

Logging into the Management Center

The following topics describe how to log into the system:

- User accounts, on page 1
- System user interfaces, on page 3
- Log into the Secure Firewall Management Center web interface, on page 5
- Log into the Firewall Management Center web interface using SSO, on page 6
- Log into the Secure Firewall Management Center with CAC credentials, on page 8
- Log into the Firewall Management Center Command Line Interface, on page 9
- View your last login, on page 9
- Logging Out of the Firewall Management Center Web Interface, on page 10
- History for logging into the management center, on page 10

User accounts

You must provide a username and password to obtain local access to the web interface or CLI on Firewall Management Center or a managed device. On managed devices, CLI users with Config level access can use the **expert** command to access the Linux shell. On the Firewall Management Center, all CLI users can use the **expert** command. The Firewall Threat Defense and Firewall Management Center can be configured to use external authentication, storing user credentials on an external LDAP or RADIUS server; you can withhold or provide CLI access rights to external users. The Firewall Management Center can be configured to support Single Sign-On (SSO) using any SSO provider conforming to the Security Assertion Markup Language (SAML) 2.0 open standard for authentication and authorization.

The Firewall Management Center CLI provides a single **admin** user who has access to all commands. The features Firewall Management Center web interface users can access are controlled by the privileges an administrator grants to the user account. On managed devices, the features that users can access for both the CLI and the web interface are controlled by the privileges an administrator grants to the user account.

Different appliances support different types of user accounts, each with different capabilities.

Secure Firewall Management Centers

Secure Firewall Management Centers support these user account types:

- A pre-defined **admin** account for web interface access, which has the administrator role and can be managed through the web interface.

- Custom user accounts, which provide web interface access and which **admin** users and users with administrator privileges can create and manage.
- A pre-defined **admin** account for CLI access. Users logging in with this account can use the **expert** command to gain access to the Linux shell.

  During initial configuration, the passwords for the CLI **admin** account and the web interface **admin** account are synchronized but, optionally, thereafter you can configure separate passwords for the two **admin** accounts.

Note The system audits user activity based on user accounts; make sure that users log into the system with the correct account.

Caution All Firewall Management Center CLI users and, on managed devices, users with Config level CLI access can obtain root privileges in the Linux shell, which can present a security risk. For system security reasons, we strongly recommend:

- If you establish external authentication, make sure that you restrict the list of users with CLI access appropriately.
- When granting CLI access privileges on managed devices, restrict the list of internal users with Config level CLI access.
- Do not establish Linux shell users; use only the pre-defined **admin** user and users created by the **admin** user within the CLI.

Caution We strongly recommend that you do not use the Linux shell unless directed by Cisco TAC or explicit instructions in the Secure Firewall user documentation.

Caution For system security reasons, Cisco strongly recommends that you not establish additional Linux shell users on any appliance.

Secure Firewall Threat Defense and Secure Firewall Threat Defense Virtual Devices

Secure Firewall Threat Defense and Secure Firewall Threat Defense Virtual devices support these user account types:

- A pre-defined **admin** account which can be used for all forms of access to the device.
- Custom user accounts, which **admin** users and users with Config access can create and manage.

The Secure Firewall Threat Defense supports external authentication for SSH users.

System user interfaces

Depending on appliance type, you can interact with appliances using a web-based GUI, auxiliary CLI, or the Linux shell. In a Secure Firewall Management Center deployment, you perform most configuration tasks from the Firewall Management Center GUI. Only a few tasks require that you access the appliance directly using the CLI or Linux shell. We strongly discourage using the Linux shell unless directed by Cisco TAC or explicit instructions in the user documentation.

For information on browser requirements, see the Secure Firewall Release Notes.



Note On all appliances, after a user makes three consecutive failed attempts to log into the CLI via SSH, the system terminates the SSH connection.

