Secure Firewall Management Center Command Line Reference

This reference explains the command line interface (CLI) for the Secure Firewall Management Center.

Note For Secure Firewall Threat Defense, see the Cisco Secure Firewall Threat Defense Command Reference.

- About the Secure Firewall Management Center CLI, on page 1
- Secure Firewall Management Center CLI Management Commands, on page 2
- Secure Firewall Management Center CLI Show Commands, on page 3
- Secure Firewall Management Center CLI Configuration Commands, on page 4
- Secure Firewall Management Center CLI System Commands, on page 5
- History for the Secure Firewall Management Center CLI, on page 8

About the Secure Firewall Management Center CLI

When you use SSH to log into the management center, you access the CLI. Although we strongly discourage it, you can then access the Linux shell using the `expert` command .

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

Caution Users with Linux shell access can obtain root privileges, 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 Linux shell access appropriately.
- Do not establish Linux shell users in addition to the pre-defined `admin` user.

You can use the commands described in this appendix to view and troubleshoot your Secure Firewall Management Center, as well as perform limited configuration operations.

Secure Firewall Management Center CLI Modes

The CLI encompasses four modes. The default mode, CLI Management, includes commands for navigating within the CLI itself. The remaining modes contain commands addressing three different areas of Secure Firewall Management Center functionality; the commands within these modes begin with the mode name: `system`, `show`, or `configure`.

When you enter a mode, the CLI prompt changes to reflect the current mode. For example, to display version information about system components, you can enter the full command at the standard CLI prompt:

```
> show version
```

If you have previously entered `show` mode, you can enter the command without the `show` keyword at the show mode CLI prompt:

```
show> version
```

Secure Firewall Management Center CLI Management Commands

The CLI management commands provide the ability to interact with the CLI. These commands do not affect the operation of the device.

exit

Moves the CLI context up to the next highest CLI context level. Issuing this command from the default mode logs the user out of the current CLI session.

Syntax

```
exit
```

Example

```
system> exit
>
```

expert

Invokes the Linux shell.

Syntax

```
expert
```

Example

```
> expert
```

? (question mark)

Displays context-sensitive help for CLI commands and parameters. Use the question mark (?) command as follows:

- To display help for the commands that are available within the current CLI context, enter a question mark (?) at the command prompt.
- To display a list of the available commands that start with a particular character set, enter the abbreviated command immediately followed by a question mark (?).
- To display help for a command's legal arguments, enter a question mark (?) in place of an argument at the command prompt.

Note that the question mark (?) is not echoed back to the console.

Syntax

```
?
abbreviated_command ?
command [arguments] ?
```

Example

```
> ?
```

Secure Firewall Management Center CLI Show Commands

Show commands provide information about the state of the appliance. These commands do not change the operational mode of the appliance and running them has minimal impact on system operation.

version

Displays the product version and build as well as the UUID and other information.

Syntax

```
show version
```

Example

```
> show version
-------------------[ fmc-austin ]-------------------
Model                     : Cisco Secure Firewall Management Center for VMware (66) Version
 7.6.0 (Build 1385)
UUID                       : a904b8b2-ca9a-11ee-a583-5e804c16b2fd
Rules update version       : 2024-05-13-001-vrt
LSP version                : lsp-rel-20240513-1955
VDB version                : 380
----------------------------------------------------
```

Secure Firewall Management Center CLI Configuration Commands

The configuration commands enable the user to configure and manage the system. These commands affect system operation.

password

Allows the current CLI user to change their password.

Caution For system security reasons, we strongly recommend that you do not establish Linux shell users in addition to the pre-defined **admin** on any appliance.

Note The `password` command is not supported in export mode. To reset password of an admin user on a secure firewall system, see Learn more. If you use `password` command in expert mode to reset admin password, we recommend you to reconfigure the password using `configure user admin password` command. After you reconfigure the password, switch to expert mode and ensure that the password hash for admin user is same in /opt/cisco/config/db/sam.config and /etc/shadow files.

After issuing the command, the CLI prompts the user for their current (or old) password, then prompts the user to enter the new password twice.

Syntax

```
configure password
```

Example

```
> configure password
Changing password for admin.
(current) UNIX password:
```

```
New UNIX password:
Retype new UNIX password:
passwd: password updated successfully
```

Secure Firewall Management Center CLI System Commands

The system commands enable the user to manage system-wide files and access control settings.

generate-troubleshoot

Generates troubleshooting data for analysis by Cisco.

Syntax

```
system generate-troubleshoot option1 optionN
```

Where options are one or more of the following, space-separated:

- `ALL`: Run all of the following options.
- `SNT`: Snort Performance and Configuration
- `PER`: Hardware Performance and Logs
- `SYS`: System Configuration, Policy, and Logs
- `DES`: Detection Configuration, Policy, and Logs
- `NET`: Interface and Network Related Data
- `VDB`: Discover, Awareness, VDB Data, and Logs
- `UPG`: Upgrade Data and Logs
- `DBO`: All Database Data
- `LOG`: All Log Data
- `NMP`: Network Map Information

Example

```
> system generate-troubleshoot VDB NMP
starting /usr/local/sf/bin/sf_troubleshoot.pl…
Please, be patient. This may take several minutes.
The troubleshoot options codes specified are VDB,NMP.
Getting filenames from [usr/local/sf/etc/db_updates/index]
Getting filenames from [usr/local/sf/etc/db_updates/base-6.2.3]
Troubleshooting information successfully created at
/var/common/results-06-14-2018—222027.tar.gz
```

lockdown

Removes the `expert` command and access to the Linux shell on the device.

Caution This command is irreversible without a hotfix from Support. Use with care.

Syntax

```
system lockdown
```

Example

```
> system lockdown
```

reboot

Reboots the appliance.

Syntax

```
system reboot
```

Example

```
> system reboot
```

restart

Restarts the appliance application.

Syntax

```
system restart
```

Example

```
> system restart
```

shutdown

Shuts down the appliance.

Syntax

```
system shutdown
```

Example

```
> system shutdown
```

secure-erase

Permanently erases the hard drive data.

Before you use this command, you must connect to the management center using the serial port. When you execute this command, the device reboots and all data is removed permanently. The process may take a few hours to complete; larger drives take longer. Ensure you have the power supply to prevent disruptions during the secure erase process. After the erase is completed, you can install a fresh software image.

Caution Erasing your hard drive results in the loss of all data on the appliance, including the ISO image.

Supported Devices

- Firepower Management Center 1600, 2600, 4600
- Firewall Management Center 1700, 2700, 4700

Syntax

```
secure-erase
```

Example

```
> secure-erase
***************************** Caution *******************************

 If you run this command:
     - The management center hard drive data, including configurations
       and bootable images, will be permanently erased.
     - The device will reboot and reinitialize.

Note: Do not power off your device during this procedure.

*********************************************************************

Do you want to proceed? (Yes/No)
```

History for the Secure Firewall Management Center CLI

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.
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
management center CLI	6.3	Any	Feature introduced. Initially supports the following commands: • `exit` • `expert` • `?` • `show version` • `configure password` • `system generate-troubleshoot` • `system lockdown` • `system reboot` • `system restart` • `system shutdown` Supported platforms: management center