Using the Command Line Interface (CLI)

The following topics explain how to use the command line interface (CLI) for Firepower Threat Defense (FTD) devices and how to interpret the command reference topics. Use the CLI for basic system setup and troubleshooting.

When you deploy a configuration change using the Firepower Management Center or Firepower Device Manager, do not use the FTD CLI for long-running commands (such as ping with a huge repeat count or size); these commands could cause a deployment failure.

- Logging Into the Command Line Interface (CLI), on page 2
- Command Modes, on page 3
- Syntax Formatting, on page 5
- Entering Commands, on page 6
- Filtering Show Command Output, on page 7
- Command Help, on page 9
Logging Into the Command Line Interface (CLI)

To log into the CLI, use an SSH client to make a connection to the management IP address. Log in using the admin username (default password is Admin123) or another CLI user account.

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. To enable SSH access, use the device manager (Firepower Management Center or Firepower Device Manager) to allow SSH connections to specific data interfaces. You cannot SSH to the Diagnostic interface.

You can create user accounts that can log into the CLI using the `configure user add` command. However, these users can log into the CLI only. They cannot log into the Firepower Device Manager web interface. The CLI supports local authentication only. You cannot access the CLI using external authentication.

**Console Port Access**

In addition to SSH, 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 FTD CLI.

- Firepower Series devices—The CLI on the Console port is FXOS. You can get to the FTD CLI using the `connect ftd` command. Use the FXOS CLI for chassis-level configuration and troubleshooting only. For the Firepower 2100, you cannot perform any configuration at the FXOS CLI. Use the FTD CLI for basic configuration, monitoring, and normal system troubleshooting. See the FXOS documentation for information on FXOS commands for the Firepower 4100 and 9300. See the *Cisco FXOS Troubleshooting Guide for the Firepower 2100 Series* for information on FXOS commands for the Firepower 2100.
Command Modes

The CLI on a Firepower Threat Defense device has different modes, which are really separate CLIs rather than sub-modes to a single CLI. You can tell which mode you are in by looking at the command prompt.

Regular Firepower Threat Defense CLI

Use this CLI for Firepower Threat Defense management configuration and troubleshooting.

> 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; more commands are available in Privileged EXEC Mode.

To enter this mode, use the `system support diagnostic-cli` command in the Firepower Threat Defense CLI.

- User EXEC Mode. The prompt reflects the system hostname as defined in the running configuration.

  firepower>

- Privileged EXEC Mode. Enter the `enable` command to enter this mode (press enter without entering a password when prompted for a password).

  firepower#

Expert Mode

Use Expert Mode only if a documented procedure tells you it is required, or if the Cisco Technical Assistance Center asks you to use it. To enter this mode, use the `expert` command in the Firepower Threat Defense CLI.

The prompt is `username@hostname` if you log in using the admin user. If you use a different user, only the hostname is shown. The hostname is the name configured for the management interface. For example,

  admin@firepower:~$

Firepower eXtensible Operating System (FXOS) CLI

On Firepower 2100, 4100, and 9300 series devices, FXOS is the operating system that controls the overall chassis. Depending on the model, you use FXOS for configuration and troubleshooting. From FXOS, you can enter the Firepower Threat Defense CLI using the `connect ftd` command.

For Firepower 2100 series devices, you can go from the Firepower Threat Defense CLI to the FXOS CLI using the `connect fxos` command.

The FXOS command prompt looks like the following, but the prompt changes based on mode. See the Cisco FXOS CLI Configuration Guide for your FXOS version and hardware model for details about FXOS CLI usage.
Command Modes

Firepower-module2>
Firepower-module2#
# Syntax Formatting

Command syntax descriptions use the following conventions:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>command</td>
<td>Command text indicates commands and keywords that you enter literally as shown.</td>
</tr>
<tr>
<td>variable</td>
<td>Variable text indicates arguments for which you supply values.</td>
</tr>
<tr>
<td>[x]</td>
<td>Square brackets enclose an optional element (keyword or argument).</td>
</tr>
<tr>
<td>[ x</td>
<td>y]</td>
</tr>
<tr>
<td>{x</td>
<td>y}</td>
</tr>
<tr>
<td>[x {y</td>
<td>z}]</td>
</tr>
</tbody>
</table>
Entering Commands

When you log into the CLI through the console port or an SSH session, you are presented with the following command prompt:

> 

You type the command at the prompt and press Enter to execute the command. Additional features include:

- **Scrolling through command history**—You can use the up and down arrow keys to scroll through the commands that you have already entered. You can reenter or edit and reenter the commands in the history.

- **Completing commands**—To complete a command or keyword after entering a partial string, press the space or Tab key. The partial string must match a single command or keyword only for it to be completed.

- **Abbreviating commands**—In the regular CLI, you cannot abbreviate commands. You must enter the full command string. However, in the diagnostic CLI, you can abbreviate most commands down to the fewest unique characters for a command; for example, you can enter `show ver` instead of `show version`.