Appliance	Web-Based GUI	Auxiliary CLI	Linux Shell
Secure Firewall Management Center	• Supported for predefined **admin** user and custom user accounts. • Can be used for administrative, management, and analysis tasks.	• Supported for predefined **admin** user and custom external user accounts. • Accessible using an SSH, serial, or keyboard and monitor connection. • Should be used only for administration and troubleshooting directed by Cisco TAC.	• Supported for predefined **admin** user. • Must be accessed via **expert** command from the Secure Firewall Management Center CLI. • Accessible using an SSH, serial, or keyboard and monitor connection. • Should be used only for administration and troubleshooting directed by Cisco TAC or by explicit instructions in the Firewall Management Center documentation.
Secure Firewall Threat Defense Secure Firewall Threat Defense Virtual	—	• Supported for predefined **admin** user and custom user accounts. • Accessible in physical devices using an SSH, serial, or keyboard and monitor connection. Accessible in virtual devices via SSH or VM console. • Can be used for setup and troubleshooting directed by Cisco TAC.	• Supported for predefined **admin** user and custom user accounts. • Accessible by CLI users with Config access using the **expert** command. • Should be used only for administration and troubleshooting directed by Cisco TAC or by explicit instructions in the Firewall Management Center documentation..

Related Topics

Add or edit an internal user

Web interface considerations

Web interface considerations are a set of guidelines that

- address authentication requirements for Common Access Cards (CACs) when external users access the appliance through LDAP
- explain how menu options and privileges affect user access and system logging, and
- describe browser behavior when processing time-intensive operations.

Web interface operational details

The web interface has specific operational characteristics:

- If your organization uses Common Access Cards (CACs) for authentication, external users authenticated with LDAP can use CAC credentials to obtain access to the web interface of an appliance.
- Menus and menu options at the top of the default home page are based on your user account privileges. Links on the home page offer choices from the full range of user privileges. If you select a link requiring privileges you do not have, the system shows a warning and records the event.
- Some processes that take a significant amount of time may cause your web browser to display a message that a script has become unresponsive. If this occurs, make sure you allow the script to continue until it finishes.

Related Topics

Specify your home page

Session timeout

A session timeout is a security mechanism that

- automatically logs users out of a session after 1 hour of inactivity by default
- can be configured to exempt certain users from automatic logout, and
- allows Administrator role users to modify the timeout interval for an appliance.

Session timeout behavior

By default, the system automatically logs you out of a session after 1 hour of inactivity unless you are exempt from session timeout by configuration.

Note For SSO users, when the Firewall Management Center session times out, the display briefly redirects to the IdP interface, and then the Firewall Management Center login page. Unless the SSO session has been terminated from elsewhere, anyone can access the Firewall Management Center without providing login credentials simply by clicking on the **Single Sign-On** link on the login page. To ensure Firewall Management Center security and prevent others from accessing the Firewall Management Center using your SSO account, we recommend you not leave a Firewall Management Center login session unattended, and log out of the SSO federation at the IdP when you log out of the Firewall Management Center.

Users with the Administrator role can change the session timeout interval for an appliance using **System** (⚙) > **Configuration** > **Session Timeout**.

Related Topics

Configure session timeouts
SAML Single Sign-On

Log into the Secure Firewall Management Center web interface

This task allows you to access the Secure Firewall Management Center web interface to manage and configure your firewall system.

Note This task applies to internal users and external users authenticated by LDAP or RADIUS servers. For SSO login, see Log into the Firewall Management Center web interface using SSO, on page 6.

Users are restricted to a single active session. If you try to log in with a user account that already has an active session, the system prompts you to terminate the other session or log in as a different user.

In a NAT environment where multiple Firewall Management Centers share the same IP address:

- Each Firewall Management Center can support only one login session at a time.
- To access different Firewall Management Centers, use a different browser for each login (for example Firefox and Chrome), or set the browser to incognito or private mode.

Before you begin

- If you do not have access to the web interface, contact your system administrator to modify your account privileges, or log in as a user with Administrator access and modify the privileges for the account.
- Create user accounts as described in Add or edit an internal user.

Follow these steps to log into the Secure Firewall Management Center web interface:

Procedure

Step 1 Direct your browser to **https://***ipaddress_or_hostname*/, where *ipaddress* or *hostname* corresponds to your Firewall Management Center.

Step 2 In the **Username** and **Password** fields, enter your user name and password. Pay attention to the following guidelines:

- User names are *not* case-sensitive.
- In a multidomain deployment, prepend the user name with the subdomain where your user account was created. You do not need to specify the Global domain. For example, if your user account was created in SubdomainA, enter your username in the following format:

  `SubdomainA\username`

  If your user was added to SubdomainB, whose parent domain is SubdomainA, enter your username in the following format:

  `SubdomainA\SubdomainB\username`
- If your organization uses SecurID® tokens when logging in, append the token to your SecurID PIN and use that as your password to log in. For example, if your PIN is `1111` and the SecurID token is `222222`, enter `1111222222`. You must have already generated your SecurID PIN before you can log into the system.

