Realms and Identity Policies

The following topics describe realms and identity policies:

About Realms and Identity Policies

A *realm* consists of one or more LDAP or Microsoft Active Directory servers that share the same directory credentials. You must configure a realm to perform user and user group queries, user control, or to configure an authoritative identity source. After configuring one or more realms, you can configure an identity policy.

An *identity policy* associates traffic on your network with an authoritative identity source and a realm. After configuring one or more identity policies, you can associate one with an access control policy and deploy the access control policy to a managed device.

About Realms

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 user agent, a TS Agent, or ISE/ISE-PIC.

You can add multiple domain controllers as directories in a realm, but they must share the same basic realm information. The directories in a realm must be exclusively LDAP or exclusively Active Directory (AD)

servers. After you enable a realm, your saved changes take effect next time the 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 for an AD server or for either the user agent or ISE/ISE-PIC

Note Configuring a realm is optional if you plan to configure SGT ISE attribute conditions but not user, group, realm, Endpoint Location, or Endpoint Profile conditions.

- A realm 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 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 or a user agent. 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.

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 User Agent data retrieval?	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 2008 and Windows Server 2012	No User agent supported on Windows Server 2008 and 2012 only	Yes	Yes	Yes

Server Type	Supported for User Agent data retrieval?	Supported for ISE/ISE-PIC data retrieval?	Supported for TS Agent data retrieval?	Supported for captive portal data retrieval?
OpenLDAP on Linux	No	No	No	Yes

Note If the TS Agent is installed on a Microsoft Active Directory Windows Server shared with another passive authentication identity source (the User Agent or 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 or 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 2008 or 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	• 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

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 User Agent Identity Source
- 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: 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 user agent or 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, user agent, 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 2008 or 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 and User Agent users is not displaying in the web interface

After the system detects activity from an ISE/ISE-PIC, user agent, 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, user agent, 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*.

About Identity Policies

Identity policies contain identity rules. Identity rules associate sets of traffic with a realm and an authentication method: passive authentication, active authentication, or no authentication.

With the exception noted in the following paragraphs, you must configure realms and authentication methods you plan to use before you can invoke them in your identity rules:

- You configure realms outside of your identity policy, at **System** > **Integration** > **Realms**. For more information, see Create a Realm, on page 9.
- You configure the user agent and ISE/ISE-PIC, passive authentication identity sources, at **System** > **Integration** > **Identity Sources**. For more information, see Configure the User Agent for User Control and Configure ISE/ISE-PIC for User Control.
- You configure the TS Agent, a passive authentication identity source, outside the Firepower System. For more information, see the *Cisco Terminal Services (TS) Agent Guide*.
- You configure captive portal, an active authentication identity source, within the identity policy. For more information, see How to Configure the Captive Portal for User Control.
- You configure Remote Access VPN, an active authentication identity source, in Remote Access VPN policies. For more information, see Remote Access VPN Authentication.

After you add multiple identity rules to a single identity policy, order the rules. The system matches traffic to rules in top-down order by ascending rule number. The first rule that traffic matches is the rule that handles the traffic.

After you configure one or more identity policies, you must associate one identity policy with your access control policy. When traffic on your network matches the conditions in your identity rule, the system associates the traffic with the specified realm and authenticates the users in the traffic using the specified identity source.

If you do not configure an identity policy, the system does not perform user authentication.

Exception to creating an identity policy

An identity policy is not required if all of the following are true:

- You use the ISE/ISE-PIC identity source.
- You do not use users or groups in access control policies.
- You use Security Group Tags (SGT) in access control policies. For more information, see ISE SGT vs Custom SGT Rule Conditions.

Video YouTube video on creating an identity policy and rule.

Related Topics

User Identity Sources

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

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

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 10.

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 27.

Step 6 Enter realm information as discussed in Realm Fields, on page 10.

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 10.

Step 8 Click **OK**.

Step 9 Configure at least one directory as discussed in Configure a Realm Directory, on page 20.

Step 10 Configure user and user group download (required for access control) as discussed in Download Users and Groups, on page 21.

Step 11 Click **Realm Configuration**.

