



# TippingPoint™ Threat Protection System (TPS)

Command Line Interface Reference

## Privacy and Personal Data Collection Disclosure

Certain features available in Trend Micro products collect and send feedback regarding product usage and detection information to Trend Micro. Some of this data is considered personal in certain jurisdictions and under certain regulations. If you do not want Trend Micro to collect personal data, you must ensure that you disable the related features.

The following link outlines the types of data that the Security Management System collects and provides detailed instructions on how to disable the specific features that feedback the information.

<https://success.trendmicro.com/data-collection-disclosure>

Data collected by Trend Micro is subject to the conditions stated in the Trend Micro Privacy Policy:

[https://www.trendmicro.com/en\\_us/about/legal/privacy-policy-product.html](https://www.trendmicro.com/en_us/about/legal/privacy-policy-product.html)

## Legal Notice

© Copyright 2018 Trend Micro Incorporated. All rights reserved.

Trend Micro, the Trend Micro t-ball logo, TippingPoint, and Digital Vaccine are trademarks or registered trademarks of Trend Micro Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.

Publication: July 2018

# Command Line Interface

In addition to the Local System Manager (LSM) and the centralized management capability of the Security Management System (SMS), you can use the Command-line Interface (CLI) to configure and manage your device.

When you initially install the device and run the Setup Wizard, you create a superuser account that you will use to access the device through the LSM or the CLI. By default, SSH and HTTPS are enabled on the device for the management port IP address. You can access the CLI directly through the system console or remotely through SSH. Non-secure connections, such as Telnet, are not permitted.



## Note

When there has been no CLI activity for 15 minutes, connection to the device times out.

Your access to the CLI is determined by your group membership and roles and capabilities. To configure granular levels of access, you can use the `aaa` (Authentication and Authorization and Auditing) context to modify users, groups, roles, and their capabilities.

## CLI syntax

The CLI uses the following syntax:

SYNTAX CONVENTION	EXPLANATION
UPPERCASE	Uppercase represents a user-supplied value.
(x)	Parentheses indicate a required argument.
[x]	Brackets indicate an optional argument.
	A vertical bar indicates a logical OR among required and optional arguments.

## Examples

The question mark displays help information:

```
ips{}traceroute ?
```

In the example below, required arguments for the `traceroute` command must either use an IP address or the hostname. An optional argument can be “from” a source IP address:

```
ips{}traceroute 198.162.0.1 from 198.162.0.2
```

## Shortcut navigation keys

The CLI has the ability to store typed commands in a circular memory. Typed commands can be recalled with the UP and DOWN arrow keys.

You can use the TAB key to complete partial commands. If the partial command is ambiguous, pressing the TAB key twice gives a list of possible commands.

SHORTCUT	DESCRIPTION
ENTER	Runs the command.
TAB	Completes a partial command.

SHORTCUT	DESCRIPTION
?	Question mark at the root prompt or after a command (separated by space) lists the next valid sub-commands or command arguments. Question mark can also be used after sub-commands for more information.  A question mark immediately following a character(s) (no space) will list commands beginning with those characters.
!	Exclamation mark before a command allows you to execute the command from any feature context or sub-level. Example: <code>ips{running-gen}!ping 203.0.113.0</code>
UP ARROW	Shows the previous command.
DOWN ARROW	Shows the next command.
Ctrl + P	Shows the previous command.
Ctrl + N	Shows the next command.
Ctrl + L	Clears the screen, does not clear history.
Ctrl + A	Returns to the start of the command you are typing.
Ctrl + E	Goes to the end of the command you are typing.
Ctrl + U	Cuts the whole line to a special clipboard.
Ctrl + K	Cuts everything after the cursor to a special clipboard.
Ctrl + Y	Pastes from the special clipboard used by Ctrl + U and Ctrl + K.

## Hierarchical context

Prompts are displayed based in a hierarchical context. The following table shows the root, edit, and log configuration modes.

PROMPT	DESCRIPTION
<code>ips{}</code>	Displays the top-level root mode. This context is displayed when you first log in to the CLI.
<code>ips{ }edit</code>	Enters the edit configuration mode.
<code>ips{running}</code>	Displays the configuration mode by changing the prompt to running. This indicates you will be making changes to the running configuration.
<code>ips{running}display</code>	Views the current configuration and any changes.
<code>ips{running}commit</code>	Commits changes to the running configuration.
<code>ips{ }log-configure</code>	Enters the log-configure context to access the log configuration mode.
<code>ips{log-configure}</code>	Displays the log configuration mode.
<code>ips{log-configure}help</code>	Displays list of valid commands and syntax usage .
<code>ips{running}exit</code>	Leaves the current configuration mode.
<code>ips{running}!</code>	Leaves the configuration mode from any context and returns to the top-level root mode.

## Help

The `help` command provides a list of commands within the current context and the command line usage. You can run issue the `help` command with or without an argument.

COMMAND	DESCRIPTION
<code>help</code> or <code>?</code>	Displays a list of all commands. (The question mark at any context level generates a list of available commands within the context, along with a brief description).
<code>help commandname</code>	Displays syntax for a command.
<code>commandname?</code>	Displays the options for a command. For example, <code>ping ?</code> .
<code>string?</code>	Shows the commands or keywords that match the string. For example, <code>s?</code> .

## Command modes

The TPS uses a hierarchical menu structure. Within this structure, commands are grouped by functional area within one of three command modes:

COMMAND MODE	DESCRIPTION/EXAMPLE
Root	When you first log in to the device, you enter the top of the hierarchy, the root mode. <code>ips{}</code>
Edit	Enters the edit mode. <code>ips{running}</code>
Log Configuration	Enters the log configuration mode. <code>ips{log-configure}</code>

A *context* is an environment in which you can configure a set of parameters for a feature or named object. A context can be the name of an instance of an object set by the administrator, or can be the feature itself. The current context is indicated in the command prompt, as shown in the examples above.

Your user role determines whether you have access to all contexts or only specific contexts. Authorization is controlled by granting users access through the authentication context (`aaa`).

The `help` and `display` commands are useful in becoming familiar with the context options. The question mark (?) lists the next valid entry and help for this entry.

If the device is managed by SMS, you will have read-only access to the system resources. To determine if an SMS controls the device, or to change the control, see the `sms` command.

## Root command mode

When you initially enter your device, either through the console or SSH, you enter at the root command mode. The system displays the `ips{}` prompt as a default. The commands available at this level manage and monitor system operations for the various subsystems.

From the root command mode you can access the configuration mode and the available operational commands that apply to the unit as a whole.

To view the commands available at the root level, type:

```
ips{}help
```

To change the default `ips {` command prompt, use the `host name` command in the `interface mgmt` context of the edit mode. For example:

```
ips{}edit
ips{running}interface mgmt
ips{running-mgmt}help host
```

This displays valid entries for configuring management port host settings.

To display valid entries for the `host` command, type:

```
ips{running-mgmt}host ?
```

To change the host name, type:

```
ips{running-mgmt}host name <yourhostname>
```

For a list of root commands and their usage see [Root commands](#).

## Edit configuration mode

The configuration mode enables administrators with the appropriate credentials to write configuration changes to the active (running) configuration. To edit the device configuration, you must either be associated with the Superuser role or the Administrator role.

This mode has different context levels that provide access to a specific set of configuration commands. As you move through the context menus the command prompt displays the current context. Remember that you can issue the `help` command to display available commands for that context or type `display` to view the current configuration for that context.

### Enter and exit the edit mode

To enter the edit configuration mode, use the `edit` command.

```
ips{}edit
ips{running}
```

The CLI prompt indicates that you are in the edit mode and you can then make configuration changes. Configuration options, and sub contexts are available for use until you exit this mode.

To exit the current context, use the `exit` command.

```
ips{running}exit
```

To exit the edit configuration mode from the top-level `ips{running}` prompt, use the `exit` command.

```
ips{running}exit
```

To exit the edit configuration mode from any context, use the `!` command.

```
ips{running}!
```

When you exit the edit configuration mode, the following warning is displayed: "WARNING: Modifications will be lost. Are you sure to exit (y/n)? [n]"

`y` discards any uncommitted changes you made to the configuration file. `n` keeps you in the edit configuration mode.

### View and commit configuration changes

The `display` command is a helpful utility to view the current running configuration and to review your configuration changes before you save them.

```
ips{running} display
```

You must use the `commit` command to save your changes to the running configuration.

## Container and object statements

The command hierarchy has two types of statements. The container statement, which contain objects, and the object statement, which are actual commands with options.

For example:

- Container statement in edit mode:

```
ips{running}log
```

```
ips{running-log}? (The question mark will list all the available entries.)
```

- Object statement:

```
ips{running}
```

```
application-visibility enable|disable (Help will display the command options.)
```

## Edit mode workflow

A brief overview of what you can do within the edit configuration mode:

- Issue a command that configures a setting in the *candidate configuration* setting. The candidate configuration allows you to make configuration changes without causing changes to the active configuration until you can review your changes and issue the `commit` command.
- Enter into a container context to access additional configuration settings.
- Run the `display` command to see your candidate configuration settings for that particular context. Any modifications you made will also be visible.
- Run the `commit` command to save any changes from your candidate configuration to the running configuration.
- Run the `exit` command to leave the current context. If you are in the top-level root **ips{}** context, this command leaves the configuration mode.
- Run the `!` command to leave the configuration mode from the current context.

## Configuration file versions

When troubleshooting or needing to rollback a configuration, the current configuration setup can be viewed. Reviewing network configuration files should be a necessary step to becoming knowledgeable about your current system setup. When the device is initially configured, make sure the settings are saved to the *persistent* configuration with the `ips{}save-config` command. It is also advisable to create a snapshot using the following command:

```
ips{}snapshot create orig_conf
```

Snapshots capture the configuration of a device, which can then be delivered to technical support for troubleshooting. Users can also use snapshots to save and re-apply configurations. Snapshots include the currently installed OS version, and cannot be restored on a device that is not running the same version of the OS. If a snapshot restore needs to be completed, use the following command:

```
ips{}snapshot restore orig_conf
```

A warning message is displayed, followed by an automatic reboot when snapshot restore is completed.

The CLI uses the *deferred-commit* model. In this capacity, the architecture maintains a set of configuration files to ensure that a working configuration is persistently maintained. This configuration set includes the following configuration files.

- *Running* configuration — This version is currently executing on the system. Any changes that administrators make from the edit mode (*except for IPS features, action sets, application groups, and notification contacts*) will take effect once they have been committed, by issuing the `commit` command. If changes are not committed, all modifications are discarded on `exit` from the running context. If multiple administrators are on the system, the version that was last committed is used as the current running configuration and is visible to other administrators, once they have exited the edit mode. A warning prompt is displayed if the committed changes would overwrite configuration that was made by another administrator since the configuration was edited.
- *Saved (persistent)* configuration — This is the running configuration that was last committed prior to executing the `save-config` command. The device copies the saved configuration to the start configuration when the system reboots.
- *Start* configuration — This is a backup copy of the configuration file saved at the time of system startup, and is loaded at the next system bootup. The `rollback-config` command can be used to rollback to a persistent and running configuration that was the last known good configuration.

**Note**

Future versions of the product will support multiple named saved configuration sets.

---

## Utilities

The `display` and `show` commands are helpful for troubleshooting and monitoring the operational status of the system. Command line usage can be found in [Root commands](#).

### Display

Enter `display` to see your candidate configuration settings for a context. Any modifications you make can be viewed using the `display` command. The output of the `display` command depends on where the command is executed. If executed at the configuration level, it displays the entire configuration of the unit. Executing the `display` command with a configuration name parameter, or from within a context displays the contents of that particular configuration.

### Show

The `show` command is most efficient in providing critical information, such as traffic usage, router platform type, operating system revision, amount of memory, and the number of interfaces. The `show` command can also be used to evaluate logging, troubleshooting, tracking resources, sessions, and security settings. To view all the available `show` utilities, enter the `help show` command at the root command level. All the available commands along with the correct command line usage are displayed.

## Global commands

Global commands can be used in any context.

### cls

Clears the terminal screen.

```
cls
```



## commit

Commits your pending configuration changes to the Running configuration.

When you commit configuration changes, or when changes are committed automatically, the changes are committed to the Running configuration, and the changes are visible to all users. However, when the device reboots, the Running configuration is reset to the Startup configuration. Uncommitted changes and committed changes in the Running configuration are lost.



### Tip

To copy the Running configuration to the Startup configuration without exiting the configuration mode, prepend the **save-config** command with an exclamation mark (!), for example **!save-config**. This command does not commit any pending changes to the Running configuration.

### Syntax

#### **commit**

To commit your pending changes to the Running configuration, and then copy the Running configuration to the Startup configuration, enter the following commands:

```
ips{running}commit
```

```
ips{running}!save-config
```

### Related commands

COMMAND	DESCRIPTION
<a href="#">save-config</a>	Copy the Running configuration to the Startup configuration.

## display

Displays the current configuration, or the candidate configuration before a commit is issued. Display options vary by context, enter the `help display` command in a context to view the available options.

### Syntax

```
display
```

```
display [xml]
```

## edit

The edit context modifies the configuration that identifies the security policy and interfaces that you can configure for your device.

Edit takes an instance of the running configuration file. This instance is your version. After making modifications to this candidate configuration version, you have the option of saving it to the running configuration, or discarding any changes you made. To discard, simply `exit`. To save your candidates configuration, enter the `commit` command before exiting the edit context. To see commands under the edit context, see [Edit configuration mode](#).

```
ips{}
```

```
ips{ }edit
```

```
ips{running}
```

Valid entries at this position are:

aaa	Configure users, roles, and remote authentication
actionsets	Enter action sets context
autodv	Enter autodv context
blockedStreams	Enter blockedStreams context
certificates	Enter certificates context
debug	Enter debug context
delete	Delete file or configuration item
display	Display file or configuration item
dns	Enter DNS context
exit	Exit edit context, see also save-config
gen	Timezone, ssh/https access, ip-to-hostname association
help	Display help information
high-availability	Enter high-availability context
interface	Enter interface context
ips	Enter IPS profile context
log	Enter log context
notifycontacts	Enter notify contacts context
ntp	Enter NTP context
reputation	Enter Reputation context
security-policy-reset	Reset IPS security policy to default values
segments	Segments context
services	Enter services context
sflow	sFlow context
snmp	Enter SNMP context
traffic-management	Enter traffic-management profile context
virtual-segments	Enter virtual-segments context
vlan-translations	Enter vlan-translations context

```
ips{running}commit
```

```
ips{running}exit
```

```
ips{}
```

**Note**

Use debug commands only when you are instructed to do so by TippingPoint product support.

## help

Displays help information.

Syntax

```
help [full|COMMAND]
```

## Root commands

The top level root command line mode displays the `ips{}` prompt. Commands at this level are used for managing and monitoring system operations for the various subsystems. From the root command mode, you can access the configuration mode, and the available commands that apply to the device as a whole. Enter **help full** or **help COMMANDNAME** at the command prompt to display a list of available commands or help on a specific command.

```
ips{}help
```

The default `ips{}` command prompt can be changed using the **host name** command in the **interface mgmt** context of the edit mode. For example:

```
ips{}edit
```

```
ips{running}interface mgmt
ips{running-mgmt}help host (displays valid entries for configuring management port host settings)
ips{running-mgmt}host ? (displays valid entries for host command)
ips{running-mgmt}host name yourhostname
```

**Note**

Use debug commands only when you are instructed to do so by TippingPoint product support.

