Command Line Reference

This reference explains the command line interface (CLI) for FirePOWER appliances, virtual devices, and the ASA FirePOWER modules of ASA FirePOWER devices. You can use the CLI to view, configure, and troubleshoot your FireSIGHT System.

Note The command line interface is not supported on Defense Centers, Series 2 appliances, Cisco NGIPS for Blue Coat X-Series, or the ASA module of ASA FirePOWER devices.

There are numerous CLI modes, such as `show` and `configure`, that contain sets of commands beginning with the mode name. You may enter a mode and then enter valid commands within that mode, or you may enter an entire full command from any mode. For example, to display information about a user account called Analyst1, you can enter the following at the CLI prompt:

```
show user Analyst1
```

If you have previously entered `show` mode, enter the following at the CLI prompt:

```
user Analyst1
```

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 in to the shell.

On Series 3 devices, you can assign command line permissions on the User Management page in the web interface; see Managing Users, page 61-1 for more information. On virtual devices and ASA FirePOWER devices, you assign command line permissions through the CLI itself.

Note If you reboot a Series 3 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.

For information about logging into the command line, see Logging into the Appliance, page 2-1.

The following sections describe the CLI commands:

Basic CLI Commands

The basic CLI commands provide the ability to interact with the CLI. These commands do not affect the operation of the device. Basic commands are available to all CLI users.

The following sections describe the basic commands:

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:
```

end

Returns the user to the default mode. (Moves the user up to the default mode from any lower-level CLI context.)

Access

Basic

Syntax

```
end
```

Example

```
configure network ipv4> end
>
```

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>
```

help

Displays an overview of the CLI syntax.

Access

Basic

Syntax

```
help
```

Example

```
> help
```

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

```
> ?
```

?? (double question marks)

Displays detailed context-sensitive help for CLI commands and parameters.

Access

Basic

Syntax

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

Example

```
> configure manager add ??
```

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.

The following sections describe the show commands:

access-control-config

Displays the currently applied access control configurations, including: Security Intelligence settings; the name of referenced SSL, network analysis, intrusion, and file policies; intrusion variable set data; logging settings; and 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 virtual devices 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 virtual devices and ASA FirePOWER devices.

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
```

bypass

On Series 3 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, 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'
```

clustering

Displays information about device clustering configuration, status, and member stacks. This command is not available on virtual devices and ASA FirePOWER devices.

Access

Basic

config

Displays the clustering configuration on the device.

Syntax

```
show clustering config
```

Example

```
> show clustering config
```

clustering ha-statistics

Displays state sharing statistics for a device in a cluster.

Syntax

```
show clustering ha-statistics
```

Example

```
> show clustering ha-statistics
```

cpu

Displays the current CPU usage statistics appropriate for the platform for all CPUs on the device. For managed 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 virtual devices and ASA FirePOWER devices, 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 managed device, it is ignored because for that platform, utilization information can only be displayed for all processors.

Example

```
> show cpu
```

database

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
```

expert

Invokes the shell.

Access

Basic

Syntax

```
expert
```

Example

```
> expert
```

fan-status

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

Access

Basic

Syntax

```
show fan-status
```

Example

```
> show fan-status
```

fastpath-rules

Displays the currently configured fastpath rules. This command is not available on virtual devices and ASA FirePOWER 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 virtual devices and ASA FirePOWER devices.

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 Defense Center. In some cases, you may need to edit the device management settings manually. For more information, see Editing Device Management Settings, page 4-53.

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
```

hyperthreading

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

Access

Basic

Syntax

```
show hyperthreading
```

Example

```
> show hyperthreading
```

iab

Displays the current Intelligent Application Bypass (IAB) configuration. This command requires Version 5.4.0.10 or later on the managed device. The Defense Center requires Version 5.4.1.9 or later to implement IAB functionality, and Version 5.4.1.10 or later to provide IAB events.

Access

Basic

Syntax

```
show iab
```

Example

```
> show iab
IAB configuration:
Performance Sample Interval      5 seconds
Bytes per Flow                   500000 kbytes
Flow Velocity                    25000 kbytes/second
Drop Percentage                  1%
Processor Utilization Percentage 95%
Packet Latency                   250 microseconds
```

inline-sets

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

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 virtual devices and ASA FirePOWER devices.

Access

Basic

Syntax

```
show lcd
```

Example

```
> show lcd
```

link-aggregation

The `show link-aggregation` commands display configuration and statistics information for link aggregation groups (LAGs). This command is not available on virtual devices 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, 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 Defense Center. Registration key and NAT ID are only displayed if registration is pending. If a device is registered to a high availability pair, information about both managing Defense Centers is displayed. If a device is configured as a secondary device in a stacked configuration, information about both the managing Defense Center 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 virtual devices and ASA FirePOWER devices.

