

# Identity Overview

The following topics discuss user identity:


- User identity, on page 1
- Host and user limits, on page 11
- Recommendation: identity realm limit, on page 14


# User identity

User identity information can help you to identify the source of policy breaches, attacks, or network vulnerabilities, and trace them to specific users.

User identity information can help you determine:

- Who owns the host targeted by an intrusion event that has a Vulnerable (level 1: red) impact level.
- Who initiated an internal attack or portscan.
- Who is attempting unauthorized access to a specified host.
- Who is consuming an unreasonable amount of bandwidth.
- Who has not applied critical operating system updates.
- Who is using instant messaging software or peer-to-peer file-sharing applications in violation of company policy.
- Who is associated with each indication of compromise on your network.

Armed with this information, you can use other features of the system to mitigate risk, perform access control, and take action to protect others from disruption. These capabilities also significantly improve audit controls and enhance regulatory compliance.

After you configure user identity sources to gather user data, you can perform user awareness and user control.

For more information about identity sources, see About user identity sources, on page 2.

### Related Topics


Identity terminology, on page 2
About user identity sources, on page 2
Identity deployments, on page 5
Set up an identity policy, on page 7

# Identity terminology

Identity terminology is a set of concepts that

- identifies users on networks using identity sources
- enables user awareness from authoritative and non-authoritative sources, and
- manages user access using identity policies.

### Key identity terminology

This topic discusses common terminology for user identity and user control.

- **User awareness**: Identifying users on your network using *identity sources* (such as, TS Agent, or Cisco ISE). User awareness enables you to identify users from both *authoritative* (such as Active Directory) and *non-authoritative* (application-based) sources. To use Active Directory as an identity source, you must configure a realm and directory. For more information, see About user identity sources, on page 2.
- **User control**: Configuring an *identity policy* that you associate with an *access control policy*. (The identity policy is then referred to as an access control *subpolicy*.) The identity policy specifies the identity source and, optionally, users and groups belonging to that source. By associating the identity policy with an access control policy, you determine whether to monitor, trust, block, or allow users or user activity in traffic on your network. For more information, see Access Control Policies.
- **Authoritative identity source**: a trusted server that validates user logins (for example, Active Directory). You can use the data obtained from authoritative logins to perform user awareness and user control. Authoritative user logins are obtained from passive and active authentications:
  - *Passive authentications* occur when a user authenticates through an external repository. ISE/ISE-PIC, the TS Agent, and Microsoft Active Directory are passive authentication user repositories supported by the system.
  - *Active authentications* occur when a user authenticates through preconfigured managed devices. Captive portal is another name for active authentication. Active authentication generally uses the same user repositories as passive authentication (the exceptions being ISE/ISE-PIC, and TS Agent, which are passive only).
- **Non-authoritative identity source**: an unknown or untrusted server that validates the user login. Traffic-based detection is the only non-authoritative identity source supported by the system. You can use the data obtained from non-authoritative logins to perform user awareness.

# About user identity sources

Learn how to select and configure user identity sources for the firewall to enable user awareness and access control policies. This overview covers supported identity sources, authentication types, and key considerations for optimizing user identity management.

The table provides a brief overview of the user identity sources supported by the system. Each identity source provides a store of users for user awareness. These users can then be controlled with identity and access control policies.

| User Identity Source | Server Requirements | Login Type | Authentication Type | User Control | For more, see... |
|---|---|---|---|---|---|
| Captive portal | OpenLDAP<br>Microsoft Active Directory | Authoritative | Active | Yes | Captive portal identity source |
| Passive authentication | OpenLDAP<br>Microsoft Active Directory | Non-authoritative | Active | Yes | Create an LDAP realm or an Active Directory realm and realm directory |
| Passive authentication with the TS Agent | Microsoft Windows Terminal Server | Authoritative | Passive | Yes | Terminal services agent identity source |
| Remote Access VPN | OpenLDAP or Microsoft Active Directory | Authoritative | Active | Yes | Remote access VPN identity sources |
| | RADIUS | Authoritative | Active | No, awareness only | |
| ISE/ISE-PIC | Microsoft Active Directory | Authoritative | Passive | Yes | The ISE/ISE-PIC identity source |
| Traffic-based detection<br>(Configured in the network discovery policy.) | — | Non-authoritative | — | No, awareness only | Traffic-based detection identity sources |

Consider the information when selecting identity sources to deploy:

- You must use traffic-based detection for non-LDAP user logins.
- You must use traffic-based detection or captive portal to record failed login or authentication activity. A failed login or authentication attempt does not add a new user to the list of users in the database.
- The captive portal identity source requires a managed device with a routed interface. You *cannot* use an inline (also referred to as tap mode) interface with captive portal.