---

## boot

Lists software packages and rollback to a previous version.

Syntax

```
boot (list-image|rollback)
```

## chpasswd

Enter this command to change the password for your local user account, or for another local user. To change the password for another user, you must be associated with the SuperUser role.

You can use this command when the device is managed by the SMS, or is unmanaged.

Syntax

```
chpasswd user_name
```

## clear

Clears system stats, logs, locked users, adaptive filter configurations (AFCs), or packet traces.

Syntax

```
clear adaptive-filter all
clear connection-table (blocks|trusts)
clear log-file (audit|fwAlert|fwBlock|ipsAlert|ipsBlock|quarantine|reputationAlert|
reputationBlock|system)
clear np engine filter
clear np engine packet
clear np engine parse
clear np engine reputation dns
clear np engine reputation ip
clear np engine rule
clear np reassembly ip
clear np reassembly tcp
clear np rule-stats
```

```
clear np softlinx
clear np tier-stats
clear counter policy
clear rate-limit streams
clear users all [locked|ip-locked]
clear users (NAME|A.B.C.D|X:X::X:X) [locked]
```

## date

Used alone to display the current date, or with arguments to configure the date in a 24-hour format. The date command shows the current time in the time zone configured on the device and the "gmt" argument shows the time in GMT (UTC).

Syntax

```
date [MMDDhhmm[[CC]YY][.ss]])
```

```
date gmt
```

## delete

Deletes various items.

Syntax

```
delete
```

Valid entries at this position are:

```
delete auxdv <auxdv name>
delete dv-toolkit
delete sms must-be-ip
delete traffic-file FILENAME
```

## delete auxdv

Delete Aux DV.

Syntax

```
delete auxdv <auxdv name>
```

## display conf

Displays information on a particular configuration file in either the start configuration or the running configuration.

Syntax

```
display conf start|running conf-name
```

Enter the **display conf** command and press the Tab key twice to display a list of available configuration files.

```
ips{}display conf running
aaa                actionsets      autodv             certificates
dns                gen              highavailability   inspection-bypass
interface          ips              log                notifycontacts
ntp                reputation        segment1           segment2
```

```
segment3      segment4      segment5      segment6
segment7      segment8      snmp          ssl-inspection
traffic-management virtual-segments vlan-translations debug
```

Displays SSL configuration.

```
ips{}display conf running ssl-inspection
```

## display-config

Displays information on the configuration specified (either the start configuration or the running configuration).

Syntax

```
display-config (start|running)
```

## edit

The edit context modifies the configuration that identifies the security policy and interfaces that you can configure for your device.

Edit takes an instance of the running configuration file. This instance is your version. After making modifications to this candidate configuration version, you have the option of saving it to the running configuration, or discarding any changes you made. To discard, simply exit. To save your candidates configuration, enter the commit command before exiting the edit context. To see commands under the edit context, see [Edit configuration mode](#).

```
ips{}
```

```
ips{}edit
```

```
ips{running}
```

Valid entries at this position are:

aaa	Configure users, roles, and remote authentication
actionsets	Enter action sets context
autodv	Enter autodv context
blockedStreams	Enter blockedStreams context
certificates	Enter certificates context
debug	Enter debug context
delete	Delete file or configuration item
display	Display file or configuration item
dns	Enter DNS context
exit	Exit edit context, see also save-config
gen	Timezone, ssh/https access, ip-to-hostname association
help	Display help information
high-availability	Enter high-availability context
interface	Enter interface context
ips	Enter IPS profile context
log	Enter log context
notifycontacts	Enter notify contacts context
ntp	Enter NTP context
reputation	Enter Reputation context
security-policy-reset	Reset IPS security policy to default values
segments	Segments context
services	Enter services context
sflow	sFlow context
snmp	Enter SNMP context
traffic-management	Enter traffic-management profile context

<code>virtual-segments</code>	Enter virtual-segments context
<code>vlan-translations</code>	Enter vlan-translations context

```
ips{running}commit
```

```
ips{running}exit
```

```
ips{}
```

**Note**

Use debug commands only when you are instructed to do so by TippingPoint product support.

---

## fips-mode-enable

Enables the Federal Information Processing Standard (FIPS) on a TPS device.

Before you run this command, always reset the device to factory default settings.

When you run this command, it prompts you to confirm that you want to enable FIPS mode. After you enable FIPS mode, it cannot be disabled except by resetting the device to factory defaults.

**Note**

Both RADIUS and TACACS+ authentication use protocols that are not FIPS-compliant. Do not enable FIPS mode if you have remote authentication configured.

---

After you run this command, you must reboot the device to enable FIPS mode. Use the **show fips-mode** command to verify FIPS mode is enabled.

Syntax

```
fips-mode-enable
```

## halt

Enter the `halt` command to shut down the TippingPoint operating system and halt the CPU while maintaining power to the device. After you run this command, the device still has power so Layer-2 Fallback (L2FB) enables traffic to pass through the device:

- For the 440T, power can be removed by unplugging the unit or by turning off the power switch on the back of the unit. To restart the 440T, wait at least 60 seconds before you re-apply power.
- For the 2200T, power can be removed by holding down the front panel power button for 5 seconds, and can be restored by pressing the power button.

Syntax

```
halt
```

## high-availability

Use the **high-availability** context to manage Intrinsic Network High Availability (INHA) and Zero-Power High Availability (ZPHA).

- *INHA* determines how the device manages traffic on each segment in the event of a system failure:

- *Layer-2 Fallback (L2FB)* – Either permits or blocks all traffic on each segment, depending on the INHA L2FB action setting for the segment. Any permitted traffic is not inspected.

**Important**

If you enable INHA L2FB, L2FB **not** persist when you reboot the device.

- *Normal* – Permits and inspects traffic across all segments.
- *ZPHA* determines how the device routes traffic in the event of a loss of system power:
  - *Bypass* – Bypasses traffic at the port level to maintain high availability of any network segments that have ZPHA support. When ZPHA bypass is enabled, the INHA Layer-2 fallback action setting for each segment is ignored.

**Important**

If you enable ZPHA bypass, bypass persists when you reboot the device.

- *Normal* – Routes traffic from each network segment to the Threat Suppression Engine (TSE) for inspection.

ZPHA support varies by device:

- On a TippingPoint TX Series device, optional bypass I/O modules provide high availability for copper and fiber segments. You can enable bypass mode on a particular slot or all slots with a bypass I/O module. When you configure a TX Series device, use the **slot** parameter to specify a particular I/O slot or the **all** parameter to specify all slots.
- On a TippingPoint 2200T security device, ZPHA support is built-in for copper segments. An external ZPHA module is required to enable ZPHA on SFP and SFP+ segments. Bypass mode can be enabled on all segments of the device only.
- On a TippingPoint 440T security device, ZPHA support is built-in for copper segments only. Bypass mode can be enabled on all segments of the device only. You do not need to specify the **all** parameter to enable ZPHA bypass on a TPS 440T or 2200T security device
- On a TippingPoint Virtual Threat Protection System (vTPS) security device, ZPHA bypass mode cannot be enabled.

**Syntax**

Enables INHA L2FB.

```
high-availability force (fallback|normal)
```

Enables ZPHA bypass.

```
high-availability zero-power (bypass|normal) (slot|all)
```

**keystore**

Changes the keystore mode to enable private keys to be secured in the device keystore or the SMS. This command automatically clears the contents of the keystore. If the device is managed by the SMS, first unmanage the device, then use this command to persist private keys on the device.

Only use this command when **absolutely necessary**, such as when the device has lost contact with the SMS, or other similar troubleshooting situations. Under normal conditions, this setting should only be changed by using the SMS.

Change the keystore mode, for example, if the SMS is unreachable and you want the device to persist its own private keys. Use the **sms-unmanage** command to unmanage the device, and then use the **keystore on-device** command to change the keystore mode to the local keystore. After you change the keystore mode, use the **save-config** command to copy the

running configuration (which includes the private keys in the Running configuration) to the Start configuration. If the private keys are not in the running configuration, for example, because you rebooted the device after you unmanaged it, use the **private-key** command to import the private keys manually.

**Note**

When the keystore mode is **sms-managed**, private keys are not persisted in the device keystore.

Syntax

```
keystore on-device|sms-managed
```

**Related commands**

COMMAND	DESCRIPTION
<i>ips{running-certificates}private-key</i>	Import the private key from your web server into the local keystore on the device.
<i>ips{running-certificates}certificate</i>	Import the certificate from your web server into the local keystore on the device.
<i>ips{running-sslinsp}server</i>	Add an SSL server to the device with the same security settings as your web server, and assign the corresponding certificate and private key.

**list**

Displays traffic capture file list.

Syntax

```
list traffic-file
```

**log-configure**

Enters log configuration context.

Syntax

```
log-configure
```

**logout**

Logs you out of the system.

Syntax

```
logout
```

**master-key**

You can set the master key to a device-generated key that is unique to the device or specify your own *master key passphrase*. By default, TOS v5.0.0 and later encrypts the system keystore with a device-generated master key.

(Best Practice) To avoid keystore issues with a TOS rollback, set the master key to a passphrase that you specify. If the keystore in the rollback image is secured with a different master key than the master key that is set on the device, you can set the master key to the correct passphrase. For more information, see the *Local Security Manager User Guide*.



Before you change the master key, keep in mind the following points:

- By default, the external user disk is not encrypted. You can easily access the contents of the external user disk from a different device.
- If you choose to encrypt the external user disk, the master key encrypts and decrypts the external user disk.
  - If you change the master key while the external user disk is encrypted, all traffic logs, snapshots, ThreatDV URL Reputation Feed, User-defined URL Entries database, and packet capture data are erased from the external user disk.
  - To access the contents of an encrypted external user disk from a different device, for example to restore a snapshot, the same master key must also be set on the device.



#### Note

For security purposes, these commands require you to re-enter your password. If you incorrectly enter your password too many times, you are temporarily locked out for two minutes. To verify your account lock status, enter the `show user locked` command.

Enter an option to set the master key:

- `passphrase` – This option allows you to specify a passphrase for the master key.

The passphrase must meet the following complexity requirements:

- Must be between 9 and 32 characters in length
- Combination of uppercase and lowercase alpha and numbers
- Must contain at least one special character (!@#\$%)
- `device-generated-key` – This option generates a passphrase for the master key.

Syntax

```
master-key (set [device-generated-key|passphrase] |reset-keystore)
```

## ping

Tests connectivity with ICMP traffic. The `mgmt` option uses the management interface.

Syntax

```
ping (A.B.C.D|HOSTNAME) [count INT] [maxhop INT] [from A.B.C.D] [datasize INT]
```

```
ping (A.B.C.D|HOSTNAME) [count (1-900000)] [maxhop (1-800)] [from A.B.C.D] [datasize (64-65468)]
```

```
ping6 (X:X::X:X|HOSTNAME) [count INT] [maxhop INT] [from X:X::X:X] [datasize INT]
```

```
ping6 (X:X::X:X|HOSTNAME) [count (1-900000)] [maxhop (1-800)] [from X:X::X:X] [datasize (64-65468)]
```

## ping6

Tests connectivity with ICMPv6 traffic.

Syntax

```
ping6 (X:X::X:X|HOSTNAME) [count (1-900000)] [maxhop (1-800)] [from X:X::X:X] [datasize (64-65468)]
```

## quarantine

Manages the quarantined traffic and IP address. Enables you to see and clear a quarantine list, and add or remove quarantined IP addresses.

Syntax

```
quarantine add <IP> <Actionset>
```

```
quarantine remove <IP>
```

```
quarantine empty
```

```
quarantine list
```

### Related commands

*show quarantine-list*

## reboot

Reboots the system. On a TPS device, this command puts the device in Intrinsic HA Layer-2 Fallback mode until the TOS completes its boot sequence. On a vTPS device, traffic flow is interrupted until the boot sequence completes because, unlike a TPS device, the network ports on the vTPS device are virtual.

Specify a full system restart with the `full` option. On a TPS device, this command temporarily removes power from the device which puts the device in ZPHA Bypass mode until the TOS completes its boot sequence. On a vTPS device, traffic flow is interrupted until the boot sequence completes because, unlike the TPS device, the network ports on the vTPS device are virtual. Syntax

```
reboot [full]
```

## reports

Configure data collection for on-box reports.

Syntax

```
reports (reset|enable|disable) [all|cpu|disk|fan|memory|network|rate-limiter|temperature|  
traffic-profile|vpn]
```

Valid entries:	
reset	Delete report data
enable	Start data collection for reports
disable	Stop data collection for reports

### Related commands

*show reports*

## resize

Resizes the terminal.

Syntax

```
resize
```

## save-config

Copies the Running configuration to the Startup configuration. When you reboot the device, the Startup configuration is applied to the device.



### Note

To run this command, you must be at the top-level root **ips{ }** mode. To run this command without exiting the current context, prepend an exclamation mark (!) to the command. When run from a context, this command does not commit your pending changes to the Running configuration.

### Syntax

```
save-config
```

### Related commands

COMMAND	DESCRIPTION
<a href="#">commit</a>	Commit your pending changes to the Running configuration.

## service-access

Enables or disables service access.

### Syntax

```
service-access (enable|disable)
```

## set

Configures an item.

### Syntax

```
set cli filtering rule (auto-comment|no-auto-comment| (last-auto-comment-value INT))
```

## setup

Runs the setup wizard.

### Syntax

```
setup
```

## show

View current system configuration, status, and statistics.

COMMAND	DESCRIPTION
<a href="#">show aaa</a>	Show AAA information.
<a href="#">show auxdv</a>	Show the AuxDV package.
<a href="#">show date</a>	Show the current router date and time.
<a href="#">show dns</a>	Show Domain Name Service.

COMMAND	DESCRIPTION
<i>show filter</i>	Show filter information.
<i>show health</i>	Show health information.
<i>show high-availability</i>	Show high-availability status.
<i>show interface</i>	Show network interface.
<i>show key</i>	Show local server SSH key information.
<i>show license</i>	Show the license number and status.
<i>show log-file</i>	Show the log files.
<i>show log-file boot</i>	Show the boot file.
<i>show mfg-info</i>	Show manufacturing information.
<i>show np engine</i>	Show net processor statistics.
<i>show np general statistics</i>	Show general network processor information.
<i>show np mcfilt-rule-stats</i>	Show microfilter rules, number of flows, successful matches.
<i>show np protocol-mix</i>	Show network processor protocol-level statistics.
<i>show np reassembly</i>	Show network processor reassembly statistics.
<i>show np rule-stats</i>	Show network processor rules, number of flows, successful matches.
<i>show np softlinx</i>	Show network processor softlinx statistics.
<i>show np tier-stats</i>	Show network processor throughput and utilization for each tier.
<i>show quarantine-list</i>	Show quarantine list information.
<i>show reports</i>	Show status of data collection for reports.
<i>show service</i>	Show network service information.
<i>show sflow</i>	Show sFlow sampling configuration information.
<i>show sms</i>	Show status of SMS control.
<i>show snmp</i>	Show SNMP information.
<i>show stacking</i>	Show stacking information.
<i>show system connections</i>	Show active socket information.
<i>show system processes</i>	Show system processes.
<i>show system queue-stats</i>	Show internal queue stats.
<i>show system statistics</i>	Show system-wide protocol-related statistics.
<i>show system usage</i>	Show system usage.
<i>show system virtual-memory</i>	Show system virtual memory.
<i>show system xms memory</i>	Show xms memory usage.
<i>show terminal</i>	Show terminal settings.
<i>show traffic-file</i>	Show network traffic from file.