Step 12 Enter user session timeout values, in minutes, for **User Agent and 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 20
- Edit, delete, enable, or disable a realm; see Manage a Realm, on page 27.
- Compare Realms, on page 27.
- Optionally, monitor the task status; see Viewing Task Messages.

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	**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 ! @ $ % ^ & * ( ) _ - . ~ ` [ ]**

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 applies to SGT mappings from a pxGrid session topic (for example, 802.1x authentication).

  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 16.

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 15.

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.

Realms and Identity Policies

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 16
Find the Active Directory Server's Name, on page 16
Configure a Realm Directory, on page 20

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

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 FMC.

What to do next

Create a realm directory.

Related Topics

Export the Active Directory Server's Root Certificate, on page 16

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.

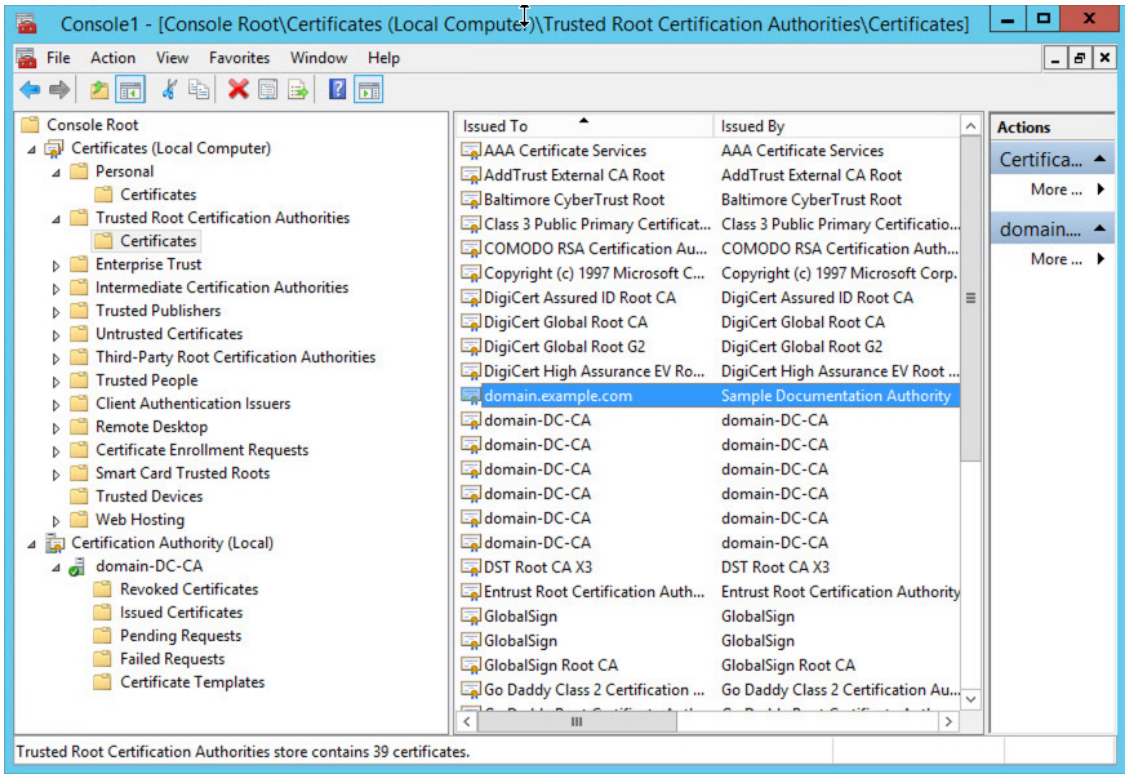
Before you begin

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.

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

c) Copy the entire certificate to the clipboard, starting with **-----BEGIN CERTIFICATE-----** and ending with **-----END CERTIFICATE-----** (including those strings).

What to do next

Import the Active Directory server's certificate into the 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 16

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.