Data from those identity sources is stored in the Secure Firewall Management Center's users database and the user activity database. You can configure Secure Firewall Management Center-server user downloads to automatically and regularly download new user data to your databases.

After you configure identity rules using the desired identity source, you must associate each rule with an access control policy and deploy the policy to managed devices for the policy to have any effect. For more information about access control policies and deployment, see Associate prefilter, decryption, and identity policies with an access control.

For general information about user identity, see User identity, on page 1.

# Best practices for user identity

## General recommendations for identity policy setup

Review the following recommendations before you set up identity policies.

- Know user limits
- Health monitor
- Use latest version of ISE/ISE-PIC, two types of remediation
- User agent support drops in 6.7
- Captive portal requires routed interface, several individual tasks

## Microsoft active directory and LDAP

Create one realm per LDAP server or Active Directory domain. The system supports Active Directory, LDAP, and other user repositories for user awareness and control. The association between an Active Directory or LDAP repository and the Secure Firewall Management Center is referred to as a *realm*. For details about which versions are supported, see Supported servers for realms.

- The only user identity source supported by LDAP is captive portal. To use other identity sources (with the exception of ISE/ISE-PIC), you must use Active Directory.
- For Active Directory only: Create one *directory* per domain controller. For details, see Create an LDAP realm or an Active Directory realm and realm directory
- Users and groups in trust relationships between two domains are supported provided you add all Active Directory domains and domain controllers as realms and directories, respectively. For more information, see Realms and trusted domains.

## Passive Identity Agent identity source
## pxGrid Cloud Identity Source
## Proxy sequence
## Health monitor

The Secure Firewall Management Center health monitor provides valuable information about the status of various Secure Firewall Management Center functions, including user/realm mismatches, Snort memory usage, and ISE connection status.

- For more information about health modules, see *Health Modules* in the *Cisco Secure Firewall Management Center Administration Guide*.
- To set up policies to monitor health modules, see *Creating Health Policies* in the *Cisco Secure Firewall Management Center Administration Guide*.

## Device-specific user limits

Every physical or virtual Firewall Management Center device has limits to the number of users that can be downloaded. When the user limit is reached, the Firewall Management Center can run out of memory and can function unreliably as a result.

- User limits are discussed in User limits for microsoft active directory, on page 12.

- If you use the ISE/ISE-PIC identity source, you can optionally limit the subnets the Firewall Management Center monitors to reduce memory usage using identity mapping filters as discussed in Create an identity policy.

### Use the latest version of ISE/ISE-PIC

If you expect to use the ISE/ISE-PIC identity source, we strongly recommend you always use the latest version to make sure you get the latest features and bug fixes.

- pxGrid 2.0 (which is used by version 2.6 patch 6 or later; or 2.7 patch 2 or later) also changes the remediation used by ISE/ISE-PIC from Endpoint Protection Service (EPS) to Adaptive Network Control (ANC). If you upgrade ISE/ISE-PIC, you must migrate your mediation policies from EPS to ANC.
- More information about using ISE/ISE-PIC can be found in Best practices for ISE/ISE-PIC integration.
- To set up the ISE/ISE-PIC identity source, see ISE/ISE-PIC configurations for user control.

### Captive portal information
### TS agent information

The TS Agent user identity source is required to identify user sessions on a Windows Terminal Server. The TS Agent software must be installed on the Terminal Server machine as discussed in the *Cisco Terminal Services (TS) Agent Guide*. In addition, you must synchronize the time on your TS Agent server with the time on the Secure Firewall Management Center.

- TS Agent data is visible in the Users, User Activity, and Connection Event tables and can be used for user awareness and user control.
- For more information, see Best practices for TS agent configuration.