COMMAND	DESCRIPTION
<i>show tse</i>	Show threat suppression engine information.
<i>show user-disk</i>	Show user-disk statistics.
<i>show users</i>	Show users information.
<i>show version</i>	Show device version information.
<i>show virtual segments</i>	Show virtual segment configuration.

## show aaa

Syntax

```
show aaa capabilities USER
```

## show auxdv

Displays AuxDV package.

Syntax

```
show auxdv
```

## show date

Shows the GMT time or the local time and time zone for the device.

Syntax

```
show date [gmt]
```

## show dns

Syntax

```
show dns
```

## show filter

Displays the filters.

Syntax

```
show filter [XFILTERNUMBER | UDVFILTERNUMBER]
```



### Note

You can locate the application filter numbers from the LSM page, **Reports > Top Filter Matches**.

## show health

Shows health information.

Syntax

```
show health
```

## show high-availability

Syntax

```
show high-availability
```

### Related Commands

```
high-availability force (fallback|normal)
```

```
high-availability zero-power (slot <number>|all) (bypass-ips|normal)
```

## show inspection-bypass

Syntax

```
show inspection-bypass
```

## show interface

Syntax

```
show interface [INTERFACE [statistics [update INT]]]
```

## show key

Shows local server SSH key.

Syntax

```
show key
```

## show license

Syntax

```
show license
```

## show log-file

The following log files are available:

- system
- audit
- boot
- ipsAlert
- ipsBlock
- reputationAlert
- reputationBlock
- quarantine

### show log-file boot

Syntax

```
show log-file boot [tail [COUNT]] [more]
```

```
show log-file boot [search [<options>]{0,2} PATTERN] [count COUNT] [more]
```

If using the more option, the colon will display in the output, to indicate more information is available. Press the Enter key for the scroll to continue, or enter a q to exit and return to the ips{ } prompt.

### show log-file FILE\_NAME

#### Syntax

```
show log-file audit      [raw|tab|csv|rawcsv] [addUUID]
                        [ASC|DESC|(tail [COUNT])] [seqnum] [more]

show log-file ipsAlert   [raw|tab|csv|rawcsv] [addUUID]
                        [ASC|DESC|(tail [COUNT])] [seqnum] [more]

show log-file ipsBlock   [raw|tab|csv|rawcsv] [addUUID]
                        [ASC|DESC|(tail [COUNT])] [seqnum] [more]

show log-file quarantine [raw|tab|csv|rawcsv] [addUUID]
                        [ASC|DESC|(tail [COUNT])] [seqnum] [more]

show log-file reputationAlert [raw|tab|csv|rawcsv]
                        [addUUID] [ASC|DESC|(tail [COUNT])] [seqnum] [more]

show log-file reputationBlock [raw|tab|csv|rawcsv]
                        [addUUID] [ASC|DESC|(tail [COUNT])] [seqnum] [more]

show log-file summary     [raw|tab|csv|rawcsv] [addUUID]
                        [ASC|DESC|(tail [COUNT])] [seqnum] [more]

show log-file system      [raw|tab|csv|rawcsv] [addUUID]
                        [ASC|DESC|(tail [COUNT])] [seqnum] [more]

show log-file boot        [raw|tab|csv|rawcsv] [addUUID]
                        [ASC|DESC|(tail [COUNT])] [seqnum] [more]

show log-file audit       [raw|tab|csv|rawcsv] [addUUID] [ASC|DESC]
                        [search [(options)]{0,2} PATTERN][start-time START] [end-time END]
                        [seqnum[ [begin BEGIN] [end END]]] [count COUNT] [more]

show log-file ipsAlert    [raw|tab|csv|rawcsv] [addUUID] [ASC|DESC]
                        [search [(options)]{0,2} PATTERN][start-time START] [end-time END]
                        [seqnum[ [begin BEGIN] [end END]]] [count COUNT] [more]

show log-file ipsBlock    [raw|tab|csv|rawcsv] [addUUID] [ASC|DESC]
                        [search [(options)]{0,2} PATTERN][start-time START] [end-time END]
                        [seqnum[ [begin BEGIN] [end END]]] [count COUNT] [more]

show log-file quarantine  [raw|tab|csv|rawcsv] [addUUID] [ASC|DESC]
                        [search [(options)]{0,2} PATTERN][start-time START] [end-time END]
                        [seqnum[ [begin BEGIN] [end END]]] [count COUNT] [more]

show log-file reputationAlert [raw|tab|csv|rawcsv] [addUUID] [ASC|DESC]
                        [search [(options)]{0,2} PATTERN][start-time START] [end-time END]
                        [seqnum[ [begin BEGIN] [end END]]] [count COUNT] [more]

show log-file reputationBlock [raw|tab|csv|rawcsv] [addUUID] [ASC|DESC]
                        [search [(options)]{0,2} PATTERN][start-time START] [end-time END]
                        [seqnum[ [begin BEGIN] [end END]]] [count COUNT] [more]

show log-file summary     [raw|tab|csv|rawcsv] [addUUID] [ASC|DESC]
                        [search [(options)]{0,2} PATTERN][start-time START] [end-time END]
```

```
[seqnum[ [begin BEGIN] [end END]]] [count COUNT] [more]

show log-file system [raw|tab|csv|rawcsv] [addUUID] [ASC|DESC]
[search [(options)]{0,2} PATTERN][start-time START] [end-time END]
[seqnum[ [begin BEGIN] [end END]]] [count COUNT] [more]

show log-file boot [raw|tab|csv|rawcsv] [addUUID] [ASC|DESC]
[search [(options)]{0,2} PATTERN][start-time START] [end-time END]
[seqnum[ [begin BEGIN] [end END]]] [count COUNT] [more]

show log-file audit [raw|tab|csv|rawcsv] [addUUID] [ASC|DESC]
[search COLUMN cmp PATTERN [and|or COLUMN cmp PATTERN]{1,25}]
[start-time START] [end-time END] [seqnum[ [begin BEGIN] [end END]]]
[count COUNT] [more]

show log-file ipsAlert [raw|tab|csv|rawcsv] [addUUID] [ASC|DESC]
[search COLUMN cmp PATTERN [and|or COLUMN cmp PATTERN]{1,25}]
[start-time START] [end-time END] [seqnum[ [begin BEGIN] [end END]]]
[count COUNT] [more]

show log-file ipsBlock [raw|tab|csv|rawcsv] [addUUID] [ASC|DESC]
[search COLUMN cmp PATTERN [and|or COLUMN cmp PATTERN]{1,25}]
[start-time START] [end-time END] [seqnum[ [begin BEGIN] [end END]]]
[count COUNT] [more]

show log-file quarantine [raw|tab|csv|rawcsv] [addUUID] [ASC|DESC]
[search COLUMN cmp PATTERN [and|or COLUMN cmp PATTERN]{1,25}]
[start-time START] [end-time END] [seqnum[ [begin BEGIN] [end END]]]
[count COUNT] [more]

show log-file reputationAlert [raw|tab|csv|rawcsv] [addUUID] [ASC|DESC]
[search COLUMN cmp PATTERN [and|or COLUMN cmp PATTERN]{1,25}]
[start-time START] [end-time END] [seqnum[ [begin BEGIN] [end END]]]
[count COUNT] [more]

show log-file reputationBlock [raw|tab|csv|rawcsv] [addUUID] [ASC|DESC]
[search COLUMN cmp PATTERN [and|or COLUMN cmp PATTERN]{1,25}]
[start-time START] [end-time END] [seqnum[ [begin BEGIN] [end END]]]
[count COUNT] [more]

show log-file summary [raw|tab|csv|rawcsv] [addUUID] [ASC|DESC]
[search COLUMN cmp PATTERN [and|or COLUMN cmp PATTERN]{1,25}]
[start-time START] [end-time END] [seqnum[ [begin BEGIN] [end END]]]
[count COUNT] [more]

show log-file system [raw|tab|csv|rawcsv] [addUUID] [ASC|DESC]
[search COLUMN cmp PATTERN [and|or COLUMN cmp PATTERN]{1,25}]
[start-time START] [end-time END] [seqnum[ [begin BEGIN] [end END]]]
[count COUNT] [more]

show log-file boot[raw|tab|csv|rawcsv] [addUUID] [ASC|DESC]
[search COLUMN cmp PATTERN [and|or COLUMN cmp PATTERN]{1,25}]
[start-time START] [end-time END] [seqnum[ [begin BEGIN] [end END]]]
[count COUNT] [more]

show log-file audit [raw|tab|csv|rawcsv] [addUUID] follow [seqnum] [more]

show log-file ipsAlert [raw|tab|csv|rawcsv] [addUUID] follow [seqnum]
[more]
```



```

show log-file ipsBlock      [raw|tab|csv|rawcsv] [addUUID] follow [seqnum]
                             [more]

show log-file quarantine    [raw|tab|csv|rawcsv] [addUUID] follow [seqnum]
                             [more]

show log-file reputationAlert [raw|tab|csv|rawcsv] [addUUID] follow [seqnum]
                             [more]

show log-file reputationBlock [raw|tab|csv|rawcsv] [addUUID] follow [seqnum]
                             [more]

show log-file summary      [raw|tab|csv|rawcsv] [addUUID] follow [seqnum] [more]

show log-file system       [raw|tab|csv|rawcsv] [addUUID] follow [seqnum] [more]

show log-file boot         [raw|tab|csv|rawcsv] [addUUID] follow [seqnum] [more]

show log-file audit stat
show log-file ipsAlert stat
show log-file ipsBlock stat
show log-file quarantine stat
show log-file reputationAlert stat
show log-file reputationBlock stat
show log-file summary stat
show log-file system stat
show log-file boot stat
show log-file summary [verbose]
show log-file boot [tail COUNT] [more]
show log-file boot [search [(options)]{0,2} PATTERN] [count COUNT] [more]

```

### show log-file FILE\_NAME stat

Shows the beginning sequence number, ending sequence number, and number of messages for the given log file.

Syntax

```
show log-file FILE_NAME stat
```

### show log-file summary

Syntax

```
show log-file summary [verbose]
```

### show mfg-info

Shows manufacturing information.

Syntax

```
show mfg-info
```

### show np engine

Shows network processor information.

Syntax

```

show np      engine(filter|packet|parse|reputation(ip|dns)|rule)
      filter - Show filter-level      statistics
      packet - Show packet-layer     statistics

```

```
parse - Show packet      parsing statistics
reputation - Show      reputation statistics on either IP or DNS
rule - Show rule        statistics
```

## **show np general statistics**

Shows general network processor information.

Syntax

```
show np general statistics
```

## **show np mcfilt-rule-stats**

Shows microfilter rules, number of flows, and successful matches.

Syntax

```
show np mcfilt-rule-stats
```

## **show np protocol-mix**

Syntax

```
show np protocol-mix
```

## **show np reassembly**

Syntax

```
show np reassembly (ip|tcp)
```

## **show np rule-stats**

Syntax

```
show np rule-stats
```

## **show np softlinx**

Syntax

```
show np softlinx
```

## **show np tier-stats**

Displays statistics for monitoring activity since the last reboot of the device. Reboot the device to reset these counters.

Syntax

```
show np tier-stats
```

## **show quarantine-list**

Syntax

```
show quarantine-list
```

## **show reports**

Shows the status of the data collection for reports.

Syntax

```
show reports
```

### **show service**

Shows the state of all the services.

Syntax

```
show service
```

### **show sflow**

Syntax

```
show sflow
```

### **show slot**

Displays slot configuration, including the module type currently in the slot. Changes to the slot configuration are not reflected in the output of this command until after you reboot the device.

Syntax

```
show slot
```

### **show sms**

Syntax

```
show sms
```

### **show snmp**

Syntax

```
show snmp
```

### **show ssl-inspection congestion**

Shows SSL inspection information, including the average number of SSL connections per second, the number of current SSL connections (and the device limit), and whether SSL sessions that exceed the device limit are not inspected or blocked. By default, SSL sessions that exceed the device limit are not inspected.

Syntax

```
show ssl-inspection congestion
```

### **show stacking**

Enter this command to show stacking status information.

Syntax

```
show stacking
```

### **Reference**

PARAMETER	INFORMATION
Stacking enabled	Indicates whether stacking is enabled on the device.

PARAMETER	INFORMATION
Stacking active	Indicates whether stacking is currently functioning.
Stack member state	Indicates the current working state of this device on the stack.
Stack master	Indicates whether this device manages the state of the stack.
Number of devices configured in stack	Indicates the number of TippingPoint TPS security devices that are connected together through the stacking bus.
Number of devices required in stack	Indicates the minimum number of devices that must be available to the stack for normal operation. If the number of normal devices falls below this threshold, the stack goes into Intrinsic HA L2FB.
Advertised state	Indicates the state that the device advertises to the stack master.

## show system connections

Syntax

```
show system connection [ipv4|ipv6|sctp|unix]
```

## show system processes

Syntax

```
show system processes [LEVEL]
brief          Brief process information
detail        Detailed processinformation
extensive     Extensive processinformation
summary       Active process information
```

## show system queue-stats

Show internal queue statistics.

Syntax

```
show system queue-stats [fast-path]
```

## show system statistics

Syntax

```
show system statistics [fast-path] [non-zero]
```

## show system usage

Shows the overall system usage. You can run once, or display an updated version every INT seconds. Ctrl-C will exit a re-occurring update.

Syntax

```
show system usage [update INT]
```

## show system virtual-memory

Shows the system's kernel memory usage in a table with the following column headings:

- name
- active\_objs
- num\_objs
- objsize
- objperslab
- pagesperslab
- tunables
- limit
- batchcount
- sharedfactor
- slabdata
- active\_slabs
- num\_slabs
- sharedavail

Syntax

```
show system virtual-memory
```

## show system xms memory

Shows xms memory statistics.

Syntax

```
show system xms memory (all| SERVICE)
```

## show terminal

Shows terminal type information.

Syntax

```
show terminal
```

## show traffic-file

Syntax

```
show traffic-file FILENAME [verbose INT] [proto PROTO] [without PROTO] [pcap FILTER]
[pager]
```

### Options

traffic-file	Show network traffic from file
FILENAME	Capture file name
verbose	Configure verbosity level

INT	Verbosity level (0: minimum verbosity)
proto	Configure captured packets protocol
PROTO	Protocol name (default: all)
without	Configure excluded packets protocol
PROTO	Protocol name (default: all)
pcap	Configure pcap-syntax filter
FILTER	Pcap filter string (e.g. "src port 22")
pager	Show all messages

## show tse

Shows threat suppression engine information.

