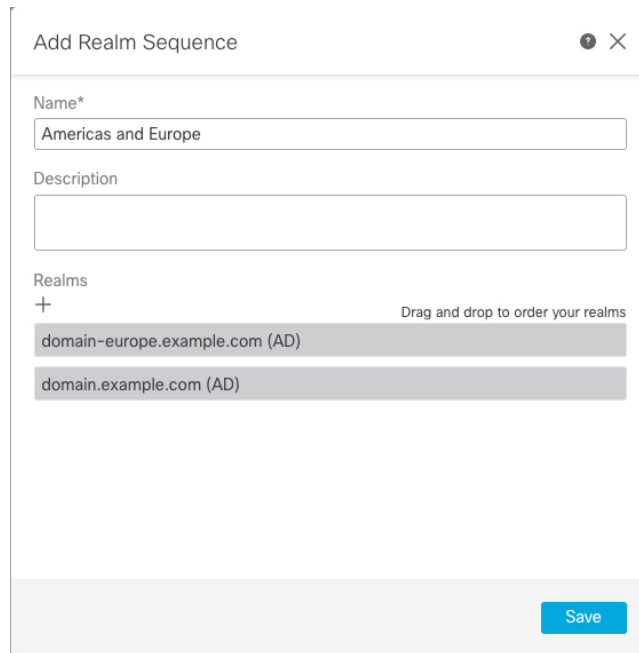
You must create and enable at least two realms, each corresponding to a connection with an Active Directory server. You cannot create realm sequences for LDAP realms.

- Create a directory as discussed in [Configure a Realm Directory, on page 15](#).
- Download users and groups and enable the realm as discussed in [Download Users and Groups, on page 17](#).

### Procedure

---

- Step 1** Log in to the Firepower Management Center if you have not already done so.
- Step 2** Click **System > Integration > 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 Firepower 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](#).

### Related Topics

[Configure a Realm Directory](#), on page 15

## Manage a Realm

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

- 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 Firepower Management Center.
- Step 2** Click **System** > **Integration**.
- Step 3** Click **Realms**.

- Step 4** To delete a realm, click **Delete** (🗑️).
- Step 5** To edit a realm, click **Edit** (✎) next to the realm and make changes as described in [Create a Realm, on page 6](#).
- Step 6** To enable a realm, slide **State** to the right; to disable a realm, slide it to the left.
- Step 7** To download users and user groups, click **Download** (↓).
- Step 8** To copy a realm, click **Copy** (📄).
- Step 9** To compare realms, see [Compare Realms, on page 20](#).
- 

## 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 Firepower Management Center.
- Step 2** Click **System > Integration**.
- Step 3** Click **Realms**.
- Step 4** Click **System > Integration**.
- Step 5** Click **Realms**.
- Step 6** Click **Compare Realms**.
- Step 7** Choose **Compare Realm** from the **Compare Against** list.
- Step 8** Choose the realms you want to compare from the **Realm A** and **Realm B** lists.
- Step 9** Click **OK**.
- Step 10** To navigate individually through changes, click **Previous** or **Next** above the title bar.
- Step 11** (Optional.) Click **Comparison Report** to generate the realm comparison report.
- Step 12** (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 Firepower Management Center's health monitor informs you of user or realm mismatches, which are defined as:

- User mismatch: A user is reported to the Firepower 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 Firepower Management Center. Review the information discussed in [Realm Fields, on page 8](#).
- Realm mismatch: A user logs into a domain that corresponds to a realm not known to the Firepower Management Center.

For example, if you defined a realm that corresponds to a domain named **domain.example.com** in the Firepower 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 Firepower 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 23](#).

**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, Firepower 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 Firepower 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 Firepower 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 server is synchronized with the time on the Firepower 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 Firepower Management Center. If the appliances are not synchronized, the system may perform user timeouts at unexpected intervals.

**Symptom: Users are not included or excluded as specified in your realm configuration**

If you configure an Active Directory realm that includes or excludes users who are members of a sub-group on your server, note that Microsoft Windows servers limit the number of users they report:

- 5000 users per group on Microsoft Windows Server 2012

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

**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 Firepower system expects and what the repository provides. For example, if you configure **Type** as **LDAP** for a Microsoft Active Directory realm, the Firepower 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.

**Symptom: User data for previously-unseen ISE 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 may 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 Firepower 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 Firepower 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 Firepower Management Center. Review the information discussed in [Realm Fields, on page 8](#).
- Realm mismatch: A user logs into a domain that corresponds to a realm not known to the Firepower Management Center.

For additional details, see [Troubleshoot Realms and User Downloads, on page 20](#).

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 Firepower 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 20](#).
- 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](#).

### 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 Firepower 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.

---

## Related Topics

- [Health Policies](#)
- [Configuring Health Monitoring](#)
- [Health Monitor Status Categories](#)



## History for Realms

Feature	Version	Details
Realm sequence	6.7.0	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.
Realms for user control.	—	Feature introduced before Version 6.0. A realm is a connection between the FMC either an Active Directory or LDAP user repository.