Access

Basic

Syntax

```
show mpls-depth
```

Example

```
> show mpls-depth
```

NAT

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

Example

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

where *allocator_id* is a valid allocator ID number.

flows

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

Syntax

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

Example

```
> show nat flows 81
```

where *allocator_id* is a valid allocator ID number.

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 virtual devices and ASA FirePOWER devices.

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 virtual devices and ASA FirePOWER devices.

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 virtual devices and ASA FirePOWER devices.

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 virtual devices and ASA FirePOWER devices.

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 virtual devices.

Access

Basic

Syntax

```
show serial-number
```

Example

```
> show serial-number
```

ssl-policy-config

Displays the currently applied 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 clustered stacks, this command also indicates that the stack is a member of a cluster. 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 virtual devices and ASA FirePOWER devices.

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, page D-26, interfaces, page D-14, device-settings, page D-10, and access-control-config, page D-6.

Access

Basic

Syntax

```
show summary
```

Example

```
> show summary
```

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 devices, and the system displays only the data plane interfaces.

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 virtual devices 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 virtual devices 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.

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 virtual devices and ASA FirePOWER devices.

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 virtual devices and ASA FirePOWER devices.

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 virtual devices.

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
- snapshot
- 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

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

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.

The following sections describe the configuration commands:

clustering

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

Access

Configuration

Syntax

```
configure clustering {disable | bypass}
```

Example

```
> configure clustering disable
```

bypass

On Series 3 devices, places an inline pair in fail-open (hardware bypass) or fail-close mode. You can use this command only when the **Bypass Mode** inline set option is set to **Bypass**.

Caution You cannot apply an access control policy or reapply an intrusion policy to a managed device where this command has put an inline set into fail-open mode.

Note that rebooting a device takes an interface pair out of fail-open made.

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
```

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 virtual devices and ASA FirePOWER devices.

Access

Configuration

Syntax

```
configure gui {enable | disable}
```

Example

```
> configure gui disable
```

iab

Configure Intelligent Application Bypass (IAB). This command requires Version 5.4.0.10 or later on the managed device. The Defense Center requires Version 5.4.1.9 or later to implement IAB functionality, and Version 5.4.1.10 or later to provide IAB events.

IAB trusts traffic to traverse your network without further inspection if performance and flow thresholds are exceeded. The system implements IAB on traffic allowed by access control rules or the access control policy's default action, before the traffic is subject to deep inspection. A test mode allows you to determine whether thresholds are exceeded and, if so, to identify the flows that would have been trusted if you had actually enabled IAB. You must deploy your access control policy to the managed device after configuring IAB.

Table D-1 Basic IAB Parameters

Parameter	Description
on	Configures IAB in active mode.
test	Configures IAB in test mode.
disable	Disables IAB.

Performance and Flow Thresholds

You must set a performance scan interval and configure at least one of four inspection performance thresholds and one of four flow bypass thresholds. When a performance threshold is exceeded, the system examines flow thresholds and, if a flow threshold is exceeded, trusts traffic. If you configure more than one of either type of threshold, only one of each must be exceeded. All thresholds are disabled (set to 0) by default.

Inspection performance thresholds—provide intrusion inspection performance limits that, if exceeded, trigger the inspection of flow thresholds. IAB does not use inspection performance thresholds set to 0.

Table D-2 Inspection Performance Threshold Parameters

Parameter	Descriptive Name	Description	Range
interval	Performance Sample Interval	The time between IAB performance sampling scans, during which the system collects system performance metrics for comparison to IAB performance thresholds.	1 - 1000 seconds
drops	Drop Percentage	Average packets dropped as a percentage of total packets, when packets are dropped because of performance overloads caused by expensive intrusion rules, file policies, decompression, and so on. This does not refer to packets dropped by normal configurations such as intrusion rules. Note that specifying an integer greater than 1 activates IAB when the specified percentage of packets is dropped. When you specify 1, any percentage from 0 through 1 activates IAB. This allows a small number of packets to activate IAB.	0 - 100 percent
cpu	Processor Utilization Percentage	Average percentage of processor resources used.	0 - 100 percent
latency	Packet Latency	Average packet latency.	0 - 1000000 microseconds
rate	Flow Rate	The rate at which the system processes flows, measured as the number of flows per second. Note that this option configures IAB to measure flow *rate*, not flow *count*.	0 - 1000000 flows/second

Flow bypass thresholds—provide flow limits that, if exceeded, trigger IAB to trust traffic in active mode or allow traffic subject to further inspection in test mode. IAB does not use flow bypass thresholds set to 0.

Table D-3 Flow Bypass Threshold Parameters

Parameter	Descriptive Name	Description	Range
kbytes	Bytes per Flow	The maximum number of kilobytes a flow can include.	0 - 2147483647 kilobytes
packets	Packets per Flow	The maximum number of packets a flow can include.	0 - 2147483647 packets
duration	Flow Duration	The maximum number of seconds a flow can remain open.	0 - 2147483647 seconds
velocity	Flow Velocity	The maximum transfer rate in kilobytes per second.	0 - 2147483647 kilobytes/second

You configure all parameters at the same time and in order. The system prompts you for the next parameter if you enter fewer than the maximum number of parameters.

Access

Configuration

Syntax