Syntax

```
show tse (connection-table(blocks|trusts)|rate-limit|ssl-inspection)
```

### show tse connection-table

Syntax

```
show tse connection-table TYPE
```

## show user-disk

Syntax

```
show user-disk
```

## show users

Syntax

```
show users [locked|ip-locked]
```

## show version

Syntax

```
show version
```

## show virtual segments

Shows virtual segment configuration.

Syntax

```
show virtual segments [summary]
```

## sms

Allows you to configure SMS settings and release SMS.

Syntax

```
sms must-be-ip (A.B.C.D|A.B.C.D/M)
```

```
sms unmanage
```

### Related commands

*show sms*

## snapshot create

Allows you to manage system snapshots.

Syntax

```
snapshot create NAME[ (reputation|manual|network) ]
```

Default is do not include the following:

manual	Include manually defined reputation entries in snapshot
network	Include Management port configuration in snapshot
reputation	Include reputation package in snapshot
nonet	Does not restore management port configuration if present in snapshot

## snapshot list

Syntax

```
snapshot list
```

## snapshot remove

Syntax

```
snapshot remove
```

## snapshot restore

A *snapshot* enables you to restore a device to a previously known working state. Restore a snapshot to the same device or to a different device. You can also export a snapshot and send it to TippingPoint Technical Support for assistance with troubleshooting or debugging the device. All snapshots are stored on the external user disk (CFast or SSD).

Make sure the device where you want to restore the snapshot meets the following requirements:

- The TOS version on the device is the same as the TOS version that was installed when the snapshot was taken.
- The device is the same model as the device where the snapshot was taken. For example, you can restore a snapshot from a 2200T to a 2200T.

When restoring a snapshot, keep in mind:

- The contents of the system keystore are not included in the snapshot. When you restore a snapshot to a different device, you should plan to also import any private key information from the device where the snapshot was taken.
- Never delete certificates that are used in snapshots that have, or have had, SSL configurations. Although the system will still complete its reboot sequence after restoring a snapshot that has had its SSL configuration (and corresponding device certificate) removed, the restored SSL configuration will not be functional until you update the private key for each certificate or replace the entire SSL configuration.
- When you want to restore a snapshot to a different device, and URL Reputation Filtering is enabled, a full synchronization of the Reputation database is required after you restore the snapshot. The snapshot does not include the ThreatDV URL Reputation Feed and User-defined URL Entries database. For more information, see the *SMS User Guide*.
- The snapshot includes the license package. The license package provides license information for each of your TippingPoint devices. If the license package that was included in the snapshot is outdated, restore the snapshot and then download and install an updated license package from the TMC.

- If an external ZPHA was configured on the original device, be sure to add an external ZPHA to the target device or update the device configuration to remove ZPHA.

Syntax

```
snapshot restore NAME
```

## tcpdump

Allows you to capture network traffic to the terminal or a file. You can specify a maximum packet count or a maximum capture file size. If you record the capture to a file you must specify a maximum packet count or maximum capture file size. Maxsize is the maximum size of the capture file in millions of bytes, which is limited by the currently available disk allocation.

Syntax

```
tcpdump INTERFACE [record FILENAME [maxsizebytes 1-10000000]]
[packetcount 1-10000000] [verbose 0-990000]
[proto (icmp|igmp|tcp|udp|esp|ah|pim|snp|vrrp|stp|isis|sctp)] [without
(icmp|igmp|tcp|udp|esp|ah|pim|snp|vrrp|stp|isis|sctp)] [pcap FILTER]
[cponly] [pager] [background]

tcpdump stop
```

## tech-support-report

Collects diagnostic information into a Tech Support Report (TSR) that TippingPoint Support can use to debug and troubleshoot system issues. It includes diagnostic commands, log files, and optionally a full system snapshot. The Tech Support Report snapshot captures the system's current running configuration.

If you include a snapshot with your Tech Support Report, the snapshot does not contain the following sensitive information:

- User names and passwords
- LDAP and remote server passwords
- SNMPv3 passphrase
- HA passphrase
- VPN IPsec keys
- Keystore

Only one report can exist on the device. When you create a new report, the previous report is replaced.

After you create a TSR, use the Local Security Manager (**Tools > Tech Support Report**) to export and view the TSR.

You should execute this command only when requested to do so by TippingPoint Support personnel.

It can take several minutes to execute this command. By default, this command is allowed to run as long as necessary to generate the TSR. Use the `max-runtime` option, if necessary, to set a maximum threshold for the amount of time, in seconds, that the command is allowed to run before interrupting the report generation.

Syntax

```
tech-support-report include-traffic-logs|exclude-traffic-logs
include-snapshot|exclude-snapshot [max-runtime INSECONDS]
```



## traceroute

Traceroute shows you the path a packet of information takes from your computer to your designation. It lists all the routers it passes through until it reaches its destination, or fails. Traceroute tells you how long router to router hops take.

### Syntax

```
traceroute (A.B.C.D|HOSTNAME) [from A.B.C.D]
(traceroute|traceroute6) X:X::X:X [from X:X::X:X]
```

## traceroute6

Trace IPv6 network routes.

### Syntax

```
ips{}traceroute6 (A.B.C.D|HOSTNAME) [from A.B.C.D]
```

## user-disk

Mounts, unmounts, and formats the external user disk (CFast or SSD).

After you mount the user disk, the device can automatically mount the disk when you reboot the device.

You can also enable encryption on the external user disk to secure its contents with the system master key. The external user disk stores all traffic logs, snapshots, and packet capture data. By default, the external user disk is not encrypted.

Before you secure the external user disk, keep in mind the following points:

- When you change the encryption status of the external user disk, the device automatically formats the disk and all traffic logs, snapshots, and packet capture data are erased. On large, external CFast disks (32 GB or more), it can take 40 seconds or more to complete disk format and encryption operations.
- The system master key encrypts and decrypts the external user disk. To access the contents of an encrypted external user disk from a different device, for example to restore a snapshot, the same master key must also be set on the device.

### Syntax

```
user-disk (encryption (enable|disable) | format | mount | unmount)
```

- *Unmount* – Unmount the external user disk.
- *Mount* – Mount the external disk and enable the device to automatically mount the disk on boot.
- *Format* – Format the external user disk.
- *Encryption Enable* – Enable encryption on the external user disk.

## Related commands

*show user-disk*

*master-key*

## Log configure commands

Enter the `log-configure` command to access the log configure context. Enter a question mark (?) at the `ips{log-configure}` prompt to display a list of valid command entries. Then enter `help` command name to display help for a specific command.

## display

Displays log configuration settings. In contrast to the `show` command, which shows the status of a configuration, the `display` command shows what you have configured. For example, if you enable high-availability on one device but not the other, the `display` command will show that you have high-availability configured and the `show` command will show that high-availability is not in effect.

Syntax

```
display [log-sessions] [xml|verbose]
```

## email

Allows you to set logging email daemon parameters.

Syntax

```
email set sleepSeconds SLEEPSEC
email set maxRequeue MAXREQUEUE
email delete (sleepSeconds|maxRequeue)
```

## log-file-size

Sets log file allocation as a percentage of the total 100 percent allowed for all log files.

```
# LOG FILE ALLOCATION SETTINGS
# INTERNAL DISK
log-file-size system          50%
log-file-size audit          50%
#                               ----
#                               Total 100%
```

Syntax

```
log-file-size FILE_NAME USAGE[%]
log-file-size
(audit|ipsAlert|ipsBlock|quarantine|reputationAlert|
reputationBlock|system|visibility) USAGE[%]
system and audit log files are kept on the internal disk
ipsAlert, ipsBlock, quarantine, reputationAlert,
reputationBlock, and visibility log files are kept on the external
or ramdisk drive
```

## log-storage

Sets local log file allocation of external user disk (CFast or SSD) space. Usage value can range from 50 to 99 percent. By default, 3.5 GB of the disk is a reserve for non-logging storage, which includes the Reputation databases. Although this space can be reduced or increased when rare circumstances require it, reducing the reserved space can interfere with URL filtering.

Syntax

```
log-storage external USAGE[%]
```

```
log-storage ramdisk USAGE[%]
```

```
log-storage externalReserve RESERVESIZE [MB]
```

## log-test

Sends a test message to the logging system(s).

Syntax

```
log-test (all|audit|quarantine|logID LOGID) [emergency [MESSAGE]]
log-test (all|audit|quarantine|logID LOGID) [alert [MESSAGE]]
log-test (all|audit|quarantine|logID LOGID) [critical [MESSAGE]]
log-test (all|audit|quarantine|logID LOGID) [error [MESSAGE]]
log-test (all|audit|quarantine|logID LOGID) [warning [MESSAGE]]
log-test (all|audit|quarantine|logID LOGID) [notice [MESSAGE]]
log-test (all|audit|quarantine|logID LOGID) [info [MESSAGE]]
log-test (all|audit|quarantine|logID LOGID) [debug [MESSAGE]]
log-test (all|audit|quarantine|logID LOGID) [msg MESSAGE]
```

Valid entries:

```
all           All log systems
audit         Audit system
quarantine    Quarantine system
logID         LogID system
LOGID         Log-session ID to test
SEVERITY      Set Severity level for log message (default: INFO)
Possible values for SEVERITY are:
emergency     EMERG level
alert         ALERT level
critical      CRIT level
error         ERR level
warning       WARNING level
notice        NOTICE level
info          INFO level (default)
debug         DEBUG level
msg           Override default message
MESSAGE       Message to send to logging system
```

## rotate

Sets log rotation parameters.

Syntax

```
rotate (set|delete) defaultCheckRecords (100-65535)
rotate (set|delete) defaultFiles (2-20)
rotate (set|delete) maxFileSize (10-500MB)
rotate (set|delete) rotateMsgSeverity SEVERITY
rotate (set|delete) sleepSeconds (1-65535)
rotate (set|delete) audit [Files (2-20)] [Records (100-65535)]
rotate (set|delete) ipsAlert [Files (2-20)] [Records (100-65535)]
rotate (set|delete) ipsBlock [Files (2-20)] [Records (100-65535)]
rotate (set|delete) quarantine [Files (2-20)] [Records (100-65535)]
rotate (set|delete) reputationAlert [Files (2-20)] [Records (100-65535)]
rotate (set|delete) reputationBlock [Files (2-20)] [Records (100-65535)]
rotate (set|delete) system [Files (2-20)] [Records (100-65535)]
rotate (set|delete) visibility [Files (2-20)] [Records (100-65535)]

sleepSeconds      Logrotation sleep time between checks
SLEEPSEC          Number of seconds logrotation waits between checks
defaultFiles      Default number of logrotation files
NUMFILES          Number of logrotation files (2 - 20)
```

defaultCheckRecords	Default number of records between log daemon size checks
NUMRECORDS	Number of records between log daemon size checks (100 - 65535)
maxFileSize	Max size a 'rotated' log file
MAXFILESIZE	Max log rotation file size in MB (10 - 500)
MB	Megabytes
FILE_NAME	Local log file name
Files	Number of logrotation files
Records	Number of records between log daemon size checks
delete	Delete the logrotation parameter

## Edit running configuration commands

Enter the `edit` command to access the configuration mode. In edit mode, you can perform numerous configurations, such as policies and authentication. After you have executed the `edit` command, the CLI prompt will be displayed as `ips{running}`. Configuration options, and sub contexts are available until you exit. To exit the edit configuration mode, enter `exit`.

The configuration mode enables administrators with the appropriate credentials to write configuration changes to the active (running) configuration. The logon account used to configure the device must either be associated with the Superuser role or the Administrator role to edit the configuration context. The configuration mode has different context levels that provide access to a specific set of configuration commands.



### Note

Use debug commands only when you are instructed to do so by TippingPoint product support.

This section is divided as follows:

- [Edit context commands](#)
- [Contexts and related commands](#)

## Edit context commands

### aaa

Syntax

```
aaa
```

### Related Commands

[running-aaa Context Commands](#)

### actionsets

Enters the action sets context mode. Changes are committed and take effect immediately.

Syntax

```
actionsets
```

### autodv

Enters Auto Digital Vaccine context mode.

Syntax  
autodv

## **blockedStreams**

Enters blockedStreams context mode.

Syntax  
blockedStreams

## **certificates**

Enters certificates context mode.

Syntax  
certificates

## **delete**

Deletes file or configuration item.

Syntax

```
delete interface
```

## **display**

Displays file or configuration item.

Syntax

```
display

Valid entries at this position are:
  <Enter>   Execute command
  CTX       Context name
  ip        Display IPv4 static routes
  ipv6      Display IPv6 static routes
  xml       Display in XML format
```

## **dns**

Enters DNS context mode.

Syntax  
dns

## **gen**

Enters general context mode.

Syntax  
gen

## **high-availability**

Enters high-availability context mode.

Syntax

high-availability

## interface

Enters interface context mode.

On TX Series devices, ports are presented in the format Slot-SegmentPort. For example, port 4A on slot 3 would be specified as “3-4A”.

Syntax

Configure network interface 1A in slot 3.

```
ips{}interface 3-1A
ips{running-3-1A}
```

Configure the management interface.

```
ips{}interface mgmt
ips{running-mgmt}
```

## physical-media settings

Valid entries are:

10half – Supported port speed and mode

10full – Supported port speed and mode

100half – Supported port speed and mode

100full – Supported port speed and mode

auto-neg – Enable auto-negotiation (default is on)

### Line speed

The line speed setting for a port.

You can set a port to 10, 100, or 1000 Kbps.

### Duplex setting

The duplex setting for the port. Copper can be set to **full** or **half**. Fiber ports can be set to **full**.

### Auto negotiation

The auto negotiation setting determines whether the port negotiates its speed based on the connection it can make.

## ips

Enters IPS profile context mode.



### Note

When IDS mode is enabled, it adjusts the device configuration so that the device operates in a manner suitable for Intrusion Detection System (IDS) scenarios and filter configurations. When IDS Mode settings are changed, reboot the device for the change to take effect.

---

Syntax

ips

## log

Enters log context mode. Note that the Management Console notification contact for the Audit log cannot be modified.

Syntax

log

## notifycontacts

Enters notify contacts context mode.

Syntax

notifycontacts

## ntp

Enters notify contacts context mode.

Syntax

ntp

## reputation

Enters Reputation context mode.

Syntax

reputation

## security-policy-reset

Resets IPS security policy to the default values.

Syntax

security-policy-reset

## segments

Enters segments context mode, which enables you to rename segments.

Syntax

```
segments
```

## services

Enters services context mode.

Syntax

```
services
```

## sflow

Enter sFlow<sup>®</sup> global configuration context mode.

Syntax

```
sflow
```

## snmp

Enters SNMP context mode.

Syntax

```
snmp
```

## ssl-inspection

Enters SSL inspection context mode.

Syntax

```
ssl-inspection
```

### Related commands

COMMAND	DESCRIPTION
<a href="#">certificates</a>	Store security certificates and private keys on the TPS as device certificates.
<a href="#">virtual-segments</a>	Assign an SSL inspection profile to a virtual segment.

