Classic Device Command Line Reference

The Classic device CLI reference applies to:

- 7000 and 8000 Series
- ASA FirePOWER
- NGIPSv

For other Firepower appliances:

- Firepower Threat Defense: See the Cisco Firepower Threat Defense Command Reference.
- Firepower Management Center: See Firepower Management Center Command Line Reference.

About the Classic Device CLI

After you log into a Classic device (7000 and 8000 Series, ASA FirePOWER, NGIPSv) via the CLI (see Logging Into the CLI on 7000/8000 Series, ASA FirePOWER, and NGIPSv Devices), you can use the commands described in this appendix to view, configure, and troubleshoot your device.

Note If you reboot a 7000 or 8000 Series device and then log in to the CLI as soon as you are able, any commands you execute are not recorded in the audit log until the web interface is available.

Note that CLI commands are case-insensitive with the exception of parameters whose text is not part of the CLI framework, such as user names and search filters.

Related Topics

Firepower System User Interfaces

Classic Device 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 classic device 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
```

Classic Device CLI Access Levels

Within each mode, the commands available to a user depend on the user's CLI access. When you create a user account, you can assign it one of the following CLI access levels:

- Basic — The user has read-only access and cannot run commands that impact system performance.
- Configuration — The user has read-write access and can run commands that impact system performance.
- None — The user is unable to log into the CLI.

On 7000 and 8000 Series devices, you can assign command line permissions on the User Management page in the local web interface. On NGIPSv and ASA FirePOWER, you assign command line permissions using the CLI.

Classic Device 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.

configure password

Allows the current user to change their password. 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.

Access

Basic

Syntax

```
configure password
```

Example

```
> configure password
Enter current password:
Enter new password:
Confirm new password:
```

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, and is equivalent to issuing the `logout` CLI command.

Access

Basic

Syntax

```
exit
```

Example

```
configure network ipv4> exit
configure network>
```

expert

Invokes the Linux shell.

Caution We strongly recommend that you do not use the Linux shell unless directed by Cisco TAC or explicit instructions in the user documentation. For more information, see Firepower System User Accounts.

Access

Configuration

Syntax

```
expert
```

Example

```
> expert
```

history

Displays the command line history for the current session.

Access

Basic

Syntax

```
history limit
```

where `limit` sets the size of the history list. To set the size to unlimited, enter zero.

Example

```
history 25
```

logout

Logs the current user out of the current CLI console session.

Access

Basic

Syntax

```
logout
```

Example

```
> logout
```

? (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.

Access

Basic

Syntax

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

Example

```
> ?
```

Classic Device CLI Show Commands

Show commands provide information about the state of the device. These commands do not change the operational mode of the device and running them has minimal impact on system operation. Most show commands are available to all CLI users; however, only users with configuration CLI access can issue the `show user` command.

access-control-config

Displays the currently deployed access control configurations, including:

- Security Intelligence settings
- Names of any subpolicies the access control policy invokes
- Intrusion variable set data
- Logging settings
- Other advanced settings, including policy-level performance, preprocessing, and general settings

Also displays policy-related connection information, such as source and destination port data (including type and code for ICMP entries) and the number of connections that matched each access control rule (hit counts).

Access

Basic

Syntax

```
show access-control-config
```

Example

```
> show access-control-config
```

alarms

Displays currently active (failed/down) hardware alarms on the device. This command is not available on NGIPSv and ASA FirePOWER devices.

Access

Basic

Syntax

```
show alarms
```

Example

```
> show alarms
```

arp-tables

Displays the Address Resolution Protocol tables applicable to your network. This command is not available on NGIPSv and ASA FirePOWER.

Access

Basic

Syntax

```
show arp-tables
```

Example

```
> show arp-tables
```

audit-log

Displays the audit log in reverse chronological order; the most recent audit log events are listed first.

Access

Basic

Syntax

```
show audit-log
```

Example

```
> show audit-log
```

audit_cert

Displays the current audit log client certificate.

Access

Basic

Syntax

```
show audit_cert
```

Example

```
> show audit_cert
```

bypass

On 7000 or 8000 Series devices, lists the inline sets in use and shows the bypass mode status of those sets as one of the following:

- `armed`—the interface pair is configured to go into hardware bypass if it fails (**Bypass Mode: Bypass**), or has been forced into fail-close with the **`configure bypass close`** command
- `engaged`—the interface pair has failed open or has been forced into hardware bypass with the **`configure bypass open`** command
- `off`—the interface pair is set to fail-close (**Bypass Mode: Non-Bypass**); packets are blocked if the interface pair fails

Access

Basic

Syntax

```
show bypass
```

Example

```
> show bypass
s1p1 ↔ s1p2: status 'armed'
s1p1 ↔ s1p2: status 'engaged'
```

high-availability Commands

Displays information about high-availability configuration, status, and member devices or stacks. This command is not available on NGIPSv and ASA FirePOWER devices.

Access

Basic

config

Displays the high-availability configuration on the device.

Syntax

```
show high-availability config
```

Example

```
> show high-availability config
```

high-availability ha-statistics

Displays state sharing statistics for a device in a high-availability pair.

Syntax

```
show high-availability ha-statistics
```

Example

```
> show high-availability ha-statistics
```

cpu

Displays the current CPU usage statistics appropriate for the platform for all CPUs on the device.

For 7000 and 8000 Series devices, the following values are displayed:

- CPU — Processor number.
- Load — The CPU utilization, represented as a number from 0 to 100. 0 is not loaded and 100 is completely loaded.

For NGIPSv and ASA FirePOWER, the following values are displayed:

- CPU — Processor number.
- %user — Percentage of CPU utilization that occurred while executing at the user level (application).

- %nice — Percentage of CPU utilization that occurred while executing at the user level with nice priority.
- %sys — Percentage of CPU utilization that occurred while executing at the system level (kernel). This does not include time spent servicing interrupts or softirqs. A softirq (software interrupt) is one of up to 32 enumerated software interrupts that can run on multiple CPUs at once.
- %iowait — Percentage of time that the CPUs were idle when the system had an outstanding disk I/O request.
- %irq — Percentage of time spent by the CPUs to service interrupts.
- %soft — Percentage of time spent by the CPUs to service softirqs.
- %steal — Percentage of time spent in involuntary wait by the virtual CPUs while the hypervisor was servicing another virtual processor.
- %guest — Percentage of time spent by the CPUs to run a virtual processor.
- %idle — Percentage of time that the CPUs were idle and the system did not have an outstanding disk I/O request.

Access

Basic

Syntax

```
show cpu [procnum]
```

where `procnum` is the number of the processor for which you want the utilization information displayed. Valid values are 0 to one less than the total number of processors on the system. If `procnum` is used for a 7000 or 8000 Series device, it is ignored because for that platform, utilization information can only be displayed for all processors.