### Associate the identity policy with an access control policy

After you configure your realm, directory, and user identity source, you must set up identity rules in an identity policy. To make the policy effective, you must associate the identity policy with an access control policy.

- For more information about creating an identity policy, see Create an identity policy.
- For more information about creating identity rules, see Create an identity rule.
- To associate an identity policy with an access control policy, see Associate prefilter, decryption, and identity policies with an access control.

# Identity deployments

The Secure Firewall Management Center uses various identity sources, such as TS Agent, ISE/ISE-PIC, pxGrid Cloud, passive identity agent, and captive portal, to collect and manage user and group data for access control and user awareness.

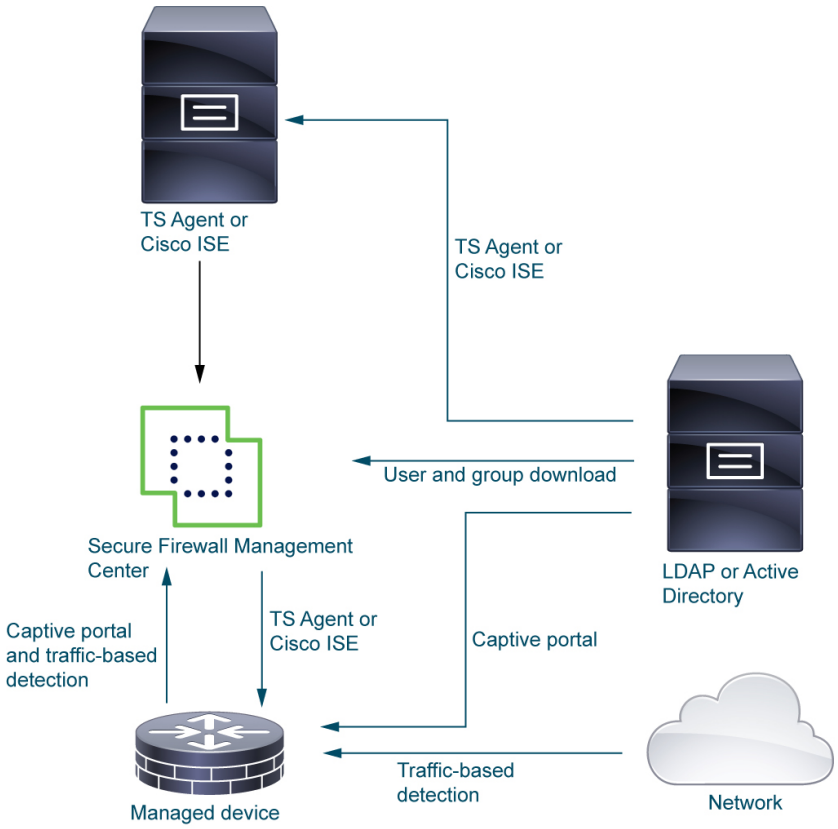
#### User data collection and storage

When the system detects user data from a user login, from any identity source, the user from the login is checked against the list of users in the Secure Firewall Management Center user database. If the login user matches an existing user, the data from the login is assigned to the user. Logins that do not match existing

users cause a new user to be created, unless the login is in SMTP traffic. Non-matching logins in SMTP traffic are discarded.

The group to which the user belongs is associated with the user as soon as the user is seen by the Secure Firewall Management Center.

This diagram illustrates how the system collects and stores user data:




Here are examples of identity deployments.

In the preceding figure, Secure Firewall Management Center and one managed device are deployed to AWS and the other devices are located on premises. These devices can be either physical or virtual; they just need to be able to communicate with each other.

LDAP or Active Directory are required only for TS Agent and captive portal, as the following paragraphs explain.

For more information about setting up a system like this, see Set up an identity policy, on page 7.

### ISE/ISE-PIC identity source

When you deploy the ISE/ISE-PIC identity source, the ISE/ISE-PIC server sends users, groups, and subscriptions to the Secure Firewall Management Center.

You can optionally have an LDAP server in an ISE/ISE-PIC deployment but because it's optional, it isn't shown in this figure.

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

### TS Agent identity source

The Terminal Services (TS) Agent software runs on a Microsoft Server and sends Secure Firewall Management Center user information based on the port range the users log in to the server with. TS Agent gets user identity information from LDAP or Active Directory and sends it to Secure Firewall Management Center.