## traffic-management

Enters traffic-management profile context.

Syntax

```
traffic-management
```

## virtual-segments

Enters virtual-segments context.

Syntax

```
virtual-segments
```

## Contexts and related commands

### running-aaa Context Commands

Immediate Commit Feature. Changes take effect immediately.



**ips{running-aaa}delete**

Delete file or configuration item.

Syntax

```
delete ldap-group (LDAPNAME|all)
delete radius-group (RADIUSNAME|all)
delete role (ROLE|all)
delete tacacs-group (TACACSNAME|all)

delete user (USER|all)
delete user-group (USERGROUP|all)
```

**ips{running-aaa}display**

Display configuration.

Syntax

```
display ldap-group LDAPGROUP [xml]
display ldap-schema LDAPSHEMA [xml]
display login-settings [xml]
display password-settings [xml]
display radius-group RADIUSGROUP [xml]
display remote-login-group [xml]
display role USER [xml]
display tacacs-group [xml]
display user USER [xml]
display usergroup USERGROUP [xml]
```

**ips{running-aaa}disable-inactive-users**

Disable users who are inactive for 35 days.

Syntax

```
disable-inactive-users
```

**ips{running-aaa}ldap-group**

Configure LDAP group. Maximum number of groups is two.

Syntax

```
ldap-group LDAPNAME
```

**ips{running-aaa}ldap-schema**

Configure LDAP schema.

Syntax

```
ldap-schema SCHEMA
SCHEMA
(active-directory|novell-edirectory|fedora-ds|rfc2798|rfc2307nis|samba|custom)
```

**ips{running-aaa}login**

Configure login settings, including the timeout period for inactivity in the CLI and the LSM. By default, the timeout period for inactivity in the CLI and the LSM is 15 minutes.

## Syntax

```
login maximum-attempts LOGINATTEMPTS
login failure-action FAILURE-ACTION
login lockout-period DURATION
login cli-inactive-timeout [MINUTES]
login lsm-inactive-timeout [MINUTES]
```

## Example of how to set a login failure action

```
ips{running-aaa}login failure-action lockout
```

## Example of help for login settings

```
ips{running-aaa}help login
```

## ips{running-aaa}login-banner

Configure login banner settings, including title and banner text.

## Syntax

```
login-banner (enable|disable)
login-banner text (1500 character max)
login-banner title (50 character max)
```

## ips{running-aaa}password

Configure password settings.

## Syntax

```
password quality (none|low|medium|high)
password expiry-time (10d|20d|30d|45d|60d|90d|6m|1y)
password expiry-action (force-change|notify-user|disable-account)
password disallow-reuse (enable|disable)
password min-lifetime (enable|disable)
```

## ips{running-aaa}radius-group

Configure Radius group. Maximum number of radius groups is 2.

## Syntax

```
radius-group RADIUSNAME
```

## ips{running-aaa}re-auth

Configure re-authentication settings. When this command is enabled, the CLI will force users to log out on any authentication changes.

## Syntax

```
re-auth (enable|disable)
```

## ips{running-aaa}remote-login-group

Configure LDAP, RADIUS group, or TACACS+ group to use for administrative login.

The name you provide for each group cannot be changed. To give a group a new name, you must delete the group and re-create it with the new name.

**Note**

Both RADIUS and TACACS+ authentication use protocols that are not FIPS-compliant. Before configuring RADIUS or TACACS+ for remote authentication, disable FIPS mode. For more information, see [fips-mode-enable](#).

**Syntax**

```
remote-login-group (administrator) (GROUP|none)
```

**ips{running-aaa}role**

Configure an access role.

**Syntax**

```
role ROLE [OLDROLE]
```

**ips{running-aaa}tacacs-group**

Configure TACACS+ group. Maximum number of TACACS+ groups is two.

**Syntax**

```
tacacs-group TACACSNAME
```

**ips{running-aaa}user**

Configure a name identified user.

**Syntax**

```
user NAME
```

**ips{running-aaa}user-group**

Configure a name identified usergroup.

**Syntax**

```
user-group GROUPNAME
```

**running-aaa-ldap-group-X Context Commands**

Immediate Commit Feature. Changes take effect immediately.

**ips{running-aaa-ldap-group-mygroup1}base-dn**

Configure base distinguished name (DN).

**Syntax**

```
base-dn DN
```

**ips{running-aaa-ldap-group-mygroup1}bind-dn**

Configure bind distinguished name (DN).

**Syntax**

```
bind-dn DN
```

**ips{running-aaa-ldap-group-mygroup1}delete**

Delete file or configuration item.

Syntax

```
delete server (ADDRESS|all)
```

**ips{running-aaa-ldap-group-mygroup1}port**

Configure LDAP port.

Syntax

```
port <0-65535>
```

**ips{running-aaa-ldap-group-mygroup1}retries**

Configure server(s) retries.

Syntax

```
retries RETRY
```

**ips{running-aaa-ldap-group-mygroup1}server**

Configure LDAP server address.

Syntax

```
server (A.B.C.D|X:X::X:X) priority (1-6)
```

**ips{running-aaa-ldap-group-mygroup1}timeout**

Configure timeout.

Syntax

```
timeout SECONDS
```

**ips{running-aaa-ldap-group-mygroup1}tls**

Configure TLS.

Syntax

```
tls (enable|disable)
tls start-tls (enable|disable)
tls require-valid-server-cert (enable|disable)
```

**running-aaa-radius-group-X Context Commands****ips{running-aaa-radius-group-2}default-usergroup**

Default usergroup.

Syntax

```
default-usergroup GROUP|none
```

### **ips{running-aaa-radius-group-2}delete**

Delete file or configuration item.

Syntax

```
delete server (A.B.C.D|X:X::X:X|all)
```

### **ips{running-aaa-radius-group-2}auth-type**

Specifies the authentication protocol for the RADIUS group. When the authentication protocol is PEAP/EAP-MSCHAPv2, be sure to also import the CA root certificate. The RADIUS group authenticates against the available CA root certificates on the device.

Syntax

```
auth-type PAP|MD5|PEAP/EAP-MSCHAPv2
```

### **Related commands**

COMMAND	DESCRIPTION
<a href="#"><i>ips{running-certificates}ca-certificate</i></a>	Import a CA certificate.

### **ips{running-aaa-radius-group-2}retries**

Configure server retries.

Syntax

```
retries (0-3)
```

### **ips{running-aaa-radius-group-2}server**

Configure server.

Syntax

```
server (A.B.C.D|X:X::X:X) [PORT] password PASSWORD priority (1-6)
timeout (1-10) [nas-id NASID]
```

## **running-aaa-tacacs-group-X Context Commands**

### **ips{running-aaa-tacacs-group-group1}auth-type**

Specifies the authentication protocol for the TACACS+ group. Supported protocols include ASCII, PAP, and CHAP. The TACACS+ group authenticates against the available CA root certificates on the device.

Syntax

```
auth-type ASCII|PAP|CHAP
```

## Related commands

COMMAND	DESCRIPTION
<a href="#"><i>ips{running-certificates}ca-certificate</i></a>	Import a CA certificate.

### **ips{running-aaa-tacacs-group-group1}default-usergroup**

Default usergroup. The default is operator.

Syntax

```
default-usergroup GROUP
```

### **ips{running-aaa-tacacs-group-group1}delete**

Delete file or configuration item.

Syntax

```
delete server (A.B.C.D|X:X::X:X|all)
```

### **ips{running-aaa-tacacs-group-group1}retries**

Configure server retries.

Syntax

```
retries (0-3)
```

### **ips{running-aaa-tacacs-group-group1}server**

Configure TACACS+ server.

Syntax

```
server (A.B.C.D|X:X::X:X) [PORT] secret SECRET priority (1-6)
timeout (1-15)
```

## running-actionsets Context Commands

Immediate Commit Feature. Changes take effect immediately.

### **ips{running-actionsets}actionset**

Enter an action set context with defined name.

Syntax

```
actionsets ACTIONSETNAME
```

### **ips{running-actionsets}rename**

Rename action set.

Syntax

```
rename actionset ACTIONSETNAME NEWACTIONSETNAME
```

## running-actionsets-X Context Commands

Immediate Commit Feature. Changes take effect immediately.

### **ips{running-actionsets-myactionset1}action**

Delete file or configuration item.

Set action type. Available values: permit, rate-limit, block, trust.

Immediate Commit Feature. Changes take effect immediately.

Syntax

```
action (permit|rate-limit|block|trust)
```

### **ips{running-actionsets-myactionset1}allow-access**

Allow quarantined host to access defined IP.

Syntax

```
allow-access DESTIP
```

### **ips{running-actionsets-myactionset1}bytes-to-capture**

Set bytes to capture for packet trace.

Syntax

```
bytes-to-capture BYTES
```

### **ips{running-actionsets-myactionset1}delete**

Delete file or configuration item.

Syntax

```
delete allow-access DESTIP
delete contact XCONTACTNAME
delete limit-quarantine SOURCEIP
delete no-quarantine SOURCEIP
```

### **ips{running-actionsets-myactionset1}http-block**

Set quarantine option to block HTTP traffic.

Syntax

```
http-block
```

### **ips{running-actionsets-myactionset1}http-redirect**

Set redirect URL for HTTP redirect option.

Syntax

```
http-redirect URL
```

**ips{running-actionsets-myactionset1}http-showdesc**

Set or clear HTTP show description display option.

Syntax

```
http-showdesc (enable|disable)
```

**ips{running-actionsets-myactionset1}limit-quarantine**

Add IP for limit quarantine.

Syntax

```
limit-quarantine SOURCEIP
```

**ips{running-actionsets-myactionset1}packet-trace**

Configure packet trace option.

Syntax

```
packet-trace (enable|disable|delete|download)
```

**ips{running-actionsets-myactionset1}priority**

Set packet trace priority.

Syntax

```
priority PRIORITY
```

**ips{running-actionsets-myactionset1}quarantine**

Set quarantine option. Available options: no, immediate, threshold.

Syntax

```
quarantine QUARANTINETYPE
```

**ips{running-actionsets-myactionset1}tcp-reset**

Set tcp reset option for block action. Available options: none (disable), source, dest, or both.

Syntax

```
tcp-reset (none|source|dest|both)
```

**ips{running-actionsets-myactionset1}threshold**

Set quarantine threshold value.

Syntax

```
threshold (2-10000) (1-60)
```

**ips{running-actionsets-myactionset1}verbosity**

Set packet trace verbosity.

Syntax



```
verbosity (partial|full)
```

## **running-autodv Context Commands**

Immediate Commit Feature. Changes take effect immediately.

### **ips{running-autodv}calendar**

Enter Calender Style.

Syntax

```
calendar
```

### **ips{running-autodv}delete**

Delete file or configuration item.

Syntax

```
delete proxy  
delete proxy-password  
delete proxy-username
```

### **ips{running-autodv}disable**

Disable service.

Syntax

```
disable
```

### **ips{running-autodv}enable**

Enable service.

Syntax

```
enable
```

### **ips{running-autodv}list**

List Installed DVs.

Syntax

```
list
```

### **ips{running-autodv}periodic**

Enter Periodic Style.

Syntax

```
periodic
```

### **ips{running-autodv}proxy**

Configures a proxy server.

Syntax

```
proxy ADDR port PORT
```

### **ips{running-autodv}proxy-password**

Sets a password for a proxy server.

Syntax

```
proxy-password PASSWD
```

### **ips{running-autodv}proxy-username**

Sets a password for a proxy server.

Syntax

```
proxy-username USER
```

### **ips{running-autodv}update**

Update AutoDV.

Syntax

```
update
```

## **running-autodv-periodic Context Commands**

Immediate Commit Feature. Changes take effect immediately.

### **ips{running-autodv-periodic}day**

Day of the week to update.

Syntax

```
day (Sunday|Monday|Tuesday|Wednesday|Thursday|Friday|Saturday)
```

### **ips{running-autodv-periodic}period**

Set number of days between update checks.

Syntax

```
period PERIOD  
PERIOD Value range is 0 - 99, unit is days
```

### **ips{running-autodv-periodic}time**

Time of day to check for updates.

Syntax

```
time HOURS:MINUTES  
HOURS Value range is 0 - 23  
MINUTES Value range is 0 - 59
```

## running-blockedStreams Context Commands

Immediate Commit Feature. Changes take effect immediately.

### **ips{running-blockedStreams}flushallstreams**

Flush All Reports.

Syntax

```
flushallstreams
```

### **ips{running-blockedStreams}flushstreams**

Flush reports.

Syntax

```
flushstreams
```

### **ips{running-blockedStreams}list**

List reports.

Syntax

```
list
```

## running-certificates Context Commands

Immediate Commit Feature. Changes take effect immediately.

### **ips{running-certificates}certificate**

Add or update a device certificate with the certificate contents from your web server. To inspect secure sessions, the TPS requires both the certificate and private key from your web server.

(Best Practice) Name the certificate so that you can safely and reliably assign it to the correct SSL server.

When the keystore mode is **sms-managed**, use the SMS to manage device certificates and private keys.

Syntax

```
certificate CERTNAME
```

### Related commands

COMMAND	DESCRIPTION
<a href="#"><i>ips{running-certificates}private-key</i></a>	Import the private key from your web server into the local keystore on the TPS device.
<a href="#"><i>ips{running-sslinsp}server</i></a>	Add an SSL server to the TPS device with the same security settings as your web server, and assign the corresponding certificate and private key.

### **ips{running-certificates}ca-certificate**

Add CA certificate.

Syntax

```
ca-certificate CANAME
```

### **ips{running-certificates}delete**

Delete file or configuration item.

Syntax

```
delete ca-certificate (all|CANAME)
```

### **ips{running-certificates}display**

Display file or configuration item.

Syntax

```
display ca-certificate CANAME [pem|text]
```

### **ips{running-certificates}private-key**

Import a private key into the keystore on the device and assign it to the specified device certificate. Use the **save-config** command to secure the private key in the keystore.

To inspect secure sessions, the TPS requires both the certificate and private key from your web server.

When the keystore mode is **sms-managed**, this command is not applicable. Use the SMS to manage device certificates and private keys.

Syntax

```
private-key CERTNAME
```

## **Related commands**

COMMAND	DESCRIPTION
<a href="#"><i>ips{running-certificates}certificate</i></a>	Import the certificate from your web server into the local keystore on the TPS device.
<a href="#"><i>ips{running-sslinsp}server</i></a>	Add an SSL server to the TPS device with the same security settings as your web server, and assign the corresponding certificate and private key.

## **running-dns Context Commands**

Immediate Commit Feature. Changes take effect immediately.

### **ips{running-dns}delete**

Immediate Commit Feature. Changes take effect immediately. Delete file or configuration item. A secondary domain-search can only be deleted if no tertiary exists. A primary domain-search can only be deleted if no secondary exists.

Syntax

```
delete domain-name
delete domain-search (primary|secondary|tertiary|all)
delete name-server (all|A.B.C.D|X:X::X:X)
delete proxy cache cleaning interval
delete proxy cache forwarder (all|A.B.C.D|X:X::X:X)
delete proxy cache maximum negative ttl
```

```
delete proxy cache maximum ttl
delete proxy cache size
```

### **ips{running-dns}domain-name**

Immediate Commit Feature. Changes take effect immediately. Configure domain name.