- **Stopping command output**—If a command produces a lot of output, you can get out of it by pressing the `q` key.

- **Stopping long-running commands**—If a command is not returning output fast enough, and you want to try a different command, press Ctrl+C.
Filtering Show Command Output

You can filter the output of `show` commands by piping the output to filtering commands. Piping output works with all `show` commands but is most useful when dealing with commands that produce a lot of text.

To use the filtering capabilities, use the following format. In this case, the vertical bar `|` after the `show` command is the pipe character and is part of the command, not part of the syntax description. The filtering options come after the `|` character.

```
show command | {grep | include | exclude | begin} regular expression
```

Filtering Commands

You can use these filtering commands:

- `grep`—Display only those lines that match the pattern.
- `include`—Display only those lines that match the pattern.
- `exclude`—Exclude all lines that match the pattern, show all other lines.
- `begin`—Find the first line that includes the pattern, and display that line and all subsequent lines.

A regular expression, typically a simple text string. Do not enclose the expression in single or double-quotes, these will be seen as part of the expression. Also, trailing spaces will be included in the expression.

The following example shows how to change the output of the `show access-list` command to show only those rules that apply to the `inside1_2` interface.

```
> show access-list | include inside1_2
access-list NGFW_ONBOX_ACL line 3 advanced trust ip ifc inside1_2 any ifc inside1_3 any
rule-id 268435458
event-log both (hitcnt=0) 0x2c7f5801
access-list NGFW_ONBOX_ACL line 4 advanced trust ip ifc inside1_2 any ifc inside1_4 any
rule-id 268435458
event-log both (hitcnt=0) 0xf170c15b
access-list NGFW_ONBOX_ACL line 5 advanced trust ip ifc inside1_2 any ifc inside1_5 any
rule-id 268435458
event-log both (hitcnt=0) 0xce627c77
access-list NGFW_ONBOX_ACL line 6 advanced trust ip ifc inside1_2 any ifc inside1_6 any
rule-id 268435458
event-log both (hitcnt=0) 0x83200d1e
access-list NGFW_ONBOX_ACL line 7 advanced trust ip ifc inside1_2 any ifc inside1_7 any
rule-id 268435458
event-log both (hitcnt=0) 0x65347856
access-list NGFW_ONBOX_ACL line 8 advanced trust ip ifc inside1_2 any ifc inside1_8 any
rule-id 268435458
event-log both (hitcnt=0) 0x6d622775
access-list NGFW_ONBOX_ACL line 9 advanced trust ip ifc inside1_3 any ifc inside1_2 any
rule-id 268435458
event-log both (hitcnt=0) 0xce627c77
access-list NGFW_ONBOX_ACL line 10 advanced trust ip ifc inside1_4 any ifc inside1_2 any
rule-id 268435458
event-log both (hitcnt=0) 0x65347856
access-list NGFW_ONBOX_ACL line 11 advanced trust ip ifc inside1_8 any ifc inside1_2 any
rule-id 268435458
event-log both (hitcnt=0) 0x6d622775
access-list NGFW_ONBOX_ACL line 12 advanced trust ip ifc inside1_3 any ifc inside1_2 any
rule-id 268435458
event-log both (hitcnt=0) 0x65347856
access-list NGFW_ONBOX_ACL line 13 advanced trust ip ifc inside1_4 any ifc inside1_2 any
rule-id 268435458
event-log both (hitcnt=0) 0x6d622775
access-list NGFW_ONBOX_ACL line 14 advanced trust ip ifc inside1_5 any ifc inside1_2 any
rule-id 268435458
```
event-log both (hitcnt=0) 0xf508bbd8
access-list NGFW_ONBOX_ACL line 27 advanced trust ip ifc inside1_6 any ifc inside1_2 any
rule-id 268435458

event-log both (hitcnt=0) 0xa6be4e58
access-list NGFW_ONBOX_ACL line 33 advanced trust ip ifc inside1_7 any ifc inside1_2 any
rule-id 268435458

event-log both (hitcnt=0) 0x699725ea
access-list NGFW_ONBOX_ACL line 39 advanced trust ip ifc inside1_8 any ifc inside1_2 any
rule-id 268435458

event-log both (hitcnt=0) 0xd2014e58
access-list NGFW_ONBOX_ACL line 47 advanced trust ip ifc inside1_2 any ifc outside any
rule-id 268435457

event-log both (hitcnt=0) 0xea5bdd6e
Command Help

Help information is available from the command line by entering the following commands:

- `?` to see a list of all commands.
- `command_name ?` to see the options for a command. For example, `show ?`.
- `string?` to show the commands or keywords that match the string. For example, `n?` shows all commands that start with the letter n.
- `help command_name` to see the syntax and limited usage information for a command. Enter `help ?` to see which commands have help pages.