```
> show cpu
```

database Commands

The `show database` commands configure the device's management interface.

Access

Basic

processes

Displays a list of running database queries.

Access

Basic

Syntax

```
show database processes
```

Example

```
> show database processes
```

slow-query-log

Displays the slow query log of the database.

Access

Basic

Syntax

```
show database slow-query-log
```

Example

```
> show database slow-query-log
```

device-settings

Displays information about application bypass settings specific to the current device.

Access

Basic

Syntax

```
show device-settings
```

Example

```
> show device-settings
```

disk

Displays the current disk usage.

Access

Basic

Syntax

```
show disk
```

Example

```
> show disk
```

disk-manager

Displays detailed disk usage information for each part of the system, including silos, low watermarks, and high watermarks.

Access

Basic

Syntax

```
show disk-manager
```

Example

```
> show disk-manager
```

dns

Displays the current DNS server addresses and search domains.

Access

Basic

Syntax

```
show dns
```

Example

```
> show dns
```

fan-status

Displays the current status of hardware fans. This command is not available on NGIPSv and ASA FirePOWER devices.

Access

Basic

Syntax

```
show fan-status
```

Example

```
> show fan-status
```

fastpath-rules

Displays the currently configured 8000 Series fastpath rules. This command is only available on 8000 Series devices.

Access

Basic

Syntax

```
show fastpath-rules
```

Example

```
> show fastpath-rules
```

gui

Displays the current state of the web interface. This command is not available on NGIPSv and ASA FirePOWER.

Access

Basic

Syntax

```
show gui
```

Example

```
> show gui
```

hostname

Displays the device's host name and appliance UUID. If you edit the host name of a device using the CLI, confirm that the changes are reflected on the managing Firepower Management Center. In some cases, you may need to edit the device management settings manually.

Access

Basic

Syntax

```
show hostname
```

Example

```
> show hostname
```

hosts

Displays the contents of an ASA FirePOWER module's /etc/hosts file.

Access

Basic

Syntax

```
show hosts
```

Example

```
> show hosts
```

http-cert-expire-date

Displays the current expiration date for the default HTTPS server certificate on the appliance. This command is not available on NGIPSv and ASA FirePOWER devices.

Access

Basic

Syntax

```
show http-cert-expire-date
```

Example

```
> show http-cert-expire-date
```

hyperthreading

Displays whether hyperthreading is enabled or disabled. This command is not available on ASA FirePOWER.

Access

Basic

Syntax

```
show hyperthreading
```

Example

```
> show hyperthreading
```

inline-sets

Displays configuration data for all inline security zones and associated interfaces. This command is not available on ASA FirePOWER.

Access

Basic

Syntax

```
show inline-sets
```

Example

```
> show inline-sets
```

interfaces

If no parameters are specified, displays a list of all configured interfaces. If a parameter is specified, displays detailed information about the specified interface.

Access

Basic

Syntax

```
show interfaces interface
```

where *interface* is the specific interface for which you want the detailed information.

Example

```
> show interfaces
```

ifconfig

Displays the interface configuration for an ASA FirePOWER module.

Access

Basic

Syntax

```
show ifconfig
```

Example

```
> show ifconfig
```

lcd

Displays whether the LCD hardware display is enabled or disabled. This command is not available on NGIPSv and ASA FirePOWER.

Access

Basic

Syntax

```
show lcd
```

Example

```
> show lcd
```

link-aggregation Commands

The `show link-aggregation` commands display configuration and statistics information for link aggregation groups (LAGs). This command is not available on NGIPSv and ASA FirePOWER devices.

Access

Basic

configuration

Displays configuration details for each configured LAG, including LAG ID, number of interfaces, configuration mode, load-balancing mode, LACP information, and physical interface type.

Access

Basic

Syntax

```
show link-aggregation configuration
```

Example

```
> show link-aggregation configuration
```

statistics

Displays statistics, per interface, for each configured LAG, including status, link state and speed, configuration mode, counters for received and transmitted packets, and counters for received and transmitted bytes.

Access

Basic

Syntax

```
show link-aggregation statistics
```

Example

```
> show link-aggregation statistics
```

link-state

Displays type, link, and speed, duplex state, and bypass mode of the ports on the device. This command is not available on ASA FirePOWER devices.

Access

Basic

Syntax

```
show link-state
```

Example

```
> show link-state
```

log-ips-connection

Displays whether the logging of connection events that are associated with logged intrusion events is enabled or disabled.

Access

Basic

Syntax

```
show log-ips-connection
```

Example

```
> show log-ips-connection
```

managers

Displays the configuration and communication status of the Firepower Management Center. Registration key and NAT ID are only displayed if registration is pending.

If a device is configured as a secondary device in a stacked configuration, information about both the managing FMC and the primary device is displayed.

Access

Basic

Syntax

```
show managers
```

Example

```
> show managers
```

memory

Displays the total memory, the memory in use, and the available memory for the device.

Access

Basic

Syntax

```
show memory
```

Example

```
> show memory
```

model

Displays model information for the device.

Access

Basic

Syntax

```
show model
```

Example

```
> show model
```

mpls-depth

Displays the number of MPLS layers configured on the management interface, from 0 to 6. This command is not available on NGIPSv and ASA FirePOWER.

Access

Basic

Syntax

```
show mpls-depth
```

Example

```
> show mpls-depth
```

NAT Commands

The `show nat` commands display NAT data and configuration information for the management interface. This command is not available on NGIPSv and ASA FirePOWER devices.

Access

Basic

active-dynamic

Displays NAT flows translated according to dynamic rules. These entries are displayed when a flow matches a rule, and persist until the rule has timed out. Therefore, the list can be inaccurate. Timeouts are protocol dependent: ICMP is 5 seconds, UDP is 120 seconds, TCP is 3600 seconds, and all other protocols are 60 seconds.

Syntax

```
show nat active-dynamic
```

Example

```
> show nat active-dynamic
```

active-static

Displays NAT flows translated according to static rules. These entries are displayed as soon as you deploy the rule to the device, and the list does not indicate active flows that match a static NAT rule.

Syntax

```
show nat active-static
```

Example

```
> show nat active-static
```

allocators

Displays information for all NAT allocators, the pool of translated addresses used by dynamic rules.

Syntax

```
show nat allocators
```

Example

```
> show nat allocators
```

config

Displays the current NAT policy configuration for the management interface.

Syntax

```
show nat config
```

Example

```
> show nat config
```

dynamic-rules

Displays dynamic NAT rules that use the specified allocator ID.

Syntax

```
show nat dynamic-rules allocator_id
```

where `allocator_id` is a valid allocator ID number.

Example

```
> show nat dynamic-rules 9
```

flows

Displays the number of flows for rules that use the specified allocator ID.

Syntax

```
show nat flows allocator-id
```

where *allocator_id* is a valid allocator ID number.

Example

```
> show nat flows 81
```

static-rules

Displays all static NAT rules.

Syntax

```
show nat static-rules
```

Example

```
> show nat static-rules
```

netstat

Displays the active network connections for an ASA FirePOWER module.

Access

Basic

Syntax

```
show netstat
```

Example

```
> show netstat
```

network

Displays the IPv4 and IPv6 configuration of the management interface, its MAC address, and HTTP proxy address, port, and username if configured.

Access

Basic

Syntax

```
show network
```

Example

```
> show network
```

network-modules

Displays all installed modules and information about them, including serial numbers. This command is not available on NGIPSv and ASA FirePOWER.

Access

Basic

Syntax

```
show network-modules
```

Example

```
> show network-modules
```

network-static-routes

Displays all configured network static routes and information about them, including interface, destination address, network mask, and gateway address.

Access

Basic

Syntax

```
show network-static-routes
```

Example

```
> show network-static-routes
```

ntp

Displays the ntp configuration.

Access

Basic

Syntax

```
show ntp
```

Example

```
> show ntp
```

perfstats

Displays performance statistics for the device.

Access

Basic

Syntax

```
show perfstats
```

Example

```
> show perfstats
```

portstats

Displays port statistics for all installed ports on the device. This command is not available on NGIPSv and ASA FirePOWER.

Access

Basic

Syntax