Syntax

```
domain-name NAME
```

### **ips{running-dns}domain-search**

Immediate Commit Feature. Changes take effect immediately. Configure domain search. A secondary domain-search can only be entered after a primary is entered and a tertiary can only be entered after a secondary is entered.

Syntax

```
domain-search (primary|secondary|tertiary) NAME
```

### **ips{running-dns}name-server**

Configure DNS server.

Syntax

```
name-server (A.B.C.D|X:X::X:X)
```

### **ips{running-dns}proxy**

Configure proxy.

Syntax

```
proxy (enable|disable)
proxy cache cleaning interval cache cleaning interval in minutes
proxy cache forwarder A.B.C.D|X:X::X:X
proxy cache maximum negative ttl cache maximum negative ttl in minutes
proxy cache maximum ttl cache maximum ttl in minutes
proxy cache size cache size in megabytes
```

## **running-gen Context Commands**

Immediate Commit Feature. Changes take effect immediately.

### **ips{running-gen}delete**

Delete file or configuration item.

Syntax

```
delete host (NAME|all)
```

### **ips{running-gen}ephemeral-port-range**

Set the range of the ephemeral port (default is 32768-61000).

Syntax

```
ephemeral-port-range (default|(LOWRANGE HIGHRANGE))
default Default port range value 32768-61000 is applied
```

```
LOWRANGE Value of the first port
HIGH RANGE Value of the last port
```

### **ips{running-gen}host**

Configure static address to host name association.

Syntax

```
host NAME (A.B.C.D|X:X::X:X)
```

### **ips{running-gen}https**

Disable and enable HTTPS access on the TPS management port. By default, HTTPS access is enabled to allow access to the device through the LSM, and to enable the Security Management System (SMS) to manage the device.

Note that this command does not disable SSH access on the TPS management port. See [\*ips{running-gen}ssh\*](#) for more information.

Syntax

```
https (enable|disable)
```

### **ips{running-gen}lsm**

Disable and enable the LSM.

Syntax

```
lsm (enable|disable)
```

### **ips{running-gen}sms-allowed-ip**

Configure allowed SMS IP addresses.

Syntax

```
sms-allowed-ip A.B.C.D (IPv4 address)
sms-allowed-ip A.B.C.D/M (IPv4 address with netmask)
sms-allowed-ip X:X::X:X (IPv6 address)
sms-allowed-ip X:X::X:X/M (IPv6 address with prefix length)
sms-allowed-ip all (All SMS IP addresses are allowed)
```

### **ips{running-gen}ssh**

Disable and enable SSH access on the TPS management port. By default, SSH access is enabled to allow CLI access to the device.

Note that this command does not disable HTTPS access on the TPS management port. See [\*ips{running-gen}https\*](#) for more information.

Syntax

```
ssh (enable|disable)
```

### **ips{running-gen}timezone**

Display or configure time zone.

**Note**

Use the US option to specify a standard time zone in the United States.

**Syntax**

```
timezone GMT
timezone REGION CITY
REGION
(Africa|America|Antarctica|Arctic|Asia|Atlantic|
Australia|Europe|Indian|US|Pacific)
```

**ips{running-gen}tls**

Enable or disable TLS versions on the management interface.

Disable older TLS versions to secure the management interface. When deciding which TLS versions to disable, keep in mind that the LSM, SMS, and Captive Portal communicate through the device's management interface.

**Syntax**

```
tls (TLSv1.0 |TLSv1.1 |TLSv1.2 ) (enable|disable)
```

**running-high-availability Context Commands**

Create or enter a high-availability context.

**ips{running-high-availability}disable**

Disables HA.

**Syntax**

```
disable
```

**ips{running-high-availability}enable**

Enables high-availability on the local device.

**Syntax**

```
enable
```

**ips{running-high-availability}encryption**

Applies encryption hash for a passphrase.

**Syntax**

```
encryption (passphrase PASSPHRASE) |enable|disable
```

**ips{running-high-availability}partner**

Specifies the HA partner.

For 440T and 2200T devices that use the HA port, enter the partner device serial number. For 8200TX and 8400TX devices that use the MGMT port, enter the partner device MGMT port IP address.

## Syntax

HA port:

```
partner SERIAL
```

MGMT port:

```
partner IP ADDRESS
```

## running-inspection-bypass Context Commands

Enables, disables, or removes inspection bypass rules. Inspection bypass rules direct traffic through the TippingPoint TPS devices without inspection. You can view a list of current inspection bypass rules with the **display** command.



### Important

When creating an inspection bypass rule that includes source and destination ports or IP addresses, you must first specify the IP protocol as UDP or TCP.

You can now define up to 32 inspection bypass rules on a TippingPoint TPS. Rule configurations that bypass IPv6 traffic or VLAN ranges require additional hardware resources. For example, a single inspection bypass rule for IPv6 or VLAN traffic can result in multiple port-VLAN rule combinations.

INSPECTION BYPASS RULE	RESULTING NUMBER OF PORT-VLAN RULE COMBINATIONS
IPv4 traffic on TCP 1556 with untagged traffic or a particular VLAN ID	1
IPv6 traffic on TCP 1556 with untagged traffic or a particular VLAN ID	2
IPv4 traffic on TCP 1556 with VLAN 10 – 100	90
IPv6 traffic on TCP 1556 with VLAN 10 – 100	180

Each TPS supports a maximum number of port-VLAN rule combinations. If the number of configured port-VLAN rule combinations exceeds the maximum threshold for the device, you cannot commit the changes.

FOR A	MAXIMUM (APPROXIMATE) NUMBER OF PORT-VLAN RULE COMBINATIONS
440T	256 when bypassing IPv4 traffic, 128 for IPv6 traffic
2200T	2560 when bypassing IPv4 traffic 1280 when bypassing IPv6 traffic
8200TX	512 when bypassing IPv4 or IPv6 traffic
8400TX	512 when bypassing IPv4 or IPv6 traffic

## Syntax

Type **help** and press Enter for more information.

```
ips{running-inspection-bypass}help
Valid commands are:
  delete RULENAME
  help [full|COMMAND]
  rule NEWRULENAME
  rule RULENAME
```

When you edit or create an inspection bypass rule, the context changes to that rule.



From the context of an inspection bypass rule, type **help** and press Enter for a list of commands, or type **help command** for help on a particular command.

### **ips{running-inspection-bypass-rule-myrule1}action**

Specify which action the rule applies to the traffic.

#### **Syntax**

```
ips{running-inspection-bypass-rule-myrule1}action <action> [PORTNAME]
```



#### **Note**

Redirect and Mirror options are not supported for inspection bypass when there are no target ports available.

To block incoming traffic:

```
ips{running-inspection-bypass-rule-myrule1}action block
```

To copy traffic entering the port and send it to segment port 5B before the traffic gets inspected:

```
ips{running-inspection-bypass-rule-myrule1}action ingress-mirror 5B
```

### **ips{running-inspection-bypass-rule-myrule1}eth**

Specifies the Ethernet Type that you do not want to inspect. When you define an inspection bypass rule, an option without a specified value defaults to a value of “any”. For example, if you do not specify a value for **eth**, it defaults to a value of any Ethernet Type.

Enter **help eth** and press Enter to display options for specifying an EtherType. Note that a value of **ip** specifies both IPv4 and IPv6.



#### **Note**

A full list of Ethernet Type values can be found at the Internet Assigned Numbers Authority [website](http://www.iana.org/). When specifying an Ethernet Type as a hexadecimal value, prepend 0x, for example, 0x0806 for ARP.

### **ips{running-inspection-bypass-rule-myrule1}ip-proto**

Specifies the IP protocols that you do not want to inspect. When you define an inspection bypass rule, an option without a specified value defaults to a value of “any”. For example, if you do not specify a value for **ip-proto**, it defaults to a value of any IP protocol.

If you change the IP protocol to a protocol other than TCP or UDP, the corresponding TCP or UDP ports are automatically removed. Edit an inspection bypass rule and enter **ip-proto udp** to not inspect UDP traffic.



#### **Note**

A full list of IP protocol values can be found at the Internet Assigned Numbers Authority website at <http://www.iana.org/assignments/protocol-numbers>.

#### **Syntax**

Enter **help ip-proto** and press Enter to display options for specifying an IP protocol.

```
ips{running-inspection-bypass-rule-myrule1}help ip-proto
Enter ip protocol for inspection bypass rule
Syntax: ip-proto PROTO_OPTION|PROTO_VALUE
```

```

ip-proto      Enter ip protocol for inspection bypass rule
PROTO_OPTION  Enter ip protocol (udp or tcp) for inspection bypass rule
Possible values for PROTO_OPTION are:
udp           udp protocol
tcp           tcp protocol
PROTO_VALUE   Enter ip protocol value (e.g. 115 for L2TP)

```

### **ips{running-inspection-bypass-rule-myrule1}vlan-id**

Specifies the VLAN traffic that you do not want to inspect. When you define an inspection bypass rule, an option without a specified value defaults to a value of “any”. For example, if you do not specify a value for **vlan-id**, it defaults to **all** tagged and untagged traffic.

#### **Syntax**

Enter **help vlan-id** and press Enter to display options for specifying a range of VLAN IDs.

```

ips{running-inspection-bypass-rule-myrule1}help vlan-id
Valid commands are:
vlan-id none
vlan-id VLANID
vlan-id range MINVLANID MAXVLANID

```

Edit an inspection bypass rule and enter **vlan-id none** to not inspect untagged VLAN traffic. Then, type **display** and press Enter to view your change.

## **running-interface Context Commands**

Create or enter an interface context.

### **ips{running}interface nM**

Enters context for configuring Ethernet settings. The port name, for example, 1A, is case-sensitive.

#### **Syntax**

```

interface nM
Valid entries at this position are:
delete      Delete file or configuration item
help        Display help information
physical-media  Configure ethernet port settings
restart     Restart Ethernet port
shutdown    Shutdown logical interface state

```

### **ips{running}interface mgmt**

Enters context for configuring management settings.

#### **Syntax**

```

interface mgmt
Valid entries at this position are:
delete      Delete file or configuration item
description Enter description for the management interface
help        Display help information
host        Configure host name, location, or contact
ip-filter    Limit which ip addresses can access mgmt port
ipaddress    Configure IP address

```

physical-media	Configure mgmt port speed/duplex
route	Add IPv4/IPv6 static route

## running-ips Context Commands

Immediate Commit Feature. Changes take effect immediately.

### ips{running-ips}afc-mode

Configures AFC mode.

Syntax

```
afc-mode AFCMODE
```

### ips{running-ips}afc-severity

Configures AFC severity level.

Syntax

```
afc-severity SEVERITY
```

### ips{running-ips}asymmetric-network

Configures asymmetric network mode.

Syntax

```
asymmetric-network enable | disable
```

### ips{running-ips}connection-table

Configures connection table timeout.

Syntax

```
connection-table TIMEOUTTYPE SECONDS
TIMEOUTTYPE          Connection table timeout type
Possible values for TIMEOUTTYPE are:
non-tcp-timeout      Connection table non-tcp timeout
timeout              Connection table timeout
trust-timeout         Connection table trust timeout
SECONDS              Connection table timeout seconds
```

### ips{running-ips}delete

Allows you to delete a profile.

Syntax

```
delete profile XPROFILENAME
```

### ips{running-ips}deployment-choices

Lists deployment choices.

Syntax

```
deployment (Aggressive|Core|Default|Edge|Perimeter)
```

### **ips{running-ips}display**

Display all IPS configuration and profiles.

Syntax

```
display
```

### **ips{running-ips}display-categoryrules**

Display category rules for all profiles.

Syntax

```
display-categoryrules
```

### **ips{running-ips}gzip-decompression**

Sets GZIP decompression mode.

Syntax

```
gzip-decompression (enable|disable)
```

### **ips{running-ips}http-encoded-resp**

Configures inspection of encoded HTTP responses.

Syntax

```
http-encoded-resp (accelerated|inspect url-ncr STATUS)|ignore
accelerated      Accelerated inspection of encoded HTTP responses
ignore           Ignore encoded HTTP responses
inspect          Inspect encoded HTTP responses
```

### **ips{running-ips}http-mode**

Configures HTTP mode, which allows all TCP ports to be treated as HTTP ports for inspection purposes. If a flow does not have HTTP traffic, HTTP processing stops so that optimum performance is maintained.

Syntax

```
http-mode enable | disable
```

### **ips{running-ips}profile**

Allows you to create or enter an IPS profile and configure whether the True-Client-IP address and additional HTTP context information are collected for the profile.

Syntax

```
profile PROFILENAME client-ip [enable|disable] http-context [enable|disable]
```

### **ips{running-ips}quarantine-duration**

Sets quarantine duration.

Syntax

```
quarantine-duration DURATION
DURATION value between 1 to 1440 minutes
```

### **ips{running-ips}rename**

Renames a profile.

Syntax

```
rename profile PROFILENAME NEWPROFILENAME
```

## **running-ips-X Context Commands**

Immediate Commit Feature. Changes take effect immediately.

### **ips{running-ips-1}categoryrule**

Enters categoryrule context.

Syntax

```
categoryrule
```

### **ips{running-ips-1}delete**

Delete file or configuration item.

Syntax

```
delete filter FILTERNUMBER
FILTERNUMBER Existing filter number
```

### **ips{running-ips-1}description**

Edit description for a profile.

Syntax

```
description DESCRIPTION
```

### **ips{running-ips-1}filter**

Creates or enters a filter context.

Syntax

```
filter FILTERNUMBER
```

## **running-log Context Commands**

Create or enter a running-log context.

### **ips{running-log}delete**

Delete file or configuration item.

Syntax

```
delete log audit CONTACT-NAME
delete log quarantine CONTACT-NAME
```

```

delete log system CONTACT-NAME
delete log-option xmsd( all)|( LOG_OPTION)
delete logging-mode
help [full|COMMAND]
log audit CONTACT-NAME [ALL|none]
log quarantine CONTACT-NAME [ALL|none]
log system CONTACT-NAME [SEVERITY]
log-option xmsd( all)|( LOG_OPTION)
logging-mode unconditional|(conditional [threshold PERCENTAGE] [period TIMEOUT])
sub-system SUBSYSTEM [SEVERITY]

```

### ips{running-log}log

Add log to a log session.

Syntax

```

log audit CONTACT-NAME [ALL|none]
log quarantine CONTACT-NAME [ALL|none]
log system CONTACT-NAME [SEVERITY]
Valid entries at this position are:
<Enter>      Execute command
audit        Configure log for audit services
quarantine    Configure log for quarantine services
system       Configure log for all services

```

### ips{running-log}log-option

Add service log option.