For more information about the TS Agent identity source, see Terminal services agent identity source.

### Captive portal

# Set up an identity policy

Set up an identity policy to control user access and filter network traffic using various user identity sources such as TS Agent, ISE/ISE-PIC, captive portal.

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

- You use the ISE or 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 SGTs versus custom SGT rule conditions.

This topic provides a high-level overview of setting up an identity policy using any available user identity source: TS Agent, ISE/ISE-PIC, captive portal.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | (Optional.) Create a realm and directory, one realm for every domain in the forest that contain users you want to use in user control. Also create one directory for every domain controller. Only users and groups that have corresponding Firewall Management Center realms and directories can be used in identity policies. | Creating a realm, realm directory is optional if any of these are true:<br>• You use SGT ISE attribute conditions but not user, group, realm, Endpoint Location, or Endpoint Profile conditions.<br>• You are using an identity policy only to filter network traffic.<br><br>The *realm* is a trusted user and group store, typically a Microsoft Active Directory repository. The Firewall Management Center downloads users and groups at intervals you specify. You can include or exclude users and groups from being downloaded.<br><br>See Create an LDAP realm or an Active Directory realm and realm directory. For details about the options to create a realm, see Realm fields.<br><br>A *directory* is an Active Directory domain controller that organizes information about a |

| | Command or Action | Purpose |
|---|---|---|
| | | computer network's users and network shares. An Active Directory controller provides Directory Services for the realm. Active Directory distributes user and group objects across multiple domain controllers, which are peers that propagate local changes between each other by the use of Directory Services. For more information, see the Active Directory technical specification glossary on MSDN.<br><br>You can specify more than one directory for a realm, in which case each domain controller is queried in the order listed on the realm's **Directory** tab page to match user and group credentials for user control.<br><br>**Note**<br>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. |
| **Step 2** | Synchronize users and groups from the realm. | To be able to control users and groups, you must synchronize them with the Firewall Management Center. You can synchronize them with users and groups whenever you want or you can configure the system to synchronize them at a specified interval.<br><br>When you synchronize users and groups, you can specify exceptions; for example, you can exclude the Engineering group from all user control for that realm, or you can exclude the user **`joe.smith`** from user controls that apply to the Engineering group.<br><br>See Synchronize users and groups |
| **Step 3** | (Optional.) Create a realm sequence. | A realm sequence is an ordered list of realms that, when used in an identity policy, causes the system to search the realms in the specified order to find users to match the rule. See Create a realm sequence. |
| **Step 4** | Create a method to retrieve user and group data (the *identity source*). | Set up an identity source with its unique configuration to be able to control users and groups using data stored in the realm. Identity sources include TS Agent, captive portal, or Remote VPN. See one of these: |

| | Command or Action | Purpose |
|---|---|---|
| | | • Configure the captive portal for user control<br>• Configure Remote Access VPN for AD-authenticated users |
| **Step 5** | Create an identity policy. | An identity policy contains one or more identity rules, optionally organized in categories. See Create an identity policy.<br>**Note**<br>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. |
| **Step 6** | Create one or more identity rules. | Identity rules enable you to specify a number of matching criteria, including the type of authentication, network zones, networks or geolocation, realms, realm sequences, and so on. See Create an identity rule. |
| **Step 7** | Associate your identity policy with an access control policy. | An access control policy filters and optionally inspects traffic. An identity policy must be associated with an access control policy to have any effect. See Associate prefilter, decryption, and identity policies with an access control. |

### What to do next

1. Deploy the access control policy to at least one managed device.

   To use your policy to control user activity, the policy must be deployed to the managed devices to which clients connect. See Deploy configuration changes.

2. Monitor user activity.

   View a list of active sessions collected by user identity sources or a list of user information collected by user identity sources. See *Using Workflows* in the *Cisco Secure Firewall Management Center Administration Guide* .

### Related Topics

Configure Traffic-Based user detection

# User activity database

The user activity database on the Secure Firewall Management Center is a logging system that contains records of user activity on your network detected or reported by all of your configured identity sources.