```
show portstats [copper | fiber | internal | external | all]
```

where copper specifies for all copper ports, fiber specifies for all fiber ports, internal specifies for all internal ports, external specifies for all external (copper and fiber) ports, and all specifies for all ports (external and internal).

Example

```
> show portstats fiber
```

power-supply-status

Displays the current state of hardware power supplies. This command is not available on NGIPSv and ASA FirePOWER.

Note If an 8000 Series managed device experiences a power failure, it may take up to 15 minutes for the show power-supply-status CLI command to reflect the correct status.

Access

Basic

Syntax

```
show power-supply-status
```

Example

```
> show power-supply-status
```

process-tree

Displays processes currently running on the device, sorted in tree format by type.

Access

Basic

Syntax

```
show process-tree
```

Example

```
> show process-tree
```

processes

Displays processes currently running on the device, sorted by descending CPU usage.

Access

Basic

Syntax

```
show processes sort-flag filter
```

where *sort-flag* can be `-m` to sort by memory (descending order), `-u` to sort by username rather than the process name, or `verbose` to display the full name and path of the command. The *filter* parameter specifies the search term in the command or username by which results are filtered. The header row is still displayed.

Example

```
> show processes -u user1
```

route

Displays the routing information for an ASA FirePOWER module.

Access

Basic

Syntax

```
show route
```

Example

```
> show route
```

routing-table

If no parameters are specified, displays routing information for all virtual routers. If parameters are specified, displays routing information for the specified router and, as applicable, its specified routing protocol type. All parameters are optional. This command is not available on NGIPSv and ASA FirePOWER.

Access

Basic

Syntax

```
show routing-table name [ ospf | rip | static ]
```

where *name* is the name of the specific router for which you want information, and `ospf`, `rip`, and `static` specify the routing protocol type.

Example

```
> show routing-table Vrouter1 static
```

serial-number

Displays the chassis serial number. This command is not available on NGIPSv.

Access

Basic

Syntax

```
show serial-number
```

Example

```
> show serial-number
```

ssl-policy-config

Displays the currently deployed SSL policy configuration, including policy description, default logging settings, all enabled SSL rules and rule configurations, trusted CA certificates, and undecryptable traffic actions.

Access

Basic

Syntax

```
show ssl-policy-config
```

Example

```
> show ssl-policy-config
```

stacking

Shows the stacking configuration and position on managed devices; on devices configured as primary, also lists data for all secondary devices. For stacks in a high-availability pair, this command also indicates that the stack is a member of a high-availability pair. The user must use the web interface to enable or (in most cases) disable stacking; if stacking is not enabled, the command will return `Stacking not currently configured`. This command is not available on NGIPSv and ASA FirePOWER.

Access

Basic

Syntax

```
show stacking
```

Example

```
> show stacking
```

summary

Displays a summary of the most commonly used information (version, type, UUID, and so on) about the device. For more detailed information, see the following `show` commands: `version`, `interfaces`, `device-settings`, and `access-control-config`.

Access

Basic

Syntax

```
show summary
```

Example

```
> show summary
```

syslog

Displays the system log in reverse chronological order. You can optionally specify a filter to display specific records based on content and the number of records to display per page view (the default is 25).

Access

Basic

Syntax

```
show syslog ["filter" records_per_page]
```

where *filter* specifies a Grep-compatible search filter and *records_per_page* specifies the number of records to display with each page view. See Syntax for System Log Filters for more information on search filters.

Example

```
> show syslog "ssh" 20
```

The system displays the 20 most recent syslog records containing the string "ssh". To display the next 20 records, press Enter; to stop the display enter q.

time

Displays the current date and time in UTC and in the local time zone configured for the current user.

Access

Basic

Syntax

```
show time
```

Example

```
> show time
```

traffic-statistics

If no parameters are specified, displays details about bytes transmitted and received from all ports. If a port is specified, displays that information only for the specified port. You cannot specify a port for ASA FirePOWER modules; the system displays only the data plane interfaces.

Note In some situations the output of this command may show packet drops when, in point of fact, the device is not dropping traffic. Drop counters increase when malformed packets are received. A malformed packet may be missing certain information in the header or it may have failed a cyclical-redundancy check (CRC). Typically, common root causes of malformed packets are data link layer issues such as bad cables or a bad interface. The dropped packets are not logged. However, if the source is a reliable transport protocol such as TCP, the packets will be retransmitted.

Access

Basic

Syntax

```
show traffic-statistics port
```

where *port* is the specific port for which you want information.

Example

```
> show traffic-statistics s1p1
```

user

Applicable to NGIPSv only. Displays detailed configuration information for the specified user(s). The following values are displayed:

- Login — the login name
- UID — the numeric user ID
- Auth (`Local` or `Remote`) — how the user is authenticated
- Access (`Basic` or `Config`) — the user's privilege level
- Enabled (`Enabled` or `Disabled`) — whether the user is active
- Reset (`Yes` or `No`) — whether the user must change password at next login
- Exp (`Never` or a number) — the number of days until the user's password must be changed
- Warn (`N/A` or a number) — the number of days a user is given to change their password before it expires
- Str (`Yes` or `No`) — whether the user's password must meet strength checking criteria
- Lock (`Yes` or `No`) — whether the user's account has been locked due to too many login failures
- Max (`N/A` or a number) — the maximum number of failed logins before the user's account is locked

Access

Configuration

Syntax

```
show user username username username ...
```

where *username* specifies the name of the user and the usernames are space-separated.

Example

```
> show user jdoe
```

users

Applicable to NGIPSv and ASA FirePOWER only. Displays detailed configuration information for all local users. The following values are displayed:

- Login — the login name
- UID — the numeric user ID
- Auth (`Local` or `Remote`) — how the user is authenticated
- Access (`Basic` or `Config`) — the user's privilege level
- Enabled (`Enabled` or `Disabled`) — whether the user is active
- Reset (`Yes` or `No`) — whether the user must change password at next login
- Exp (`Never` or a number) — the number of days until the user's password must be changed
- Warn (`N/A` or a number) — the number of days a user is given to change their password before it expires
- Str (`Yes` or `No`) — whether the user's password must meet strength checking criteria
- Lock (`Yes` or `No`) — whether the user's account is locked due to too many login failures
- Max (`N/A` or a number) — the maximum number of failed logins before the user's account is locked

Access

Configuration

Syntax

```
show users
```

Example

```
> show users
```

version

Displays the product version and build. If the `detail` parameter is specified, displays the versions of additional components.

Note The `detail` parameter is not available on ASA with FirePOWER Services.

Access

Basic

Syntax

```
show version [detail]
```

Example

```
> show version
```

virtual-routers

If no parameters are specified, displays a list of all currently configured virtual routers with DHCP relay, OSPF, and RIP information. If parameters are specified, displays information for the specified router, limited by the specified route type. All parameters are optional. This command is not available on NGIPSv and ASA FirePOWER.

Access

Basic

Syntax

`show virtual-routers [ dhcprelay | ospf | rip ] name`

where `dhcprelay`, `ospf`, and `rip` specify for route types, and *name* is the name of the specific router for which you want information. If you specify `ospf`, you can then further specify `neighbors`, `topology`, or `lsadb` between the route type and (if present) the router name.

Example

```
> show virtual-routers ospf VRouter2
```

virtual-switches

If no parameters are specified, displays a list of all currently configured virtual switches. If parameters are specified, displays information for the specified switch. This command is not available on NGIPSv and ASA FirePOWER.

Access

Basic

Syntax

`show virtual-switches name`

Example