Syntax

```

log-option xmsd( all)|( LOG_OPTION)
log-option      Add service log option
xmsd            Configure xmsd log options
all             Enable logging all options
LOG_OPTION      Log-option item for XMSD
Possible values for LOG_OPTION are:
segments        Enable logging segments
mgmt            Enable logging mgmt
interface       Enable logging interface
xms_configure   Enable logging xms configure
xms_process     Enable logging xms process
xms_stream      Enable logging xms stream
aaa             Enable logging aaa
dns             Enable logging dns
ethernet        Enable logging ethernet
highavailability Enable logging highavailability
linkmonitor     Enable logging linkmonitor
log             Enable logging log
ntp             Enable logging ntp
ports           Enable logging ports
services        Enable logging services
udm-conf-handler Enable logging UDM configuration handler
snmp            Enable logging snmp
system          Enable logging system
qos             Enable logging qos
virtual-segments Enable logging virtual-segments
xmsupdate       Enable logging xmsupdate
vrf             Enable logging vrf

```

x509	Enable logging x509
xipc	Enable logging xipc requests
trafficlights	Enable logging trafficlights requests
vlan-translations	Enable logging vlan-translations

### **ips{running-log}logging-mode**

Configure logging behavior when the system is congested.

Syntax

```
logging-mode unconditional|(conditional [threshold PERCENTAGE]
                        [period TIMEOUT])
logging-mode          Configure logging behavior when the system is congested
unconditional         Always log even if traffic is dropped under high load
conditional           Disable logging if needed to prevent congestion (default)
threshold             Congestion threshold at which to disable logging (default: 1.0%)
PERCENTAGE            Congestion percentage (0.1% to 99.9%)
period               Amount of time to disable logging (default: 600 seconds)
TIMEOUT              Log disable time in seconds (60 to 3600)
```

### **ips{running-log}sub-system**

Sets sub-system log level.

Syntax

```
sub-system SUBSYSTEM [SEVERITY]
sub-system (COROSYNC|HTTPD|INIT|LOGIN|TOS|XMS|CRMADMIN)
[alert|critical|debug|emergency|error|info|notice|warning|none]
Possible values for SEVERITY are:
emergency Panic condition messages (TOS critical)
alert Immediate problem condition messages
critical Critical condition messages
error Error messages
warning Warning messages
notice Special condition messages
info Informational messages
debug Debug messages
debug0 TOS Debug0 messages
debug1 TOS Debug1 messages
debug2 TOS Debug2 messages
debug3 TOS Debug3 messages
none Turn off messages
```

## **running-notifycontacts (email) Context Commands**

Immediate Commit Feature. Changes take effect immediately.

### **ips{running-notifycontacts}contact**

Create or edit a notify contact.

Syntax

```
contact CONTACTNAME
contact NEWNAME email
contact NEWNAME snmp COMMUNITY IP [PORT]
```

**ips{running-notifycontacts}delete**

Delete a contact or an email setting.

Syntax

```
delete contact XCONTACTNAME
delete EMAILSETTING
```

**ips{running-notifycontacts}email-from-address**

From email address.

Syntax

```
email-from-address EMAIL
```

**ips{running-notifycontacts}email-from-domain**

From domain name.

Syntax

```
email-from-domain DOMAIN
```

**ips{running-notifycontacts}email-server**

Set mail server IP.

Syntax

```
email-server IP
```

**ips{running-notifycontacts}email-threshold**

Set email threshold per minute

Syntax

```
email-threshold THRESHOLD
THRESHOLD Threshold-value, value range 1-35 per minute
```

**ips{running-notifycontacts}email-to-default-address**

Default to email address.

Syntax

```
email-to-default-address EMAIL
```

**ips{running-notifycontacts}rename**

Rename contact with new name.

Syntax

```
rename contact XCONTACTNAME NEWNAME
```



## running-ntp Context Commands

Immediate Commit Feature. Changes take effect immediately.

### ips{running-ntp}delete

Delete file or configuration item.

Syntax

```
delete key (all|ID)
delete server (all|HOST)
Valid entries:
key Delete key from configuration
all Delete all keys
ID Key identifier
server Delete remote NTP server
all Delete all servers
HOST Remote server address or name
```

### ips{running-ntp}key

Configure NTP authentication key.

Syntax

```
key (1-65535) VALUE
Valid entries:
(1-65535) Key ID, required for authentication
VALUE Key value (1-32 characters)
```

### ips{running-ntp}ntp

Enable or disable NTP service.

Syntax

```
ntp (enable|disable)
```

### ips{running-ntp}polling-interval

Configure NTP server minimum polling interval.

Syntax

```
polling-interval SECONDS
SECONDS Interval in seconds
Possible values for SECONDS are:
2 2 seconds
4 4 seconds
8 8 seconds
16 16 seconds
32 32 seconds
64 64 seconds
```

### ips{running-ntp}server

Configure remote NTP server.

Syntax

```
server (dhcp|A.B.C.D|X:X::X:X|FQDN) [key ID] [prefer]
dhcp    Get server address from dhcp
NAME    NTP remote server
key     Key to be used
ID      Key identifier
prefer  Mark server as preferred
```

## running-rep Context Commands

Immediate Commit Feature. Changes take effect immediately.

### ips{running-rep}delete

Delete file or configuration item.

Syntax

```
delete group USERGROUP
delete profile XPPROFILENAME
Valid entries:
group    Reputation group
profile  Delete reputation profile
```

### ips{running-rep}group

Create or enter reputation group context.

Syntax

```
group USERGROUP
Valid entries:
USERGROUP    Reputation usergroup name
```

### ips{running-rep}nxdomain-response

Responds with NXDOMAIN (name does not exist) to clients that make DNS requests for hosts that are blocked.

Syntax

```
nxdomain-response (enable|disable)
```

### ips{running-rep}profile

Create or enter reputation profile context.

Syntax

```
profile PROFILENAME
```

### ips{running-rep}rename

Rename a reputation profile or group.

Syntax

```
rename group USERGROUP NEWUSERGROUP
rename profile XPROFILENAME NEWPROFILENAME
Valid entries:
```

```
group Reputation group
profile Reputation profile
```

## running-rep-X (group X) Context Commands

Immediate Commit Feature. Changes take effect immediately.

### ips{running-rep-1}delete

Delete file or configuration item.

Syntax

```
delete domain DOMAINNAME
delete ip (A.B.C.D|A.B.C.D/M|X:X::X:X|X:X::X:X/M)
Valid entries:
domain Domain name
ip IP address IPv4/IPv6/CIDR
```

### ips{running-rep-1}description

Add a description to the reputation group.

Syntax

```
description DESCRIPTION
```

### ips{running-rep-1}domain

New domain name.

Syntax

```
domain NEWDOMAIN
```

### ips{running-rep-1}ip

New IP address (IPv5/IPv6/CIDR).

Syntax

```
ip IPADDRESS
```

## running-rep-X (profile X) Context Commands

Immediate Commit Feature. Changes take effect immediately.

### ips{running-rep-abc}action-when-pending

Set pending action to permit or drop.

Syntax

```
action-when-pending (permit|drop)
```

### ips{running-rep-abc}check-destination-address

Enables or disables check destination address.

Syntax

```
check-destination-address (enable|disable)
```

### **ips{running-rep-abc}check-source-address**

Enables or disables check source address.

Syntax

```
check-source-address (enable|disable)
Valid entries:
enable  Enable check source address
disable Disable check source address
```

### **ips{running-rep-abc}delete**

Delete file or configuration item.

Syntax

```
delete dns-except DOMAINNAME
delete filter REPGROUP
delete ip-except (A.B.C.D|A.B.C.D/M|X:X::X:X|X:X::X:X/M)
(A.B.C.D|A.B.C.D/M|X:X::X:X|X:X::X:X/M)
```

### **ips{running-rep-abc}dns-except**

DNS domain exception.

Syntax

```
dns-except DOMAINNAME
```

### **ips{running-rep-abc}filter**

Add a reputation filter rule.

Syntax

```
filter ALLGROUPNAME(enable [threshold [XACTIONSETNAME]]) |
(disable)
Valid entries:
enable Enable filter rule
THRESHOLD Set threshold (0-100)
XACTIONSETNAME Apply action set name
disable Disable filter rule
```

### **ips{running-rep-abc}ip-except**

Add IP address exception.

Syntax

```
ip-except SOURCEIP DESTINATIONIP
SOURCEIP A.B.C.D or A.B.C.D/M or X:X::X:X or X:X::X:X/M
DESTINATIONIP A.B.C.D or A.B.C.D/M or X:X::X:X or X:X::X:X/M
```

### **security-policy-reset**

Resets the IPS security policy to the default values.

## Syntax

security-policy-reset

## running-segments-segmentX Context Commands

Immediate Commit Feature. Changes take effect immediately.

### ips{running-segments-segment0}description

Apply segment description.

Syntax

```
description TEXT
```

### ips{running-segments-segment0}display

Display a segment configuration.

Syntax

```
display
```

### ips{running-segments-segment0}high-availability

Intrinsic HA Layer 2 Fallback action block or permit.

Syntax

```
high-availability (block|permit)
block  Enable block all
permit Enable permit all
```

### ips{running-segments-segment0}link-down

Link down synchronization mode.

Syntax

```
link-down breaker [wait-time WAIT-TIME]
link-down hub
link-down wire [wait-time WAIT-TIME]
Valid entries:
breaker      Enable breaker action
hub          Enable hub action
wire         Enable wire action
WAIT-TIME    Time to wait before synchronizing in seconds
```

### ips{running-segments-segment0}restart

Restart both ethernet ports of segment.

Syntax

```
restart
```

### ips{running-segments-segment0}sflow

Configure sFlow packet export.

## Syntax

```
sflow enable sample-rate [SAMPLE-RATE]|disable
```

**running-services Context Commands**

Immediate Commit Feature. Changes take effect immediately.

**Syntax**

```
ips{}edit
ips{running}services
Entering Immediate Commit Feature. Changes take effect immediately.
ips{running-services}
Valid entries at this position are:
    display          Display all services
    help             Display help information
    service          Edit a service
ips{running-services}help service
Edit a service
Syntax: service SERVICE
    service          Edit a service
    SERVICE          Service name

ips{running-services}service portmapper
ips{running-services-portmapper}
Valid entries at this position are:
    delete          Delete file or configuration item
    display          Display service configuration
    help            Display help information
    port            Add port(s) to service

ips{running-services-portmapper}display
# DEFAULT ENTRIES
port tcp 111
port tcp 32770 to 32779
port udp 111
port udp 32770 to 32779
exit
ips{running-services-portmapper}help port
Add port(s) to service
Syntax: port tcp PORT [to LAST-PORT]
        port udp PORT [to LAST-PORT]
    port            Add port(s) to service
    tcp            TCP
    PORT           Port number
    to             Enter range of ports
    LAST-PORT      Last port of range
    udp           UDP

ips{running-services-portmapper}help delete port
Delete port(s) from service
Syntax: delete port tcp PORT [to LAST-PORT]
        delete port udp PORT [to LAST-PORT]
    delete          Delete file or configuration item
    port            Delete port(s) from service
    tcp            TCP
    PORT           Port number
    to             Enter range of ports
```

LAST-PORT	Last port of range
udp	UDP

## Notes

- You cannot create new services.
- You cannot delete services.
- You cannot delete the set of default ports assigned to services.
- You can add additional ports to a service.
- You can delete user-added ports from a service.
- TCP or UDP option is available depending on the service (some services are TCP only).

## ips{running-services}display

Display service(s).

Syntax

```
display service (all|SERVICENAME)
```

## ips{running-services}service

Edit a service.

Syntax

```
service SERVICENAME
```

## running-services-X Context Commands

Immediate Commit Feature. Changes take effect immediately.

## ips{running-services-myservice1}delete

Delete service parameters.

Syntax

```
delete icmp (all|NAME|NUMBER)
delete icmpv6 (all|NAME|NUMBER)
delete port tcp PORT [to LASTPORT]
delete port udp PORT [to LASTPORT]
delete port tcp all
delete port udp all
delete protocol (all|PROTONUM)
delete service (all|SERVICENAME)
Valid entries:
icmp      Delete ICMPv4
icmpv6    Delete ICMPv6
port      Delete port(s)
protocol  Delete packet protocol number(s)
service   Delete member service
```

## ips{running-services-myservice1}port

Apply TCP or UDP port number.

## Syntax

```
port tcp PORT [to LASTPORT]
port udp PORT [to LASTPORT]
Valid entries:
tcp          Apply TCP
PORT         Apply port number
to           Set port range to
LAST-PORT   Apply last port of range
udp          Apply UDP
```

**running-snmp Context Commands**

Immediate Commit Feature. Changes take effect immediately.

**ips{running-snmp}authtrap**

Enable or disable SNMP authentication failure trap.

## Syntax

```
authtrap (enable|disable)
```

**ips{running-snmp}community**

Configure SNMP read-only community.

## Syntax

```
community COMMUNITY [SOURCE]
COMMUNITY      Text to identify SNMP system community
SOURCE         IP (A.B.C.D|X:X::X:X), subnet (A.B.C.D/M|X:X::X:X/M), or "default"
default        allow any IPv4/6 source
```

**ips{running-snmp}delete**

Delete file or configuration item.

## Syntax

```
delete community (COMMUNITY|all)
delete trapsession ((A.B.C.D|X:X::X:X|FQDN) ver VERSION) |all)
delete username (USERNAME|all)
Valid entries:
community     Delete SNMP read-only community
trapsession   Delete a configured trap session
username      Delete a configured user
```

**ips{running-snmp}engineID**

Configure SNMPv3 engine ID.

## Syntax

```
engineID ENGINE-ID
ENGINE-ID      SNMPv3 Engine ID (1-32 hex octets, ex: 0x800012ef0302a11aab33f4)
```

**ips{running-snmp}snmp**

Enable or disable SNMP.



## Syntax

```
snmp (enable|disable)
```

**ips{running-snmp}trapdest**

Configure SNMP v2c or v3 trap destinations.

## Syntax

```
trapdest HOST [port PORT] ver 2c COMMUNITY [inform]
trapdest HOST [port PORT] ver 3 USERNAME [inform]
trapdest HOST [port PORT] ver 3 USERNAME authtype AUTHTYPE AUTHPASS [inform]
trapdest HOST [port PORT] ver 3 USERNAME authtype AUTHTYPE AUTHPASS privproto
```

## Valid entries:

HOST	IP address or DNS host name
port	Configure SNMP port
PORT	SNMP port (default 162)
ver	Configure SNMP version (2c, or 3)
2c	SNMPv2c
COMMUNITY	Text to identify SNMP system community
inform	Send information message instead of a trap
3	SNMPv3
USERNAME	Text to identify USM user name (for authentication/privacy)
level	Configure security level (noAuthNoPriv authNoPriv authPriv)
noAuthNoPriv	No authentication, no privacy
authNoPriv	Authentication, no privacy
authtype	Configure authentication type (MD5 SHA)
AUTHTYPE	Authentication type
Possible values for AUTHTYPE are:	
MD5	Message Digest 5
SHA	Secure Hash Algorithm
AUTHPASS	Authentication passphrase - must be at least 8 characters
authPriv	Authentication and privacy
privproto	Configure privacy protocol (DES AES)
PRIVPROTO	Privacy protocol
Possible values for PRIVPROTO are:	
DES	Data Encryption Security
AES	Advanced Encryption Security
PRIVPASS	Optional privacy passphrase - must be at least 8 characters

**ips{running-snmp}username**

Configure SNMPv3 USM read-only user.