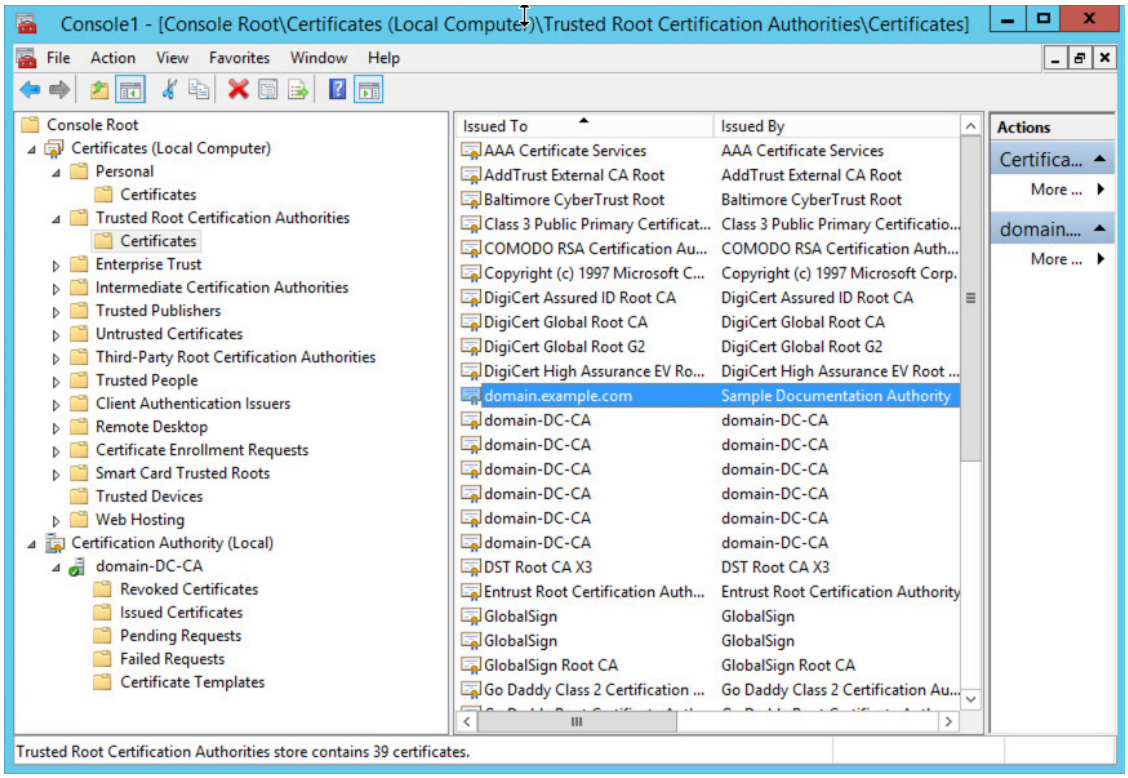
Before you begin

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.

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

What to do next

Import the Active Directory server's certificate into the 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 16

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

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 FMC.

What to do next

Create a realm directory.

Related Topics

Export the Active Directory Server's Root Certificate, on page 16

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 10.

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 16
- Find the Active Directory Server's Name, on page 16

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 21.

Related Topics

Export the Active Directory Server's Root Certificate, on page 16
Find the Active Directory Server's Name, on page 16

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 10.

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 an Identity Policy

Before you begin

An identity policy is required to use users and groups in a realm in access control policies. Create and enable one or more realms as described in Create a Realm, on page 9.

An identity policy is not required if all of the following are true:

- You use the ISE/ISE-PIC identity source.
- You do not use users or groups in access control policies.

- You use Security Group Tags (SGT) in access control policies. For more information, see ISE SGT vs Custom SGT Rule Conditions.

Procedure

Step 1 Log in to the Firepower Management Center.

Step 2 Click **Policies** > **Access Control** > **Identity** and click **New Policy**.

Step 3 Enter a **Name** and, optionally, a **Description**.

Step 4 Click **Save**.

Step 5 To add a rule to the policy, click **Add Rule** as described in Create an Identity Rule, on page 23.

Step 6 To create a rule category, click **Add Category**.

Step 7 To configure captive portal active authentication, click **Active Authentication** as described in Configure the Captive Portal Part 1: Create an Identity Policy.

Step 8 Click **Save** to save the identity policy.

What to do next

- Add rules to your identity policy that specify which users to match and other options; see Create an Identity Rule, on page 23.
- Associate the identity policy with an access control policy to allow or block selected users from accessing specified resources; see Associating Other Policies with Access Control.
- Deploy configuration changes to managed devices; see Deploy Configuration Changes.