Step 3 Click **Login**.

You are successfully logged into the Secure Firewall Management Center web interface and can begin managing your firewall configuration.

Related Topics

Session timeout, on page 4

Log into the Firewall Management Center web interface using SSO

This task enables secure access to the Firewall Management Center web interface using existing SSO credentials, eliminating the need for separate authentication.

The Firewall Management Center can be configured to participate in any Single-Sign On (SSO) federation implemented with an SSO provider conforming to the Security Assertion Markup Language (SAML) 2.0 open standard. SSO user accounts must be established at the identity provider (IdP) and must use email addresses for their account names. If your user name is not an email address, or SSO login fails, contact your system administrator.

Note The Firewall Management Center does not support logging in with CAC credentials for SSO accounts.

Users are restricted to a single active session. If you try to log in with a user account that already has an active session, the system prompts you to terminate the other session or to sign in as a different user.

In a NAT environment where multiple Firewall Management Centers share the same IP address:

- Each Firewall Management Center can support only one login session at a time.
- To access different Firewall Management Centers, use a different browser for each login (for example Firefox and Chrome), or set the browser to incognito or private mode.

Before you begin

- Configure the Firewall Management Center for SSO access. See SAML Single Sign-On.
- If you do not have access to the web interface, contact your system administrator to configure your account at the SSO IdP.

Follow these steps to log into the Firewall Management Center web interface using SSO:

Procedure

Step 1 Direct your browser to **https://***ipaddress_or_hostname*/, where *ipaddress* or *hostname* corresponds to your Firewall Management Center.



Note SSO users must consistently access the Firewall Management Center using the login URL specifically configured for SSO access; ask your administrator for this information.

Step 2 Click the **Single Sign-On** link.

Step 3 The system may display one of two responses:

- If you are already logged into the SSO federation, the Firewall Management Center default home page appears.
- If you are not already logged into the SSO federation, the Firewall Management Center redirects your browser to the login page for your IdP. After you complete the login process at the IdP, the Firewall Management Center default home page appears.

You are successfully logged into the Firewall Management Center web interface and can access the default home page to begin managing your firewall configurations.

Related Topics

Session timeout, on page 4
SAML Single Sign-On

Log into the Secure Firewall Management Center with CAC credentials

This task enables secure access to the Secure Firewall Management Center web interface using CAC authentication credentials.

Users are restricted to a single active session. If you try to log in with a user account that already has an active session, the system prompts you to end the other session or log in as a different user.

In a NAT environment where multiple Firewall Management Centers share the same IP address:

- Each Firewall Management Center can support only one login session at a time.
- To access different Firewall Management Centers, use a different browser for each login, such as Firefox or Chrome, or set the browser to incognito or private mode.



Caution Do **not** remove a CAC during an active browsing session. If you remove or replace a CAC during a session, your web browser terminates the session and the system logs you out of the web interface.

Before you begin

- If you do not have access to the web interface, ask your system administrator to change your account privileges. Alternatively, log in as a user with administrator access to modify account privileges.
- Create user accounts. For more information, refer to Add or edit an internal user.
- Configure CAC authentication and authorization. For more information, refer to Configure common access card authentication with LDAP.

Follow these steps to log into the Secure Firewall Management Center with CAC credentials:

Procedure

Step 1 Insert a CAC as instructed by your organization.

Step 2 Direct your browser to **https://***ipaddress_or_hostname/*, where *ipaddress* or *hostname* corresponds to your Firewall Management Center.

Step 3 If prompted, enter the PIN associated with the CAC you inserted in step 1.

Step 4 If prompted, choose the appropriate certificate from the drop-down list.

Step 5 Click **Continue**.

You are successfully logged into the Secure Firewall Management Center web interface using CAC authentication.

Related Topics

Configure common access card authentication with LDAP

Session timeout, on page 4
Guidelines for SSO configuration on Firewall Management Center

Log into the Firewall Management Center Command Line Interface

This task enables CLI access to the Firewall Management Center for administrative and external users.

The **admin** CLI user and certain custom external users can log into the Firewall Management Center CLI.