### User activity logging events

The system logs events in these circumstances:

- When it detects individual logins or logoffs.
- When it detects a new user.
- When a system administrator manually delete a user.
- When the system detects a user that is not in the database, but cannot add the user because you have reached your user limit.
- When you resolve an indication of compromise associated with a user, or enable or disable indication of compromise rules for a user.



**Note** If the TS Agent monitors the same users as another passive authentication identity source (such as the ISE/ISE-PIC), the Firewall Management Center prioritizes the TS Agent data. If the TS Agent and another passive source report identical activity from the same IP address, only the TS Agent data is logged to the Firewall Management Center.

You can view user activity detected by the system using the Secure Firewall Management Center. (**Analysis** > **Users heading** > **User Activity**.)

# Users database

A users database on the Secure Firewall Management Center is a system component that

- contains a record for each user detected or reported by all configured identity sources
- stores data obtained from authoritative sources for user control, and
- prioritizes user data based on identity source type when user limits are reached.

### User database management and limitations

For more information about the supported non-authoritative and authoritative identity sources, refer to About user identity sources, on page 2.

The total number of users the Secure Firewall Management Center can store depends on the Secure Firewall Management Center model, as described in User limits for microsoft active directory, on page 12. After the user limit is reached, the system prioritizes previously-undetected user data based on its identity source, as described in this list:

- Non-authoritative identity source: If the new user is from a non-authoritative identity source, the system does not add the user to the database. To allow new users to be added, you must delete users manually or with a database purge.
- Authoritative identity source: If the new user is from an authoritative identity source, the system deletes the non-authoritative user who has remained inactive for the longest period and adds the new user to the database.

If an identity source is configured to exclude specific user names, user activity data for those user names are not reported to the Secure Firewall Management Center. These excluded user names remain in the database, but are not associated with IP addresses. For more information about the type of data stored by the system, refer to *User Data* in the *Cisco Secure Firewall Management Center Administration Guide*.

If you have Firewall Management Center high availability configured and the primary fails, no logins reported by a captive portal, ISE/ISE-PIC, TS Agent, or Remote Access VPN device can be identified during failover downtime, even if the users were previously seen and downloaded to the Firewall Management Center. The unidentified users are logged as Unknown users on the Firewall Management Center. After the downtime, the Unknown users are reidentified and processed according to the rules in your identity policy.

**Note** If the TS Agent monitors the same users as another passive authentication identity source (ISE/ISE-PIC), the Firewall Management Center prioritizes the TS Agent data. If the TS Agent and another passive source report identical activity from the same IP address, only the TS Agent data is logged to the Firewall Management Center.

When the system detects a new user session, the user session data remains in the users database until one of these conditions occurs:

- A user on the Firewall Management Center manually deletes the user session.
- An identity source reports the logoff of that user session.
- A realm ends the user session as specified by the realm's **User Session Timeout: Authenticated Users**, **User Session Timeout: Failed Authentication Users**, or **User Session Timeout: Guest Users** setting.

# Host and user limits

Host and user limits are deployment restrictions that determine how many individual hosts you can monitor with your deployment, as well as how many users you can monitor and use to perform user control.

## Host limits

The system adds a host to the network map when it detects activity associated with an IP address in your monitored network (as defined in your network discovery policy). The number of hosts a Secure Firewall Management Center can monitor, and therefore store in the network map, depends on its model.

***Table 1: Host Limits by Secure Firewall Management Center Model***

| Firewall Management Center Model | Hosts |
|---|---|
| MC1000 | 50,000 |
| MC1600 | 50,000 |
| MC2500 | 150,000 |
| MC2600 | 150,000 |

| Firewall Management Center Model | Hosts |
|---|---|
| MC4500 | 600,000 |
| MC4600 | 600,000 |
| virtual | 50,000 |

You cannot view contextual data for hosts not in the network map. However, you can perform access control. For example, you can perform application control on traffic to and from a host not in the network map, even though you cannot use a compliance allow list to monitor the host's network compliance.



**Note** The system counts MAC-only hosts separately from hosts identified by both IP addresses and MAC addresses. All IP addresses associated with a host are counted together as one host.

### Reaching the host limit and deleting hosts

The network discovery policy controls what happens when you detect a new host after reaching the host limit. You can drop the new host, or replace the host that has been inactive for the longest time. You can also set the period after which the system removes a host from the network map due to inactivity. Although you can manually delete a host, an entire subnet, or all of your hosts from the network map, if the system detects activity associated with a deleted host, it re-adds the host.