```
> show virtual-switches Vswitch1
```

vmware-tools

Indicates whether VMware Tools are currently enabled on a virtual device. This command is available only on NGIPSv.

VMware Tools is a suite of utilities intended to enhance the performance of the virtual machine. These utilities allow you to make full use of the convenient features of VMware products. The system supports the following plugins on all virtual appliances:

- guestInfo
- powerOps
- timeSync
- vmbackup

For more information about VMware Tools and the supported plugins, see the VMware website (http://www.vmware.com).

Access

Basic

Syntax

```
show vmware-tools
```

Example

```
> show vmware-tools
```

VPN Commands

The `show VPN` commands display VPN status and configuration information for VPN connections. This command is not available on NGIPSv and ASA FirePOWER devices.

Access

Basic

config

Displays the configuration of all VPN connections.

Syntax

```
show vpn config
```

Example

```
> show vpn config
```

config by virtual router

Displays the configuration of all VPN connections for a virtual router.

Syntax

```
show vpn config virtual router
```

Example

```
> show vpn config VRouter1
```

status

Displays the status of all VPN connections.

Syntax

```
show vpn status
```

Example

```
> show vpn status
```

status by virtual router

Displays the status of all VPN connections for a virtual router.

Syntax

```
show vpn status virtual router
```

Example

```
> show vpn status VRouter1
```

counters

Displays the counters for all VPN connections.

Syntax

```
show vpn counters
```

Example

```
> show vpn counters
```

counters by virtual router

Displays the counters of all VPN connections for a virtual router.

Syntax

```
show vpn counters virtual router
```

Example

```
> show vpn counters VRouter1
```

Classic Device CLI Configuration Commands

The configuration commands enable the user to configure and manage the system. These commands affect system operation; therefore, with the exception of Basic-level `configure password`, only users with configuration CLI access can issue these commands.

audit_cert Commands

The `configure audit_cert` commands configure the device's audit log client certificate for secure audit log streaming.

Access

Configuration

delete

Deletes the current client certificate for secure audit log streaming.

Syntax

```
configure audit_cert delete
```

Example

```
> configure audit_cert delete
```

import

Imports a client certificate for secure audit log streaming. After the user enters the command, the CLI prompts the user to provide either a client certificate and private key, or a certificate chain.

Syntax

```
configure audit_cert import
```

Example

```
> configure audit_cert import
***************Import Audit Client Certificate**************

1 Import Client Certificate and Private Key
2 Import Certificate Chain
0 Exit

************************************************************
Enter choice: 1
Enter your audit client certificate (PEM format) here:
-----BEGIN CERTIFICATE-----
MIIEoTCCA4mgAwIBAgICAR4wDQYJK0ZIhvcNaQALBWAugYICzAJBqNVBATYAiVT
   ...certificate details ...
Tx*FAhnXeUZ78hFepg1yHQMYWTkD7hCqmSN3UkAb1l0IoBcxTA==
-----END CERTIFICATE-----

Enter your private key (PEM format) here:
-----BEGIN RSA PRIVATE KEY-----
miiieOWobabkc3qwaOgVx0Tt61eY83Mrqa+bek_qPetcHRAw6ea4p0TlMVVsE7qr
   ...private key details ...
nRI6QNkoumLUT9EvjF6bFoT3M6eDI7+NdDIhjVeOP*E4+hxEX50jM
-----END RSA PRIVATE KEY-----

Client certificate import succeed, exiting...
```

bypass

On 7000 or 8000 Series devices, places an inline pair in fail-open (hardware bypass) or fail-close mode. You can use this command only when the inline set **Bypass Mode** option is set to **Bypass**.

Note that rebooting a device takes an inline set out of fail-open mode.

Access

Configuration

Syntax

```
configure bypass {open | close} {interface}
```

where `interface` is the name of either hardware port in the inline pair.

Example

```
> configure bypass open s1p1
```

high-availability

Disables or configures bypass for high availability on the device. This command is not available on NGIPSv, ASA FirePOWER, or on devices configured as secondary stack members.

Access

Configuration

Syntax

```
configure high-availability {disable | bypass}
```

Example

```
> configure high-availability disable
```

gui

Enables or disables the device web interface, including the streamlined upgrade web interface that appears during major updates to the system. This command is not available on NGIPSv and ASA FirePOWER.

Access

Configuration

Syntax

```
configure gui [enable | disable]
```

Example

```
> configure gui disable
```

lcd

Enables or disables the LCD display on the front of the device. This command is not available on NGIPSv and ASA FirePOWER.

Access

Configuration

Syntax

```
configure lcd {enable | disable}
```

Example

```
> configure lcd disable
```

log-ips-connections

Enables or disables logging of connection events that are associated with logged intrusion events.

Access

Configuration

Syntax

```
configure log-ips-connections {enable | disable}
```

Example

```
> configure log-ips-connections disable
```

manager Commands

The `configure manager` commands configure the device's connection to its managing Firepower Management Center.

Access

Configuration

add

Configures the device to accept a connection from a managing Firepower Management Center. This command works only if the device is not actively managed.

A unique alphanumeric registration key is always required to register a device to a Firepower Management Center. In most cases, you must provide the hostname or the IP address along with the registration key. However, if the device and the Firepower Management Center are separated by a NAT device, you must enter a unique NAT ID, along with the registration key, and specify `DONTRESOLVE` instead of the hostname.

Syntax

```
configure manager add {hostname | IPv4_address | IPv6_address | DONTRESOLVE} regkey [nat_id]
```

where `{`hostname `|` IPv4_address `|` IPv6_address `|` `DONTRESOLVE}` specifies the DNS host name or IP address (IPv4 or IPv6) of the Firepower Management Center that manages this device. If the Firepower Management Center is not directly addressable, use `DONTRESOLVE`. If you use`DONTRESOLVE`, nat_id is required. regkey is the unique alphanumeric registration key required to register a device to the Firepower Management Center. nat_id is an optional alphanumeric string used during the registration process between the Firepower Management Center and the device. It is required if the hostname is set to `DONTRESOLVE`.

Example

```
> configure manager add DONTRESOLVE abc123 efg456
```

delete

Removes the Firepower Management Center's connection information from the device. This command only works if the device is not actively managed.

Syntax

```
configure manager delete
```

Example

```
> configure manager delete
```

mpls-depth

Configures the number of MPLS layers on the management interface. This command is not available on NGIPSv and ASA FirePOWER.

Access

Configuration

Syntax

```
configure mpls-depth depth
```

where *depth* is a number between 0 and 6.

Example

```
> configure mpls-depth 3
```

network Commands

The `configure network` commands configure the device's management interface.

Access

Configuration

dns searchdomains

Replaces the current list of DNS search domains with the list specified in the command.

Syntax

```
configure network dns searchdomains {searchlist}
```

where `searchlist` is a comma-separated list of domains.

Example

```
> configure network dns searchdomains foo.bar.com,bar.com
```

dns servers

Replaces the current list of DNS servers with the list specified in the command.

Syntax

```
configure nework dns servers {dnslist}
```

where dnslist is a comma-separated list of DNS servers.

Example

```
> configure network dns servers 10.123.1.10,10.124.1.10
```

hostname

Sets the hostname for the device.

Syntax

```
configure network hostname {name}
```

where name is the new hostname.

Example

```
> configure network hostname sfrocks
```

http-proxy

On 7000 & 8000 Series and NGIPSv devices, configures an HTTP proxy. After issuing the command, the CLI prompts the user for the HTTP proxy address and port, whether proxy authentication is required, and if it is required, the proxy username, proxy password, and confirmation of the proxy password.

Use this command on NGIPSv to configure an HTTP proxy server so the virtual device can submit files to the AMP cloud for dynamic analysis.

Syntax

The proxy password can use only alphanumeric characters.