If you encounter issues, see Troubleshoot User Control.

Create an Identity Rule

For details about configuration options for identity rules, see Identity Rule Fields, on page 24.

Before you begin

You must create and enable a realm.

- Create a realm as discussed in Create a Realm, on page 9.
- Create a directory as discussed in Configure a Realm Directory, on page 20.
- Download users and groups and enable the realm as discussed in Download Users and Groups, on page 21.

Procedure

Step 1 If you haven't done so already, log in to the Firepower Management Center.

Step 2 Click **Policies** > **Access Control** > **Identity** .

Step 3 Click **Edit** ( ) next to the identity policy to which to add the identity rule.

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

Step 4 Click **Add Rule**.

Step 5 Enter a **Name**.

Step 6 Specify whether the rule is **Enabled**.

Step 7 To add the rule to an existing category, indicate where you want to **Insert** the rule. To add a new category, click **Add Category**.

Step 8 Choose a rule **Action** from the list.

Step 9 Click **Realms & Settings**.

Step 10 Choose a realm for the identity rule from the **Realms** list. You must associate a realm with every identity rule.

The only exception to the realm requirement is implementing user control using only the ISE SGT attribute tag. In this case, you do not need to configure a realm for the ISE server. ISE SGT attribute conditions can be configured in policies with or without an associated identity policy.

Step 11 If you're configuring captive portal, see How to Configure the Captive Portal for User Control.

Step 12 (Optional) To add conditions to the identity rule, see Rule Condition Types.

Step 13 Click **Add**.

Step 14 In the policy editor, set the rule position. Click and drag or use the right-click menu to cut and paste. Rules are numbered starting at 1. The system matches traffic to rules in top-down order by ascending rule number. The first rule that traffic matches is the rule that handles that traffic. Proper rule order reduces the resources required to process network traffic and prevents rule preemption.

Step 15 Click **Save**.

Related Topics

Snort® Restart Scenarios

Identity Rule Fields

Use the following fields to configure identity rules.

Enabled

Choosing this option enables the identity rule in the identity policy. Deselecting this option disables the identity rule.

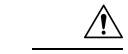
Action

Specify the type of authentication you want to perform on the users in the specified realm: **Passive Authentication** (default), **Active Authentication**, or **No Authentication**. You must fully configure the authentication method, or *identity source*, before selecting it as the action in an identity rule.

Additionally, if VPN is enabled (configured on at least one managed device), remote access VPN sessions are actively authenticated by VPN. Other sessions use the rule action. This means that, if VPN is enabled, VPN identity determination is performed first for all sessions regardless of the selected action. If a VPN

identity is found on the specified realm, this is the identity source used. No additional captive portal active authentication is done, even if selected.

If the VPN identity source is not found, the process continues according to the specified action. You cannot restrict the identity policy to VPN authentication only because if the VPN identity is not found, the rule is applied according to the selected action.



Caution Adding the first or removing the last active authentication rule when SSL decryption is disabled (that is, when the access control policy does not include an SSL policy) restarts the Snort process when you deploy configuration changes, temporarily interrupting traffic inspection. Whether traffic drops during this interruption or passes without further inspection depends on how the target device handles traffic. See Snort® Restart Traffic Behavior for more information.

Note that an active authentication rule has either an **Active Authentication** rule action, or a **Passive Authentication** rule action with **Use active authentication if passive or VPN identity cannot be established** selected.

For information about which passive and active authentication methods are supported in your version of the Firepower System, see About User Identity Sources.

Realm

The realm containing the users you want to perform the specified **Action** on. You must fully configure a realm before selecting it as the realm in an identity rule.

Note If remote access VPN is enabled and your deployment is using a RADIUS server group for VPN authentication, make sure you specify the realm associated with this RADIUS server group.

Note If you select **`Kerberos`** (or **`HTTP Negotiate`**, if you want Kerberos as an option) as the **Authentication Protocol** for the 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.

Use active authentication if passive or VPN identity cannot be established

Selecting this option authenticates users using captive portal active authentication if a passive or a VPN authentication fails to identify them. You must configure captive portal active authentication in your identity policy in order to select this option.

If you disable this option, users that do not have a VPN identity or that passive authentication cannot identify are identified as Unknown.

