Logging into the Management Center

The following topics describe how to log into the system:

User Accounts

You must provide a username and password to obtain local access to the web interface or CLI on 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 management center, all CLI users can use the `expert` command. The threat defense and 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 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 management center CLI provides a single **admin** user who has access to all commands. The features 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.

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

Caution All 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.

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

Secure Firewall Management Centers

Secure Firewall Management Centers support the following 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.

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 the following 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 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 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 management center documentation..

Related Topics

Add or Edit an Internal User

Web Interface Considerations

- 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.
- The menus and menu options listed at the top of the default home page are based on the privileges for your user account. However, the links on the default home page include options that span the range of user account privileges. If you click a link that requires different privileges from those granted to your account, the system displays a warning message and logs the activity.
- 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

Specifying Your Home Page

Session Timeout

By default, the system automatically logs you out of a session after 1 hour of inactivity, unless you are otherwise configured to be exempt from session timeout.

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

Users with the Administrator role can change the session timeout interval for an appliance via the following settings:

System > **Configuration** > **Shell Timeout**

Related Topics

Configure Session Timeouts
Configure SAML Single Sign-On

Logging Into the Secure Firewall Management Center Web Interface

Note This task applies to internal users and external users authenticated by LDAP or RADIUS servers. For SSO login, see Logging Into the 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 management centers share the same IP address:

- Each management center can support only one login session at a time.
- To access different 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.

Procedure

Step 1 Direct your browser to **https://***ipaddress_or_hostname*/, where *ipaddress* or *hostname* corresponds to your 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 domain where your user account was created. You are not required to prepend any ancestor domains. For example, if your user account was created in SubdomainB, which has an ancestor DomainA, enter your user name in the following format:

  `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**.

Related Topics

Session Timeout, on page 4

Logging Into the Management Center Web Interface Using SSO

The 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 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 log in as a different user.

In a NAT environment where multiple management centers share the same IP address:

- Each management center can support only one login session at a time.
- To access different 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 management center for SSO access. See Configure 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.

Procedure

Step 1 Direct your browser to **https://***ipaddress_or_hostname/*, where *ipaddress* or *hostname* corresponds to your management center.

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

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

Step 3 The system responds in one of two ways:

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

Related Topics

Session Timeout, on page 4
Configure SAML Single Sign-On

Logging Into the Secure Firewall Management Center with CAC 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 terminate the other session or log in as a different user.

In a NAT environment where multiple management centers share the same IP address:

- Each management center can support only one login session at a time.
- To access different management centers, use a different browser for each login (for example Firefox and 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, 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 the Add or Edit an Internal User.
- Configure CAC authentication and authorization as described in Configure Common Access Card Authentication with LDAP.

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 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**.

Related Topics

Configure Common Access Card Authentication with LDAP
Session Timeout, on page 4
SSO Guidelines for the Management Center

Logging Into the Management Center Command Line Interface

The **admin** CLI user and certain custom external users can log into the 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 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 Logging In for the First Time.

Procedure

Step 1 Use the **admin** user name and password to connect to the 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.

View Your Last Login

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.

Logging Out of the Management Center Web Interface

When you are no longer actively using the 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. Logging out ends your web session and ensures that no one can use the interface with your credentials.

Note If you are logging out of an SSO session at the management center, when you log out the system redirects your browser to the SSO IdP for your organization. To ensure management center security and prevent others from accessing the 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 management center, the system redirects you to the SSO IdP for your organization. Log out at the IdP to ensure management center security.

Related Topics

Session Timeout, on page 4

History for Logging into the Management Center

Feature	Minimum Management Center	Minimum 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 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: management center

Feature	Minimum Management Center	Minimum Threat Defense	Details
Automatic CLI access for the management center	6.5	Any	When you use SSH to log into the management center, you automatically access the CLI. Although strongly discouraged, you can then use the CLI `expert` command to access the Linux shell. **Note** This feature deprecates the Version 6.3 ability to enable and disable CLI access for the management center. As a consequence of deprecating this option, the virtual management center no longer displays the **System** > **Configuration** > **Console Configuration** page, which still appears on physical 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 management center	6.3	Any	New/Modified screens: New check box available to administrators in management center web interface: **Enable CLI Access** on the **System** (⚙) > **Configuration** > **Console Configuration** page. • Checked: Logging into the management center using SSH accesses the CLI. • Unchecked: Logging into 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: management center