```
configure network http-proxy
```

Example

```
> configure network http-proxy
Manual proxy configuration
Enter HTTP Proxy address:
Enter HTTP Proxy Port:
Use Proxy Authentication? (y/n) [n]:
Enter Proxy Username:
Enter Proxy Password:
Confirm Proxy Password:
```

http-proxy-disable

On 7000 Series, 8000 Series, or NGIPSv devices, deletes any HTTP proxy configuration.

Syntax

```
configure network http-proxy-disable
```

Example

```
> configure network http-proxy-disable
Are you sure that you wish to delete the current
http-proxy configuration? (y/n):
```

ipv4 delete

Disables the IPv4 configuration of the device's management interface.

Syntax

```
configure network ipv4 delete [management_interface]
```

where *management_interface* is the management interface ID. If you do not specify an interface, this command configures the default management interface. This parameter is needed only if you use the **configure management-interface** commands to enable more than one management interface. Multiple management interfaces are supported on 8000 series devices and the ASA 5585-X with FirePOWER services only. Do not specify this parameter for other platforms. The management interface IDs are **eth0** for the default management interface and **eth1** for the optional event interface.

Example

```
> configure network ipv4 delete eth1
```

ipv4 dhcp

Sets the IPv4 configuration of the device's management interface to DHCP. The management interface communicates with the DHCP server to obtain its configuration information.

Syntax

```
configure network ipv4 dhcp [management_interface]
```

where *management_interface* is the management interface ID. DHCP is supported only on the default management interface, so you do not need to use this argument.

Example

```
> configure network ipv4 dhcp
```

ipv4 manual

Manually configures the IPv4 configuration of the device's management interface.

Syntax

```
configure network ipv4 manual ipaddr netmask [gw] [management_interface]
```

where *ipaddr* is the IP address, *netmask* is the subnet mask, and *gw* is the IPv4 address of the default gateway. The *management_interface* is the management interface ID. If you do not specify an interface, this command configures the default management interface. This parameter is needed only if you use the **configure management-interface** commands to enable more than one management interface. Multiple management interfaces are supported on 8000 series devices and the ASA 5585-X with FirePOWER services only. Do not specify this parameter for other platforms. The management interface IDs are **eth0** for the default management interface and **eth1** for the optional event interface.

Example

```
> configure network ipv4 manual 10.123.1.10 255.255.0.0 10.123.1.1
```

ipv6 delete

Disables the IPv6 configuration of the device's management interface.

Syntax

```
configure network ipv6 delete [management_interface]
```

where *management_interface* is the management interface ID. If you do not specify an interface, this command configures the default management interface. This parameter is needed only if you use the **configure management-interface** commands to enable more than one management interface. Multiple management interfaces are supported on 8000 series devices and the ASA 5585-X with FirePOWER services only. Do not specify this parameter for other platforms. The management interface IDs are **eth0** for the default management interface and **eth1** for the optional event interface.

Example

```
> configure network ipv6 delete
```

ipv6 dhcp

Sets the IPv6 configuration of the device's management interface to DHCP. The management interface communicates with the DHCP server to obtain its configuration information.

Syntax

```
configure network ipv6 dhcp [management_interface]
```

where *management_interface* is the management interface ID. DHCP is supported only on the default management interface, so you do not need to use this argument.

Example

```
> configure network ipv6 dhcp
```

ipv6 manual

Manually configures the IPv6 configuration of the device's management interface.

Syntax

```
configure network ipv6 manual ip6addr/ip6prefix [ip6gw] [management_interface]
```

where *ip6addr*/*ip6prefix* is the IP address and prefix length and *ip6gw* is the IPv6 address of the default gateway. The *management_interface* is the management interface ID. If you do not specify an interface, this command configures the default management interface. This parameter is needed only if you use the **configure management-interface** commands to enable more than one management interface. Multiple management interfaces are supported on 8000 series devices and the ASA 5585-X with FirePOWER services only. Do not specify this parameter for other platforms. The management interface IDs are **eth0** for the default management interface and **eth1** for the optional event interface.

Example

```
> configure network ipv6 manual 2001:DB8:3ffe:1900:4545:3:200:f8ff:fe21:67cf 64
```

ipv6 router

Sets the IPv6 configuration of the device's management interface to Router. The management interface communicates with the IPv6 router to obtain its configuration information.

Syntax

```
configure network ipv6 router [management_interface]
```

where *management_interface* is the management interface ID. If you do not specify an interface, this command configures the default management interface. This parameter is needed only if you use the **configure management-interface** commands to enable more than one management interface. Multiple management interfaces are supported on 8000 series devices and the ASA 5585-X with FirePOWER services only. Do not specify this parameter for other platforms. The management interface IDs are **eth0** for the default management interface and **eth1** for the optional event interface.

Example

```
> configure network ipv6 router
```

management-interface disable

Disables a management interface. Multiple management interfaces are supported on 8000 series devices and the ASA 5585-X with FirePOWER services only.

Syntax

```
configure network management-interface disable ethn
```

where *n* is the number of the management interface you want to configure. **eth0** is the default management interface and **eth1** is the optional event interface. Cisco recommends that you leave the eth0 default management interface enabled, with both management and event channels enabled. See Management Interfaces for detailed information about using a separate event interface on the Firepower Management Center and on the managed device.

Example

```
> configure network management-interface disable eth1
```

management-interface disable-event-channel

Disables the event traffic channel on the specified management interface. Multiple management interfaces are supported on 8000 series devices and the ASA 5585-X with FirePOWER services only.

Syntax

```
configure network management-interface disable-event-channel ethn
```

where *n* is the number of the management interface you want to configure. **eth0** is the default management interface and **eth1** is the optional event interface. Cisco recommends that you leave the eth0 default management interface enabled, with both management and event channels enabled. See Management Interfaces for detailed information about using a separate event interface on the Firepower Management Center and on the managed device.

Example

```
> configure network management-interface disable-event-channel eth1
```

management-interface disable-management-channel

Disables the management traffic channel on the specified management interface. Multiple management interfaces are supported on 8000 series devices and the ASA 5585-X with FirePOWER services only.

Syntax

```
configure network management-interface disable-management-channel ethn
```

where *n* is the number of the management interface you want to configure. **eth0** is the default management interface and **eth1** is the optional event interface. Cisco recommends that you leave the eth0 default management interface enabled, with both management and event channels enabled. See Management Interfaces for detailed information about using a separate event interface on the Firepower Management Center and on the managed device.

Example

```
> configure network management-interface disable-management-channel eth1
```

management-interface enable

Enables the specified management interface. Multiple management interfaces are supported on 8000 series devices and the ASA 5585-X with FirePOWER services only.

Syntax

