Logging into the Firepower System

The following topics describe how to log into the Firepower System:

Firepower System User Accounts

You must provide a username and password to obtain local access to the web interface, shell, or CLI on an FMC or managed device. On managed devices, CLI users with Config level access can use the `expert` command to access the Linux shell. On the FMC, all CLI users can use the `expert` command. The FTD and FMC can be configured to use external authentication, storing user credentials on an external LDAP or RADIUS server; you can withhold or provide CLI/shell access rights to external users.

The FMC CLI provides a single **admin** user who has access to all commands. The features FMC 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 FMC 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/shell 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 Firepower user documentation.

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

Firepower Management Centers

Firepower 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 shell access, which can obtain root privileges.

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

7000 & 8000 Series Devices

7000 & 8000 Series 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 the administrator role can create and manage.

The 7000 & 8000 Series supports external authentication for users.

NGIPSv Devices

NGIPSv 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 NGIPSv does not support external authentication for users.

Firepower Threat Defense and Firepower Threat Defense Virtual Devices

Firepower Threat Defense and Firepower 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 Firepower Threat Defense does not support external authentication for SSH or HTTP users.

ASA FirePOWER Devices

The ASA FirePOWER module supports the following user account types:

- A pre-defined **admin** account.
- Custom user accounts, which **admin** users and users with Config access can create and manage.

The ASA FirePOWER module does not support external authentication for users. Accessing ASA devices via the ASA CLI and ASDM is described in the *Cisco ASA Series General Operations CLI Configuration Guide* and the *Cisco ASA Series General Operations ASDM Configuration Guide*.

Firepower System User Interfaces

Depending on appliance type, you can interact with Firepower appliances using a web-based GUI, auxiliary CLI, or the Linux shell. In a Firepower Management Center deployment, you perform most configuration tasks from the FMC 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 Firepower user documentation.

For information on browser requirements, see the Firepower Release Notes.

Appliance	Web-Based GUI	Auxiliary CLI	Linux Shell
Firepower 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 or by explicit instructions in the FMC documentation.

Appliance	Web-Based GUI	Auxiliary CLI	Linux Shell
7000 & 8000 Series devices	• Supported for predefined **admin** user and custom user accounts. • Can be used for initial setup, basic analysis, and configuration tasks only.	• Supported for predefined **admin** user and custom user accounts. • Accessible using an SSH, serial, or keyboard and monitor connection. • 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 FMC documentation.
Firepower Threat Defense Firepower 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 FMC documentation..
NGIPSv	—	• Supported for predefined **admin** user and custom user accounts • Accessible using an SSH connection 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 explicit instructions in the FMC documentation..

Appliance	Web-Based GUI	Auxiliary CLI	Linux Shell
ASA FirePOWER module	—	• Supported for predefined **admin** user and custom user accounts. • Accessible using an SSH connection. Also accessible using a keyboard and monitor connection for ASA 5585-X devices (hardware module), or the console port for other ASA 5500-X series devices (software modules). • Can be used for configuration and management tasks.	• 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 FMC documentation..

Related Topics

Managing User Accounts

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 first time you visit the appliance home page during a web session, you can view information about your last login session for that appliance. You can see the following information about your last login:
  - the day of the week, month, date, and year of the login
  - the appliance-local time of the login in 24-hour notation
  - the host and domain name last used to access the 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 Firepower System automatically logs you out of a session after 1 hour of inactivity, unless you are otherwise configured to be exempt from session timeout.

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

Appliance	Setting
Firepower Management Center	**System** > **Configuration** > **Shell Timeout**
7000 & 8000 Series devices	**Devices** > **Platform Settings** > **Shell Timeout**

Related Topics

Configure Session Timeouts

Logging Into the Firepower Management Center Web Interface

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 FMCs share the same IP address:

- Each FMC can support only one login session at a time.
- To access different FMCs, 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 Creating a User Account.

Procedure

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

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 Firepower System.

Step 3 Click **Login**.

Related Topics

Session Timeout, on page 6

Logging Into the Web Interface of a 7000 or 8000 Series Device

Users are restricted to a single active session on a 7000 & 8000 Series device. 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.

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.
- Complete the initial setup process and create user accounts as described in the Firepower getting started guide appropriate to the device, and Creating a User Account.