Identify as Special Identities/Guest if authentication cannot identify user

Selecting this option allows users who fail captive portal active authentication the specified number of times times to access your network as a guest. These users appear in the Firepower Management Console identified by their username (if their username exists on the AD or LDAP server) or by **Guest** (if their user name is unknown). Their realm is the realm specified in the identity rule. (By default, the number of failed logins is 3.)

This field is displayed only if you configure **Active Authentication** (that is, captive portal authentication) as the rule **Action**.

Authentication Protocol

The method to use to perform captive portal active authentication. The selections vary depending on the type of realm, LDAP or AD:

- Choose **HTTP Basic** if you want to authenticate users using an unencrypted HTTP Basic Authentication (BA) connection. Users log in to the network using their browser's default authentication popup window.

  Most web browsers cache the credentials from **HTTP Basic** logins and use the credentials to seamlessly begin a new session after an old session times out.

- Choose **NTLM** to authenticate users using a NT LAN Manager (NTLM) connection. This selection is available only when you select an AD realm. If transparent authentication is configured in a user's browser, the user is automatically logged in. If transparent authentication is not configured, users log in to the network using their browser's default authentication popup window.
- Choose **Kerberos** to authenticate users using a Kerberos connection. This selection is available only when you select an AD realm for a server with secure LDAP (LDAPS) enabled. If transparent authentication is configured in a user's browser, the user is automatically logged in. If transparent authentication is not configured, users log in to the network using their browser's default authentication popup window.

Note The **Realm** you select must be configured with an **AD Join Username** and **AD Join Password** to perform Kerberos captive portal active authentication.

Note If you are creating an identity rule to perform Kerberos captive portal and you have DNS resolution configured, you must configure your DNS server to resolve the fully qualified domain name (FQDN) of the captive portal device. The FQDN must match the host name you provided when configuring DNS.

For ASA with FirePOWER Services and Firepower Threat Defense devices, the FQDN must resolve to the IP address of the routed interface used for captive portal.

- Choose **HTTP Negotiate** to allow the captive portal server to choose between HTTP Basic, Kerberos, or NTLM for the authentication connection. This type is available only when you select an AD realm.

Note The **Realm** you choose must be configured with an **AD Join Username** and **AD Join Password** for **HTTP Negotiate** to choose Kerberos captive portal active authentication.

Note If you are creating an identity rule to perform **HTTP Negotiate** captive portal and you have DNS resolution configured, you must configure your DNS server to resolve the fully qualified domain name (FQDN) of the captive portal device. The FQDN of the device you are using for captive portal must match the hostname you provided when configuring DNS.

For ASA with FirePOWER Services devices, the FQDN is the FQDN of the ASA FirePOWER module.

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 9.

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 27.

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.

Manage an Identity Policy

In a multidomain deployment, the system displays policies created in the current domain, which you can edit. It also displays policies created in ancestor domains, which you cannot edit. To view and edit policies created in a lower domain, switch to that domain.

Procedure

Step 1 If you haven't done so already, log in to the Firepower Management Center.
Step 2 Click **Policies** > **Access Control** > **Identity** .
Step 3 To delete a policy, click **Delete** ( ). If the controls are dimmed, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.
Step 4 To edit a policy, click **Edit** ( ) next to the policy and make changes as described in Create an Identity Policy, on page 22. If **View** ( ) appears instead, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.
Step 5 To copy a policy, click **Copy** ( ).
Step 6 To generate a report for the policy, click **Report** ( ) as described in Generating Current Policy Reports.
Step 7 To compare policies, see Comparing Policies.

Manage an Identity Rule

Procedure

Step 1 If you haven't already done so, log in to the Firepower Management Center.

Step 2 Click **Policies** > **Access Control** > **Identity** .

Step 3 Click **Edit** ( ) next to the policy you want to edit. If **View** ( ) appears instead, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.

Step 4 To edit an identity rule, click **Edit** ( ) and make changes as described in Create an Identity Policy, on page 22.

Step 5 To delete an identity rule, click **Delete** ( ).

Step 6 To create a rule category, click **Add Category** and choose the position and the rule.

Step 7 Click **Save**.

What to do next

- Deploy configuration changes; see Deploy Configuration Changes.

History for Realms

Feature	Version	Details
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.