```
configure network management-interface enable ethn
```

where *n* is the number of the management interface you want to enable. **eth0** is the default management interface and **eth1** is the optional event interface.

For device management, the Firepower Management Center management interface carries two separate traffic channels: the management traffic channel carries all internal traffic (such as inter-device traffic specific to the management of the device), and the event traffic channel carries all event traffic (such as web events). You can optionally configure a separate event-only interface on the Management Center to handle event traffic (see the Firepower Management Center web interface do perform this configuration). You can only configure one event-only interface. Event traffic can use a large amount of bandwidth, so separating event traffic from management traffic can improve the performance of the Management Center.

The default eth0 interface includes both management and event channels by default. You can optionally enable the eth0 interface as an event-only interface. Event traffic is sent between the device event interface and the Firepower Management Center event interface if possible. If the event network goes down, then event traffic reverts to the default management interface. Separate event interfaces are used when possible, but the management interface is always the backup.

When you enable a management interface, both management and event channels are enabled by default. We recommend that you use the default management interface for both management and eventing channels; and then enable a separate event-only interface. The Firepower Management Center event-only interface cannot accept management channel traffic, so you should simply disable the management channel on the device event interface.

Use the **configure network** {**ipv4** | **ipv6**} **manual** commands to configure the address(es) for management interfaces.

Example

```
> configure network management-interface enable eth1
> configure network management-interface disable-management-channel eth1
```

management-interface enable-event-channel

Enables the event traffic channel on the specified management interface. Multiple management interfaces are supported on 8000 series devices and the ASA 5585-X with FirePOWER services only.

Syntax

```
configure network management-interface enable-event-channel ethn
```

where *n* is the number of the management interface you want to configure. **eth0** is the default management interface and **eth1** is the optional event interface. Cisco recommends that you leave the eth0 default management interface enabled, with both management and event channels enabled. See Management Interfaces for detailed information about using a separate event interface on the Firepower Management Center and on the managed device.

Example

```
> configure network management-interface enable-event-channel eth1
```

management-interface enable-management-channel

Enables the management traffic channel on the specified management interface. Multiple management interfaces are supported on 8000 series devices and the ASA 5585-X with FirePOWER services only.

Syntax

```
configure network management-interface enable-management-channel ethn
```

where *n* is the number of the management interface you want to configure. **eth0** is the default management interface and **eth1** is the optional event interface. Cisco recommends that you leave the eth0 default management interface enabled, with both management and event channels enabled. See Management Interfaces for detailed information about using a separate event interface on the Firepower Management Center and on the managed device.

Example

```
> configure network management-interface enable-management-channel eth1
```

management-interface tcpport

Changes the value of the TCP port for management.

Syntax

```
configure network management-interface tcpport port
```

where *port* is the management port value you want to configure.

Example

```
> configure network management-interface tcpport 8500
```

management-port

Sets the value of the device's TCP management port.

Syntax

```
configure network management-port number
```

where *number* is the management port value you want to configure.

Example

```
> configure network management-port 8500
```

static-routes ipv4 add

Adds an IPv4 static route for the specified management interface.

Syntax

```
configure network static-routes ipv4
add interface destination netmask gateway
```

where interface is the management interface, destination is the destination IP address, netmask is the network mask address, and gateway is the gateway address you want to add.

Example

```
> configure network static-routes ipv4
add eth1 10.115.24.0 255.255.255.0 10.115.9.2
```

static-routes ipv4 delete

Deletes an IPv4 static route for the specified management interface.

Syntax

```
configure network static-routes ipv4
delete interface destination netmask gateway
```

where interface is the management interface, destination is the destination IP address, netmask is the network mask address, and gateway is the gateway address you want to delete.

Example

```
> configure network static-routes ipv4
delete eth1 10.115.24.0 255.255.255.0 10.115.9.2
```

static-routes ipv6 add

Adds an IPv6 static route for the specified management interface.

Syntax

```
configure network static-routes ipv6
add interface destination prefix gateway
```

where interface is the management interface, destination is the destination IP address, prefix is the IPv6 prefix length, and gateway is the gateway address you want to add.

Example

```
> configure network static-routes ipv6
add eth1 2001:DB8:3ffe:1900:4545:3:200: f8ff:fe21:67cf 64
```

static-routes ipv6 delete

Deletes an IPv6 static route for the specified management interface.

Syntax

```
configure network static-routes ipv6
delete interface destination prefix gateway
```

where interface is the management interface, destination is the destination IP address, prefix is the IPv6 prefix length, and gateway is the gateway address you want to delete.

Example

```
> configure network static-routes ipv6
delete eth1 2001:DB8:3ffe:1900:4545:3:200:f8ff: fe21:67cf 64
```

password

Allows the current user to change their password. 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.

Access

Basic

Syntax

```
configure password
```

Example

```
> configure password
Enter current password:
Enter new password:
Confirm new password:
```

stacking disable

On 7000 and 8000 Series devices, removes any stacking configuration present on that device:

- On devices configured as primary, the stack is removed entirely.
- On devices configured as secondary, that device is removed from the stack.

This command is not available on NGIPSv or ASA FirePOWER modules, and you cannot use it to break a device high-availability pair.

Use this command when you cannot establish communication with appliances higher in the stacking hierarchy. If the Firepower Management Center is available for communication, a message appears instructing you to use the Firepower Management Center web interface instead; likewise, if you enter `stacking disable` on a device configured as secondary when the primary device is available, a message appears instructing you to enter the command from the primary device.

Access

Configuration

Syntax

```
configure stacking disable
```

Example

```
> configure stacking disable
```

user Commands

Applicable only to NGIPSv, the `configure user` commands manage the device's local user database.

Access

Configuration

access

Modifies the access level of the specified user. This command takes effect the next time the specified user logs in.

Syntax

```
configure user access username [basic | config]
```

where *username* specifies the name of the user for which you want to modify access, `basic` indicates basic access, and `config` indicates configuration access.

Example

```
> configure user access jdoe basic
```

add

Creates a new user with the specified name and access level. This command prompts for the user's password.

Syntax

```
configure user add username [basic | config]
```

where username specifies the name of the new user, `basic` indicates basic access, and `config` indicates configuration access.

Example

```
> configure user add jdoe basic
Enter new password for user jdoe:
Confirm new password for user jdoe:
```

aging

Forces the expiration of the user's password.

Syntax

```
configure user aging username max_days warn_days
```

where `username` specifies the name of the user, `max_days` indicates the maximum number of days that the password is valid, and`warn_days` indicates the number of days that the user is given to change the password before it expires.

Example

```
> configure user aging jdoe 100 3
```

delete

Deletes the user and the user's home directory.

Syntax

```
configure user delete username
```

where `username` specifies the name of the user.

Example

```
> configure user delete jdoe
```

disable

Disables the user. Disabled users cannot login.

Syntax

```
configure user disable username
```

where `username` specifies the name of the user.

Example

```
> configure user disable jdoe
```

enable

Enables the user.

Syntax

```
configure user enable username
```

where username specifies the name of the user.

Example

```
> configure user enable jdoe
```

forcereset

Forces the user to change their password the next time they login. When the user logs in and changes the password, strength checking is automatically enabled.

Syntax

```
configure user forcereset username
```

where *username* specifies the name of the user.

Example

```
> configure user forcereset jdoe
```

maxfailedlogins

Sets the maximum number of failed logins for the specified user.

Syntax

```
configure user maxfailedlogins username number
```

where *username* specifies the name of the user, and *number* specifies the maximum number of failed logins.

Example

```
> configure user maxfailedlogins jdoe 3
```

minpasswdlen

Sets the minimum number of characters a user password must contain.

Syntax

```
configure user minpasswdlen username number
```

Where *username* specifies the name of the user account, and *number* specifies the minimum number of characters the password for that account must contain (ranging from 1 to 127).

Example

```
> configure user minpasswdlen jdoe 13
```

password

Sets the user's password. This command prompts for the user's password.

Syntax

```
configure user password username
```

where *username* specifies the name of the user.

Example