Caution We strongly recommend that you do not use the Linux shell unless directed by Cisco TAC or explicit instructions in the Firewall Management Center documentation.

Note For all appliances, after a user makes three consecutive failed attempts to log into the CLI via SSH, the system terminates the SSH connection.

Before you begin

Complete the initial configuration process as the **admin** user. See First-time login.

Procedure

Step 1 Use the **admin** user name and password to connect to the Firewall Management Center via SSH or the console port.

If your organization uses SecurID® tokens when logging in, append the token to your SecurID PIN and use that as your password to log in. For example, if your PIN is **1111** and the SecurID token is **222222**, enter **1111222222**. You must have already generated your SecurID PIN before you can log in.

Step 2 Use any of the available CLI commands.

You are now logged into the Firewall Management Center CLI and can execute administrative commands.

View your last login

View your last login information to verify that no unauthorized users have accessed your account using your credentials.

If you suspect that an unauthorized user has used your credentials to sign in to the Secure Firewall Management Center, you can see the date, time, and IP address from which your credentials were last used to log in.

Before you begin

This feature is not available if you are using the Classic theme. You can select a UI theme in User Preferences.

Procedure

Step 1 Sign in to the Secure Firewall Management Center.

Step 2 At the top right corner of your browser window, look for the User ID that you used to sign in.

Step 3 Click your user name.

Step 4 Information about your previous login is shown at the bottom of the menu that appears.

You can view the date, time, and IP address of your last login to verify account security.

Logging Out of the Firewall Management Center Web Interface

Logging out ends your web session and ensures that no one can use the interface with your credentials.

When you are no longer actively using the Firewall Management Center web interface, Cisco recommends that you log out, even if you are only stepping away from your web browser for a short period of time.

Note If you are logging out of an SSO session at the Firewall Management Center, when you log out the system redirects your browser to the SSO IdP for your organization. To ensure Firewall Management Center security and prevent others from accessing the Firewall Management Center using your SSO account, we recommend you log out of the SSO federation at the IdP.

Procedure

Step 1 From the drop-down list under your user name, choose **Logout**.

Step 2 If you are logging out of an SSO session at the Firewall Management Center, the system redirects you to the SSO IdP for your organization. Log out at the IdP to ensure Firewall Management Center security.

Your web session is terminated and you are logged out of the Firewall Management Center web interface.

Related Topics

Session timeout, on page 4

History for logging into the management center

This reference provides a comprehensive history of login-related features and enhancements for the Management Center across different software versions. The information includes feature descriptions, supported versions, platform compatibility, and implementation details for Single Sign-On capabilities, CLI access controls, login security measures, and user interface modifications.

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Added support for Single Sign-On (SSO) using any SAML 2.0-compliant SSO provider.	6.7	Any	Added the ability for users configured at any third-party SAML 2.0-compliant identity provider (IdP) to log into the Firewall Management Center using a new **Single Sign-On** link on the login page. New/Modified screen: Login screen
View information about the last time you signed in to the Secure Firewall Management Center	6.5	Any	View the date, time, and IP address from which you last logged in. New/Modified menus: The menu at the top right of the window that shows the username that you used to log in. Supported platforms: Firewall Management Center
Automatic CLI access for the Firewall Management Center	6.5	Any	When you use SSH to log into the Firewall Management Center, you automatically access the CLI. You can then use the CLI `expert` command to access the Linux shell, however, doing so is strongly discouraged.". **Note** This feature deprecates the Version 6.3 ability to enable and disable CLI access for the Firewall Management Center. As a consequence of deprecating this option, the virtual Firewall Management Center no longer displays the **System** > **Configuration** > **Console Configuration** page, which still appears on physical Firewall Management Centers.
Limit number of SSH login failures	6.3	Any	When a user accesses any device via SSH and fails three successive login attempts, the device terminates the SSH session.
Ability to enable and disable CLI access for the Firewall Management Center	6.3	Any	New/Modified screens: New check box available to administrators in Firewall Management Center web interface: **Enable CLI Access** on the **System** > **Configuration** > **Console Configuration** page. • Checked: Logging into the Firewall Management Center using SSH accesses the CLI. • Unchecked: Logging into Firewall Management Center using SSH accesses the Linux shell. This is the default state for fresh Version 6.3 installations as well as upgrades to Version 6.3 from a previous release. Supported platforms: Firewall Management Center