Procedure

Step 1 Direct your browser to `https://hostname/`, where *`hostname`* corresponds to the host name of the managed device you want to access.

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.
- 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 Firepower System.

Step 3 Click **Login**.

Related Topics

Session Timeout, on page 6

Logging Into the Firepower 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 FMCs share the same IP address:

- Each FMC can support only one login session at a time.
- To access different FMCs, 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 Creating a User Account.
- Configure CAC authentication and authorization as described in Configuring CAC Authentication.

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 FMC.

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

CAC Authentication
Session Timeout, on page 6

Logging Into a 7000 or 8000 Series Device with CAC Credentials

Users are restricted to a single active session on a 7000 & 8000 Series device.

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 Creating a User Account.
- Configure CAC authentication and authorization as described in Configuring CAC Authentication.

Procedure

Step 1 Insert a CAC as instructed by your organization.

Step 2 Direct your browser to `https://hostname/`, where *hostname* corresponds to the host name of the appliance you want to access.

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

CAC Authentication
Session Timeout, on page 6

Logging Into the CLI on 7000/8000 Series, ASA FirePOWER, and NGIPSv Devices

With a minimum of basic CLI configuration access, you can log directly into Classic managed devices.

Before you begin

- Complete the initial setup process using the default **admin** user for the initial login.
- Create additional user accounts that can log into the CLI using the **configure user add** command.
- For the 7000 & 8000 Series devices, create user accounts at the web interface as described in Creating a User Account.

Procedure

Step 1 SSH to the device's management interface (hostname or IP address) or use the console.

With the exception of ASA 5585-X devices, which have dedicated ASA FirePOWER console port, ASA FirePOWER devices accessed via the console default to the operating system CLI. This requires an extra step to access the Firepower CLI: **`session sfr`**.

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 At the CLI prompt, use any of the commands allowed by your level of command line access.

Logging Into the Command Line Interface on Firepower Threat Defense Devices

You can log directly into the command line interface on Firepower Threat Defense managed devices.

Before you begin

Complete the initial setup process using the default **admin** user for the initial login. Create additional user accounts that can log into the CLI using the **configure user add** command.

Procedure

Step 1 Connect to the Firepower Threat Defense CLI, either from the console port or using SSH.

You can SSH to the management interface of the Firepower Threat Defense device. You can also connect to the address on a data interface if you open the interface for SSH connections. SSH access to data interfaces is disabled by default. See Configure Secure Shell to allow SSH connections to specific data interfaces.

You can directly connect to the Console port on the device. Use the console cable included with the device to connect your PC to the console using a terminal emulator set for 9600 baud, 8 data bits, no parity, 1 stop bit, no flow control. See the hardware guide for your device for more information about the console cable.

The initial CLI you access on the Console port differs by device type.

- ASA Series devices—The CLI on the Console port is the regular Firepower Threat Defense CLI.
- Firepower Series devices—The CLI on the Console port is FXOS. You can get to the Firepower Threat Defense CLI using the **connect ftd** command. Use the FXOS CLI for chassis-level configuration and troubleshooting only. Use the Firepower Threat Defense CLI for basic configuration, monitoring, and normal system troubleshooting. See the FXOS documentation for information on FXOS commands.

Step 2 Log in with the **admin** username and password.

Step 3 At the CLI prompt (>), use any of the commands allowed by your level of command line access.

Step 4 (Optional) Access the diagnostic CLI:

system support diagnostic-cli

Use this CLI for advanced troubleshooting. This CLI includes additional **show** and other commands, including the **session wlan console** command needed to enter the CLI for the wireless access point on an ASA 5506W-X.

This CLI has two sub-modes: user EXEC and privileged EXEC mode. More commands are available in privileged EXEC mode. To enter privileged EXEC mode, enter the **enable** command; press enter without entering a password when prompted.

Example:

```
> system support diagnostic-cli
firepower> enable
Password:
firepower#
```

To return to the regular CLI, type **Ctrl-a**, **d**.

Logging Out of a Firepower System Web Interface

When you are no longer actively using a Firepower System 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 FMC, when you log out the system redirects your browser to the SSO IdP for your organization. To ensure FMC security and prevent others from accessing the FMC 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 FMC, the system redirects you to the SSO IdP for your organization. Log out at the IdP to ensure FMC security.

Related Topics

Session Timeout, on page 6