```
> configure user pasword jdoe
Enter new password for user jdoe:
Confirm new password for user jdoe:
```

strengthcheck

Enables or disables the strength requirement for a user's password. When a user's password expires or if the configure user forcereset command is used, this requirement is automatically enabled the next time the user logs in.

Syntax

```
configure user strengthcheck username {enable | disable}
```

where *username* specifies the name of the user, `enable` sets the requirement for the specified users password, and `disable` removes the requirement for the specified user's password.

Example

```
> configure user strengthcheck jdoe enable
```

unlock

Unlocks a user that has exceeded the maximum number of failed logins.

Syntax

```
configure user unlock username
```

where *username* specifies the name of the user.

Example

```
> configure user unlock jdoe
```

vmware-tools

Enables or disables VMware Tools functionality on NGIPSv. This command is available only on NGIPSv.

VMware Tools is a suite of utilities intended to enhance the performance of the virtual machine. These utilities allow you to make full use of the convenient features of VMware products. The system supports the following plugins on all virtual appliances:

- guestInfo
- powerOps
- timeSync
- vmbackup

For more information about VMware Tools and the supported plugins, see the VMware website (http://www.vmware.com).

Access

Basic

Syntax

```
configure vmware-tools [enable | disable]
```

Example

```
> configure vmware-tools enable
```

Classic Device CLI System Commands

The system commands enable the user to manage system-wide files and access control settings. Only users with configuration CLI access can issue commands in system mode.

access-control Commands

The `system access-control` commands enable the user to manage the access control configuration on the device.

Access

Configuration

archive

Saves the currently deployed access control policy as a text file on `/var/common`.

Syntax

```
system access-control archive
```

Example

```
> system access-control archive
```

clear-rule-counts

Resets the access control rule hit count to 0.

Syntax

```
system access-control clear-rule-counts
```

Example

```
> system access-control clear-rule-counts
```

rollback

Reverts the system to the previously deployed access control configuration. You cannot use this command with devices in stacks or high-availability pairs.

Syntax

```
system access-control rollback
```

Example

```
> system access-control rollback
```

compliance Commands

The `compliance` commands display and configure the device's security certifications compliance mode.

Caution After you enable this setting, you cannot disable it. If you need to do so, contact Support for assistance.

Access

Configuration

enable cc

Configures the device's security certifications compliance to Common Criteria (CC) mode.

Caution After you enable this setting, you cannot disable it. If you need to do so, contact Support for assistance.

Syntax

```
system compliance enable cc
```

Example

```
> system compliance enable cc
```

enable ucapl

Configures the device's security certifications compliance to Unified Capabilities Approved Products List (UCAPL) mode.

Caution After you enable this setting, you cannot disable it. If you need to do so, contact Support for assistance.

Syntax

```
system compliance enable ucapl
```

Example

```
> system compliance enable ucapl
```

show

Displays the device's current security certifications compliance mode.

Syntax

```
system compliance show
```

Example

```
> system compliance show
```

disable-http-user-cert

Disables the requirement that the browser present a valid client certificate.

Access

Configuration

Syntax

```
system disable-http-user-cert
```

Example

```
> system disable-http-user-cert
```

file Commands

The `system file` commands enable the user to manage the files in the common directory on the device.

Access

Configuration

copy

Uses FTP to transfer files to a remote location on the host using the login username. The local files must be located in the common directory.

Syntax

```
system file copy hostname username path filenames filenames ...
```

where `hostname` specifies the name or ip address of the target remote host, `username` specifies the name of the user on the remote host, `path` specifies the destination path on the remote host, and `filenames` specifies the local files to transfer; the file names are space-separated.

Example

```
> system file copy sfrocks jdoe /pub *
```

delete

Removes the specified files from the common directory.

Syntax

```
system file delete filenames filenames ...
```

where `filenames` specifies the files to delete; the file names are space-separated.

Example

```
> system file delete *
```

list

If no file names are specified, displays the modification time, size, and file name for all the files in the common directory. If file names are specified, displays the modification time, size, and file name for files that match the specified file names.

Syntax

```
system file list filenames
```

where *filenames* specifies the files to display; the file names are space-separated.

Example

```
> system file list
```

secure-copy

Uses SCP to transfer files to a remote location on the host using the login username. The local files must be located in the `/var/common` directory.

Syntax

```
system file secure-copy hostname username path filenames filenames ...
```

where *hostname* specifies the name or ip address of the target remote host, *username* specifies the name of the user on the remote host, *path* specifies the destination path on the remote host, and *filenames* specifies the local files to transfer; the file names are space-separated.

Example

```
> system file secure-copy 10.123.31.1 jdoe /tmp *
```

generate-troubleshoot

Generates troubleshooting data for analysis by Cisco.

Caution Generating troubleshooting files for lower-memory devices can trigger Automatic Application Bypass (AAB) when AAB is enabled, At a minimum, triggering AAB restarts the Snort process, temporarily interrupting traffic inspection. Whether traffic drops during this interruption or passes without further inspection depends on how the target device handles traffic. See Snort® Restart Traffic Behavior for more information. In some such cases, triggering AAB can render the device temporarily inoperable. If inoperability persists, contact Cisco Technical Assistance Center (TAC), who can propose a solution appropriate to your deployment. Susceptible devices include Firepower 7010, 7020, and 7030; ASA 5508-X, 5516-X , 5515-X, and 5525-X; NGIPSv.

Access

Configuration

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
```

ldapsearch

Enables the user to perform a query of the specified LDAP server. Note that all parameters are required.

Access

Configuration

Syntax

```
system ldapsearch host port baseDN userDN basefilter
```

where host specifies the LDAP server domain, port specifies the LDAP server port, baseDN specifies the DN (distinguished name) that you want to search under, userDN specifies the DN of the user who binds to the LDAP directory, and basefilter specifies the record or records you want to search for.

Example

```
> system ldapsearch ldap.example.com 389 cn=users,

dc=example,dc=com cn=user1,cn=users,dc=example,dc=com, cn=user2
```

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.

Access

Configuration

Syntax

```
system lockdown
```

Example

```
> system lockdown
```

nat rollback

Reverts the system to the previously applied NAT configuration. This command is not available on NGIPSv or ASA FirePOWER. You cannot use this command with devices in stacks or high-availability pairs.

Access

Configuration

Syntax

```
system nat rollback
```

Example

```
> system nat rollback
```

renew-http-cert

Renews the default HTTPS server certificate provided with the system, optionally with a new key. The renewed certificate is valid for three years. This command is not available on NGIPSv and ASA FirePOWER devices.

Access

Configuration

Syntax

```
system renew-http-cert [newkey]
```

Example

```
> system renew-http-cert newkey
```

reboot

Reboots the device.

Access

Configuration

Syntax

```
system reboot
```

Example

```
> system reboot
```

restart

Restarts the device application.

Access

Configuration

Syntax

```
system restart
```

Example

```
> system restart
```

support Commands

The `system support` commands enable the user to manage special SSL ClientHello processing on the device.

Access

Configuration

ssl-client-hello-display

Displays the current settings for processing the ClientHello message during an SSL handshake. For a description of these settings, see the `ssl-client-hello-enabled` and `ssl-client-hello-tuning` commands.

Access

Basic

Syntax

```
system support ssl-client-hello-display
```

Example

```
> system support ssl-client-hello-display
```

ssl-client-hello-enabled

Controls special processing of the ClientHello message during the SSL handshake.

Caution Use these commands *only* if advised to do so by Cisco TAC.