### Related Topics

Network discovery data storage settings

# User limits for microsoft active directory

User limits impact monitoring and login capacity in Secure Firewall Management Center and Secure Firewall Threat Defense models for Microsoft Active Directory realms. These limits include maximum downloaded users and concurrent session limits. User prioritization, session management, and troubleshooting information help manage user database constraints.

### About user limits

Your Firewall Management Center model determines how many individual users you can monitor. The user is added to the Firewall Management Center user database when:

- The user is downloaded from a realm.
- A captive portal or RA-VPN user logs in.
- A user is detected from any identity source (for example, TS Agent).

Only authoritative users are available for user control with access control policies.

Note the following:

- The maximum number of *downloaded* users depends on your Firewall Management Center model.

- The maximum number of *concurrent* user sessions (that is, logins) depends on your managed device model. A single user can have multiple sessions from different unique IP addresses.

**Note** The system downloads all user sessions to all Firewall Threat Defense devices. If you have devices with different user concurrent user session limits, the Firewall Threat Defense with the smallest limit reports health warnings when its memory reaches the configured limit. (For example, if your Firewall Management Center manages a Firepower 2110 and a 4125, the 2110 reports health warnings when the number of concurrent user sessions approaches its maximum of 64,000.)

### User limits for microsoft active directory

***Table 2: Maximum Concurrent User Login Limits by Firewall Threat Defense***

| Firewall Threat Defense Model | Maximum Concurrent User Logins per Realm |
|---|---|
| Firewall Threat Defense Virtual 5, 10, 20, 30, 50 (any supported hypervisor) | 64,000 |
| Firepower 1010, 1120, 1140, 1150<br>Firepower 2110, 2120, 2130<br>Secure Firewall 3105, 3110, 3120 | 64,000 |
| Firepower 2140<br>Secure Firewall 3130, 3140<br>Firepower 4112, 4115, 4125 | 150,000 |
| Firepower 4145<br>Firepower 9300 | 300,000 |

User limits are applied per Microsoft Active Directory realm. That is, if you attempt to download more than the maximum users in a *single* realm, the download stops after that many users and a health alert is displayed. If, however, you attempt to download more than the maximum number of users spread across *different* realms, the download succeeds (unless any one realm has more than 150,000 users, in which case the download fails for that realm).

***Table 3: Maximum Downloaded Users by Firewall Management Center Model***

| Firewall Management Center Model | Maximum Downloaded Users |
|---|---|
| FMC 1000 | 50,000 |
| FMC 1600 | 50,000 |
| FMC 2500 | 150,000 |
| FMC 2600 | 150,000 |

| Firewall Management Center Model | Maximum Downloaded Users |
|---|---|
| FMC 4500 | 600,000 |
| FMC 4600 | 600,000 |
| Firewall Management Center Virtual (any supported hypervisor) | 50,000 |
| Firewall Management Center Virtual 300 (any supported hypervisor) | 150,000 |

When the system detects a new, previously-undetected user after the limit has been reached, it prioritizes user data based on their identity source:

- If the new user is from a non-authoritative source, the system does not add the non-authoritative user to the database. To allow new users to be added, you must delete users manually or purge the database.
- If the new user is from an authoritative identity source, the system deletes the non-authoritative user who has remained inactive for the longest period and adds the new authoritative user to the database.

  If there are only authoritative users, the system deletes the authoritative user who has remained inactive for the longest period of time and adds the new user to the database.

Troubleshooting information can be found in Troubleshoot user control.

**Tip** Note that if you are using traffic-based detection, you can restrict user logging by protocol to help minimize username clutter and preserve space in the database. For example, you could prevent the system from adding users discovered in AIM, POP3, and IMAP traffic because you know it is traffic from specific contractors or visitors you do not want to monitor.

# Recommendation: identity realm limit

We limit you to a maximum of 25 realms regardless of Firewall Threat Defense model; the same limit applies to the Cloud-Delivered Firewall Management Center.

The number of *users* you can download to a system is limited according to the information provided in:

User limits for microsoft active directory, on page 12