```
configure iab {on | test} interval drops cpu latency rate kbytes packets duration velocity
```

Example

```
configure iab on 5 1 95 250 0 500000 0 0 25000
```

Related Command

```
show iab
```

lcd

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

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

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

Access

Configuration

add

Configures the device to accept a connection from a managing Defense 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 Defense Center. In most cases, you must provide the hostname or the IP address along with the registration key. However, if the device and the Defense 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 Defense Center that manages this device. If the Defense 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 Defense Center. *`nat_id`* is an optional alphanumeric string used during the registration process between the Defense Center and the device. It is required if the hostname is set to `DONTRESOLVE`.

Example

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

delete

Removes the Defense 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 virtual devices and ASA FirePOWER devices.

Access

Configuration

Syntax

```
configure mpls-depth {depth}
```

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

Example

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

network

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 Series 3 and virtual 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 a virtual device to configure an HTTP proxy server so the virtual device can submit files to the Collective Security Intelligence Cloud for dynamic analysis.

Syntax

```
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 Series 3 and virtual 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
```

Example

```
> configure network ipv4 delete
```

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
```

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
```

where *ipaddr* is the IP address, *netmask* is the subnet mask, and *gw* is the IPv4 address of the default gateway.

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
```

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
```

Example

```
> configure network ipv6 dhcp
```

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
```

Example

```
> configure network ipv6 router
```

ipv6 manual

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

Syntax

configure network ipv6 manual *ip6addr*/ip6*prefix* [ip6*gw*]

where *ip6addr/ip6prefix* is the IP address and prefix length and ip6*gw* is the IPv6 address of the default gateway.

Example

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

management-interface disable

Disables the specified management interface.

Syntax

configure network management-interface disable *ethn*

where *n* is the number of the management interface you want to disable.

Example

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

management-interface disable-event-channel

Disables event transmission over the specified management interface.

Syntax

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

where *n* is the number of the management interface you want to disable.

Example

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

management-interface disable-management-channel

Disables management transmission over the specified management interface.

Syntax

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

where *n* is the number of the management interface you want to disable.

Example

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

management-interface enable

Enables the specified management interface.

Syntax

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

where *n* is the number of the management interface you want to enable.

Example

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

management-interface enable-event-channel

Enables event transmission over the specified management interface.

Syntax

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

where *n* is the number of the management interface you want to enable.

Example

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

management-interface enable-management-channel

Enables management transmission over the specified management interface.

Syntax

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

where *n* is the number of the management interface you want to enable.

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 managed 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 virtual devices or ASA FirePOWER devices and you cannot use it to break a clustered stack.

Use this command when you cannot establish communication with appliances higher in the stacking hierarchy. If the Defense Center is available for communication, a message appears instructing you to use the Defense 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

Applicable only to virtual devices, 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]
```

Example

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

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

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
```

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 a virtual device. This command is available only on virtual devices.

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
- snapshot
- 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
```

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.

The following sections describe the system commands:

access-control

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

Access

Configuration

archive

Saves the currently applied 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 applied access control configuration. You cannot use this command with clustered or stacked devices.

Syntax

```
system access-control rollback
```

Example

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

disable-http-user-cert

Removes all HTTP user certification present on the system.

Access

Configuration

Syntax

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

Example

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

file

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 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.

Access

Configuration

Syntax

```
system generate-troubleshoot
```

This syntax displays a list of optional parameters to specify what troubleshooting data should be displayed.

Example

```
> system generate-troubleshoot
```

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-sensor

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

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

Access

Configuration

Syntax

```
system lockdown-sensor
```

Example

```
> system lockdown-sensor
```

nat rollback

Reverts the system to the previously applied NAT configuration. This command is not available on virtual devices and ASA FirePOWER devices. You cannot use this command with clustered or stacked devices.

Access

Configuration

Syntax

```
system nat rollback
```

Example

```
> system nat rollback
```

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
```

shutdown

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

Access

Configuration

Syntax

```
system shutdown
```

Example

```
> system shutdown
```