Access

Configuration

Syntax

`system support ssl-client-hello-enabled` *`setting`* `{true | false}`

Possible *setting* values are:

feature
Controls all special handling of ClientHello messages.

curves
Controls stripping of elliptic curves that the Firepower System does not support:

- `true` (enabled)—The system strips any unsupported elliptic curves from the ClientHello message, increasing the likelihood of traffic decryption. You must also enable the `extensions` setting.
- `false` (disabled)—The system retains unsupported elliptic curves in the ClientHello message, decreasing the likelihood of traffic decryption.

ciphers
Controls stripping of cipher suites that the Firepower System does not support:

- `true` (enabled)—The system strips unsupported cipher suites from ClientHello messages, increasing the likelihood of traffic decryption.
- `false` (disabled)—The system retains unsupported cipher suites in ClientHello messages. This decreases the likelihood of traffic decryption and can result in a number of `Unsupported` or `Unknown Cipher` errors in the SSL Flow Error field of associated connection events.

extensions

Controls stripping of TLS extensions that prevent decryption:

- `true` (enabled)—The system identifies TLS extensions that prevent decryption and strips them from the ClientHello message. This value is required if you want to enable **curves**, **session_ticket**, and **alpn**.
- `false` (disabled)—The system retains all TLS extensions in the ClientHello message. This decreases the likelihood of traffic decryptions and can result in `Unknown Session` errors in the SSL Flow Error field of associated connection events.

session_ticket

Controls processing of the SessionTicket extension in ClientHello messages. If the system can match a SessionTicket value in an incoming ClientHello message to cached session data, it can resume the session without the client and server performing the full SSL handshake.

- `true` (enabled)—The system strips unrecognized SessionTicket values from the ClientHello message. This increases the likelihood of traffic decryption for the resumed session. You must also enable the `extensions` setting.
- `false` (disabled)—The system retains all SessionTicket values in the ClientHello message. This decreases the likelihood of traffic decryption and can result in `Uncached Session` errors in the SSL Flow Error field of associated connection events.

session_id

Controls processing of the Session Identifier element in ClientHello messages. If the system can match the Session Identifier in an incoming ClientHello message to cached session data, it can resume the session without the client and server performing the full SSL handshake.

- `true` (enabled)—The system strips unrecognized Session Identifier values from the ClientHello message. This increases the likelihood of traffic decryption for the resumed session.
- `false` (disabled)—The system retains all Session Identifier values in the ClientHello message. This decreases the likelihood of traffic decryption and can result in `Uncached Session` errors in the SSL Flow Error field of associated connection events.

alpn

Controls stripping of ALPN protocol values that cannot be decrypted, specifically, the SPDY and HTTP2 protocols:

- `true` (enabled)—The system prevents the client from establishing SPDY or HTTP2 sessions, increasing the likelihood of traffic decryption and inspection. You must also enable the `extensions` setting.
- `false` (disabled)—The system allows the client to establish SPDY or HTTP2 sessions with the server, decreasing the likelihood of traffic decryption and inspection.

compression
Controls stripping of TLS compression requests from ClientHello messages:

- `true` (enabled)—The system prevents the client from establishing a TLS compressed session with the server.
- `false` (disabled)—The system allows the client to establish a TLS compressed session with the server. This prevents traffic decryption for the session and can result in `Compression Used` errors in the SSL Flow Error field of associated connection events.

tls13_downgrade
Determines whether or not the FTD attempts to downgrade to TLS 1.2 a server request for a TLS 1.3 connection. FTD does not currently support TLS 1.3.

- `true` (enabled)—The system attempts to downgrade a TLS 1.3 connection to TLS 1.2.
- `false` (disabled)—The system does not attempt to downgrade, resulting in a failed connection.

aggressive_tls13_downgrade
Use this command *only* if advised to do so by Cisco TAC.

Example

```
> system support ssl-client-hello-enabled feature false
```

ssl-client-hello-force-reset

Resets the configurable settings for ClientHello message processing to default values. The system does not require user confirmation before proceeding.

Caution Do **not** use this command unless you are directed to do so by Support.

Access

Configuration

Syntax

```
system support ssl-client-hello-force-reset
```

Example

```
> system support ssl-client-hello-force-reset
```

ssl-client-hello-reset

Resets the configurable settings for ClientHello message processing to default values. The system requires user confirmation before proceeding.

Caution Do **not** use this command unless you are directed to do so by Support.

Access

Configuration

Syntax

```
system support ssl-client-hello-reset
```

Example

```
> system support ssl-client-hello-reset
```

ssl-client-hello-tuning

Allows you to refine how the managed device modifies ClientHello messages during SSL handshakes. This command tunes the default lists of cipher suites, elliptic curves, and extensions that the system allows in ClientHello messages. This command only adds entries to or removes entries from the default lists of allowed values. It does not overwrite the default lists.

Caution Do **not** use this command unless you are directed to do so by Support.

Access

Configuration

Syntax

`system support ssl-client-hello-tuning` *`setting value`*

The *value* element supports a comma-delimited list of values. Possible values for the *setting* and *value* elements include:

Setting	**System Action**	***Value***
`ciphers_allow`	Allows the specified cipher suites in ClientHello messages. If you use this command, the system retains the specified cipher suites in any ClientHello messages it modifies.	Obtain individual cipher suite numbers from the IANA website: https://www.iana.org/assignments/tls-parameters/tls-parameters.xhtml#tls-parameters-4 IANA provides values in hexadecimal. Convert them to decimal for use in this command.
`ciphers_remove`	Disallows the specified cipher suites in ClientHello messages. If you use this command, the system strips the specified cipher suites from any ClientHello message it modifies.	

Setting	System Action	*Value*
`curves_allow`	Allows the specified elliptic curves in ClientHello messages. If you use this command, the system retains the specified elliptic curves in any ClientHello message it modifies.	Obtain curve numbers from the IANA website: https://www.iana.org/assignments/tls-parameters/tls-parameters.xhtml#tls-parameters-8
`curves_remove`	Disallows the specified elliptic curves in ClientHello messages. If you use this command, the system strips the specified elliptic curves from any ClientHello message it modifies.	
`extensions_allow`	Allows the specified extensions in ClientHello messages. If you use this command, the system retains the specified extensions in any ClientHello message it modifies.	Obtain extension numbers from the IANA website: https://www.iana.org/assignments/tls-extensiontype-values/tls-extensiontype-values.xhtml
`extensions_remove`	Disallows the specified elliptic curves in ClientHello messages. The system strips the specified extensions from any ClientHello message it modifies. By default, the system disallows extensions 22, 23, and 30032.	

Example

```
> system support ssl-client-hello-tuning ciphers_allow 4,7,16,22
```

shutdown

Shuts down the device. This command is not available on ASA FirePOWER modules.

Access

Configuration

Syntax

```
system shutdown
```

Example

```
> system shutdown
```

History for Classic Device CLI

Feature	Version	Details
HTTPS Certificates	6.3	The default HTTPS server certificate provided with the system now expires in three years. If your appliance uses a default certificate that was generated before you upgraded to Version 6.3, the certificate will expire 20 years from when it was first generated. If you are using the default HTTPS server certificate the system now provides the ability to renew it. New classic CLI commands: **show http-cert-expire date**, **`system renew-http-cert`** Supported platforms: Physical FMCs, 7000 and 8000 Series devices
Classic CLI command `system lockdown-sensor` syntax.	6.3	The **system lockown-sensor** command in the Classic CLI is now **system lockdown**.