## Syntax

```
username USERNAME
username USERNAME authtype AUTHTYPE AUTHPASS
username USERNAME authtype AUTHTYPE AUTHPASS privproto PRIVPROTO [PRIVPASS]
```

## Valid entries:

USERNAME	Text to identify USM user name (for authentication/privacy)
level	Configure security level (noAuthNoPriv authNoPriv authPriv)
noAuthNoPriv	No authentication, no privacy
authNoPriv	Authentication, no privacy
authtype	Configure authentication type (MD5 SHA)
AUTHTYPE	Authentication type
Possible values for AUTHTYPE are:	

MD5	Message Digest 5
SHA	Secure Hash Algorithm
AUTHPASS	Authentication passphrase - must be at least 8 characters
authPriv	Authentication and privacy
privproto	Configure privacy protocol (DES AES)
PRIVPROTO	Privacy protocol
Possible values for PRIVPROTO are:	
DES	Data Encryption Security
AES	Advanced Encryption Security
PRIVPASS	Optional privacy passphrase - must be at least 8 characters

## running-sslinsp Context Commands

Use the **ssl-insp** context to specify the SSL sessions you want to inspect and to enable or disable SSL inspection.



### Note

While SSL inspection is disabled, you can configure SSL inspection to specify the SSL sessions you want to inspect.

Syntax

```
ips{running-sslinsp}
```

### ips{running-sslinsp}enable

Use the **enable** command to begin inspecting SSL sessions based on the configuration you specify. While SSL inspection is disabled, you can configure SSL inspection, but no sessions are inspected.

To enable SSL inspection, the TPS device must be licensed for SSL inspection. Use the LSM to verify the SSL inspection license.

Syntax

```
ips{running-sslinsp} [enable|disable]
```

### ips{running-sslinsp}log sslInspection

Use the **log sslInspection** command to save SSL inspection logging information to a particular notification contact. By default, the TPS device saves SSL inspection log information to the "Management Console" notification contact which is available for display from the LSM and is found in the *sslInspection.log* on the device.



### Important

To generate SSL inspection log entries, enable logging on the SSL server for troubleshooting purposes only. By default, an SSL server does not generate logging information. See [ips{running-sslinsp}server](#).

Syntax

```
log sslInspection CONTACT-NAME [ALL|none]
```

### ips{running-sslinsp}profile

Add, edit, or delete an SSL inspection profile. An SSL inspection *profile* describes the encrypted traffic that you want to protect using one or more server policies. A *server policy* consists of an SSL server, and any source IP address exceptions. When you add or edit an SSL inspection profile, the CLI context changes to that profile. From the profile subcontext, view and change the default settings for that profile, for example, to add a server policy.

**Note**

To exit the edit configuration mode from any context, type the **!** command and press Enter.

When you create a new profile, you must add a policy named `mypolicy` to the profile and assign an SSL inspection server named **mysslserver** to the policy. The SSL server specifies the range of server IP addresses you want to protect along with your SSL server configuration details.

You can also update the policy to specify any source IP addresses that you do not want to inspect. Secure sessions between the server and the specified source IP addresses are not inspected.

Syntax

```
[delete] profile PROFILENAME
```

**Related commands**

COMMAND	DESCRIPTION
<i>ips{running-certificates}certificate</i>	Import the certificate from your web server into the local keystore on the device.
<i>ips{running-certificates}private-key</i>	Import the private key from your web server into the local keystore on the device.
<i>ips{running-vsegs-VSEG_NAME}ssl-profile</i>	Update the virtual segment to assign the SSL inspection profile.
<i>ips{running-sslinsp}server</i>	Add an SSL server with its assigned security certificate and private key.

**ips{running-sslinsp}server**

Add or edit an SSL server to specify the SSL server configuration you want the TippingPoint security device to proxy, including the SSL service. You must specify the type of secure traffic that is accepted on the SSL detection port. For example, if the server accepts POP3S traffic on port 2000, add an SSL server with a Detection Port of 2000 and a Decrypted Service of POP3. From the server subcontext, you can view and change the default settings for that server. When you finish, assign the SSL server to an SSL inspection profile. Enable logging on the SSL server for troubleshooting purposes only.

**Note**

To exit the edit configuration mode from any context, type the **!** command and press Enter.

The `protocol SSL-PROTOCOL` and `cipher-suite SSL-PROTOCOL` options have "auto-" commands to allow selection of cipher suites by protocol or protocols by cipher suite, respectively. Use the "auto-" command to add or delete ciphers based on what protocol is selected and what it supports.

By default, the IP address and device certificate for the server are not defined, and must be specified separately. Specify the **IP address** of your web server by entering up to 8 IPv4 addresses (separated by commas), or by specifying a CIDR range, such as 192.168.0.1/24. Specify the **device certificate** that the TPS device uses to decrypt and encrypt HTTP traffic across the specified range of server IP addresses. Make sure that the corresponding private key is assigned to the device certificate.

Syntax

```
[delete] server SERVERNAME
```

## Related commands

COMMAND	DESCRIPTION
<i>ips{running-certificates}certificate</i>	Import the certificate from your web server into the local keystore on the device.
<i>ips{running-certificates}private-key</i>	Import the private key from your web server into the local keystore on the device.
<i>ips{running-vsegs-VSEG_NAME}ssl-profile</i>	Update the virtual segment to assign the SSL inspection profile.
<i>ips{running-sslinsp}profile</i>	Assign the SSL server to an SSL inspection profile.

## running-traffic-management Context Commands

Immediate Commit Feature. Changes take effect immediately.

When you create a traffic profile and add traffic filters, more options become available.

### ips{running-trafmgmt}delete

Delete a traffic-management profile.

Syntax

```
delete PROFILE
```

### ips{running-trafmgmt}profile

Create or enter traffic-management profile context. When traffic filters are added to a profile, more options become available.

Syntax

```
profile NEWTRAFPROFNAME
profile TRAFPROFNAME
```

### ips{running-trafmgmt}rename

Rename traffic-management profile.

Syntax

```
rename profile TRAFPROFNAME NEWTRAFPROFNAME
```

## running-virtual-segments Context Commands

Physical segments have predefined virtual segments. CIDRs and profiles are applied to the virtual segment. Virtual segments enable further management of VLAN traffic. Use this context to define an individual virtual segment.

### Syntax

```
ips{running}virtual-segments
ips{running-vsegs}?
Valid entries at this position are:
delete          Delete file or configuration item
help            Display help information
rename          Rename virtual-segment
```

<code>virtual-segment</code>	Create or enter virtual-segment context
<code>display</code>	Display file or configuration item

## Notes

- A maximum of 64 virtual segments can be configured.
- Each virtual segment name must be unique.

### `ips{running-vsegs}delete virtual-segment`

Delete a virtual-segment context. The position value for any higher virtual segments will be renumbered. Only user-created virtual segments can be deleted.

Syntax

```
delete virtual-segment VSEGNAME
```

### `ips{running-vsegs}display`

Display file or configuration item.

Syntax

```
display {xml}
```

### `ips{running-vsegs}rename virtual-segment`

Rename the virtual segment. Each virtual segment name must be unique.

Syntax

```
rename virtual-segment VSEGNAME NEWVSEGNAME
```

### `ips{running-vsegs}virtual-segment`

Create or enter virtual-segment context.

Syntax

```
virtual-segment VSEGNAME
virtual-segment NEWVSEGNAME
```

## running-virtual-segment Context Commands

Physical segments have predefined virtual segments. CIDRs and profiles are applied to the virtual segment. Virtual segments enable further management of VLAN traffic.

## Syntax

```
ips{running-vsegs}virtual-segment segmentname
ips{running-vsegs-segmentname}?
Valid entries at this position are:
  bind          Bind physical ports to virtual segment
  delete        Delete file or configuration item
  description    Update virtual segment description
  display        Display file or configuration item
  dst-address    Add destination address to a virtual segment
  help          Display help information
```

<code>ips-profile</code>	Virtual segment ips profile
<code>move</code>	Move virtual segment priority position
<code>reputation-profile</code>	Virtual segment reputation profile
<code>src-address</code>	Add source address to a virtual segment
<code>ssl-profile</code>	Virtual segment SSL profile
<code>traffic-profile</code>	Virtual segment traffic-management profile
<code>vlan-id</code>	Add vlan id or range to virtual segment

## Notes

- A maximum of 64 virtual segments can be configured.
- Each virtual segment name must be unique.
- You can configure up to 4094 VLAN IDs per virtual segment.
- Each VLAN ID in a range counts individually. For example, `vlan-id range 1 5` counts as five IDs.
- A CIDR counts as a single address. For example, `192.168.1.0/24` counts as one address.
- At least one traffic criteria must be defined for each virtual segment. Traffic criteria can be VLAN IDs, src-addresses, and dst-addresses.
- If no physical ports are defined on a virtual segment, the virtual segment will apply to all physical ports.
- If no VLAN IDs are defined on a virtual segment, all VLAN IDs are included.
- If no source addresses are defined, all source addresses are included. If no destination addresses are defined, all destination addresses are included.
- Position values must remain contiguous across all defined virtual segments, so there should never be a gap in the sequence.
- Position values start with 1 and increment by one for each new virtual segment added. The highest possible position value that can be configured is 64.

## **ips{running-vsegs}bind**

Bind physical ports to virtual-segment.

Syntax

```
bind in-port PHYSPORT out-port PHYSPORT
```

## **ips{running-vsegs}delete bind**

Delete a port-pair association from this virtual segment.

Syntax

```
delete bind in-port EXISTING_PHYSPORT out-port EXISTING_PHYSPORT
```

## **ips{running-vsegs}description**

Add or edit the description of a virtual segment.

Syntax

```
description TEXT
```

## **ips{running-vsegs}display**

Display file or configuration item.

Syntax

```
display {xml}
```

### **ips{running-vsegs}dst-address**

Associate an IPv4 or IPv6 destination address or subnet, in CIDR format, with this virtual segment.

Syntax

```
dst-address ABCD|ABCDM|XXXX|XXXXM
```

Host IP addresses will include the submasks. For example, entering 192.168.1.1 will display as 192.168.1.1/32. You can associate a maximum of 250 destination addresses.

### **ips{running-vsegs}delete dst-address**

Delete an IPv4 or IPv6 destination address or subnet associated with this virtual segment.

Syntax

```
delete dst-address all|ABCD|ABCDM|XXXX|XXXXM
```

If the all keyword is specified, all destination addresses are deleted from this virtual segment. Otherwise, specify an address.



#### **Note**

Host addresses are stored with a netmask of /32 or /128 for IPv4 or IPv6, respectively. Any address deletion requires that the netmask be supplied. For example, delete dst-address 192.168.1.1/32.

### **ips{running-vsegs-VSEG\_NAME}ips-profile**

Associate an existing IPS security profile with this virtual segment.

Syntax

```
ips-profile PROFILENAME
```

### **ips{running-vsegs-VSEG\_NAME}delete ips-profile**

Delete an existing IPS security profile associated with this virtual segment.

Syntax

```
delete ips-profile PROFILENAME
```

### **ips{running-vsegs-VSEG\_NAME}reputation-profile**

Associate an existing reputation profile with this virtual segment.

Syntax

```
reputation-profile PROFILENAME
```

### **ips{running-vsegs-VSEG\_NAME}delete reputation-profile**

Delete an existing reputation profile associated with this virtual segment.

Syntax

```
delete reputation-profile PROFILENAME
```

### **ips{running-vsegs-VSEG\_NAME}ssl-profile**

Edit the virtual segment to assign an SSL inspection profile.

Syntax

```
ssl-profile PROFILENAME
```

### **Related commands**

COMMAND	DESCRIPTION
<a href="#"><i>ips{running-sslinsp}profile</i></a>	Create an SSL-inspection profile.

### **ips{running-vsegs-VSEG\_NAME}delete ssl-profile**

Delete an existing SSL inspection profile associated with this virtual segment.

Syntax

```
delete ssl-profile PROFILENAME
```

### **ips{running-vsegs}move**

Add or edit the description of a virtual segment.

Syntax

```
move after VSEGNAME
move before VSEGNAME
move to position VALUE
```

Only user-created virtual segments can be moved.

Position values must remain contiguous across all defined virtual segments, so there should never be a gap in the sequence. Virtual segments in between the segment you are moving and the target may be renumbered. A virtual segment cannot be moved to a lower priority than a system-defined virtual segment.

VALUE must be an unsigned, non-zero integer number.

If VSEGNAME is the name of this virtual segment, the position value remains unchanged.

### **ips{running-vsegs}src-address**

Associate an IPv4 or IPv6 source address or subnet, in CIDR format, with this virtual segment.

Syntax

```
src-address ABCD|ABCDM|XXXX|XXXXM
```

Host IP addresses will include the submasks. For example, entering 192.168.1.1 will display as 192.168.1.1/32. You can associate a maximum of 250 source addresses.

### **ips{running-vsegs}delete src-address**

Delete an IPv4 or IPv6 source address or subnet associated with this virtual segment.

Syntax



```
delete src-address all | ABCD | ABCDM | XXXX | XXXXM
```

If the `all` keyword is specified, all source addresses are deleted from this virtual segment. Otherwise, specify an address.



#### Note

Host addresses are stored with a netmask of /32 or /128 for IPv4 or IPv6, respectively. Any address deletion requires that the netmask be supplied. For example, `delete src-address 192.168.1.1/32`.

### **ips{running-vsegs-vsegsname}vlan-id**

Associate a single VLAN ID or a range of consecutive VLAN IDs with this virtual-segment.

#### Syntax

```
vlan-id VLANID_NUMBER
vlan-id range MINADDR MAXADDR
```

This command can only be used after an individual virtual segment is defined.

Valid IDs can range from 1–4094. All 4094 VLAN IDs can be used.

### **ips{running-vsegs}delete vlan-id**

Delete a single VLAN ID or a range of consecutive VLAN IDs associated with this virtual-segment.

#### Syntax

```
delete vlan-id all | EXISTING_VLANIDNUMBER
delete vlan-id range MINADDR MAXADDR
```

If the `all` keyword is specified, all VLAN IDs get deleted, including any VLAN ranges. Otherwise, specify the VLAN ID to be deleted.

## **running-vlan-translations Context Commands**

Adds or removes a VLAN translation setting. Use the **auto-reverse** flag to automatically create a reverse VLAN translation.

#### Syntax

```
ips{running-vlan-translations}help
Valid commands are:
  add-translation PORT VLANIN VLANOUT [auto-reverse]
  delete-translation PORT VLANIN
  help [full|COMMAND]
```

### **ips{running-vlan-translations}**

Adds or removes a VLAN translation setting. The IPS creates a separate VLAN translation rule for each port you want to translate. A maximum of 8000 VLAN translation rules can be defined on a 440T or 2200T TPS. If the number of VLAN translation rules you want to commit exceed the specified limit, the device does not commit your changes.

Use the **auto-reverse** flag to automatically create a reverse VLAN translation.

#### Syntax

```
add-translation <PORT> <incoming VLAN ID> <outgoing VLAN ID> [auto-reverse]
```

```
delete-translation <PORT> <incoming VLAN ID>
```