Legal and notice information

© Copyright 2017 Trend Micro

Trend Micro Incorporated makes no warranty of any kind with regard to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Trend Micro Incorporated shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

This document contains proprietary information, which is protected by copyright. No part of this document may be photocopied, reproduced, or translated into another language without the prior written consent of Trend Micro Incorporated. The information is provided “as is” without warranty of any kind and is subject to change without notice. The only warranties for Trend Micro Incorporated products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Trend Micro Incorporated shall not be liable for technical or editorial errors or omissions contained herein.

TippingPoint, the TippingPoint logo, and Digital Vaccine are trademarks or registered trademarks of Trend Micro Incorporated. All other company and/or product names may be trademarks or registered trademarks of their respective owners. This document contains confidential information, trade secrets or both, which are the property of Trend Micro Incorporated. No part of this documentation may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from Trend Micro Incorporated or one of its subsidiaries.

All other company and product names may be trademarks of their respective holders.

TippingPoint Threat Protection System Command Line Interface Reference
Publication Part Number: 5900-4128
# Contents

**About this guide**......................................................................................................................................1

- Target audience...................................................................................................................................... 1
- Related documentation...........................................................................................................................2
- Conventions............................................................................................................................................ 2
- Product support...................................................................................................................................... 3
- New and changed information in this edition.........................................................................................3

**Command Line Interface**........................................................................................................................ 7

- CLI syntax...............................................................................................................................................7
- Shortcut navigation keys........................................................................................................................ 8
- Hierarchical context................................................................................................................................ 9
- Help.......................................................................................................................................................10
- Command modes................................................................................................................................. 10
  - Root command mode........................................................................................................................ 11
  - Edit configuration mode.................................................................................................................... 12
- Configuration file versions.................................................................................................................... 14
- Utilities................................................................................................................................................ 14
  - Display............................................................................................................................................. 15
  - Show................................................................................................................................................ 15

**Global commands**................................................................................................................................. 16

- commit..................................................................................................................................................16
- display.................................................................................................................................................. 16
- edit......................................................................................................................................................... 17
- help...................................................................................................................................................... 18
Root commands

boot
chpasswd
clear
date
debug
delete
delete auxdv
display
display conf
display-config
display-config
edit
halt
help
high-availability
keystore
list
log-configure
logout
master-key
ping
ping6
quarantine
reboot

Threat Protection System Command Line Interface Reference
reports................................................................................................................................................... 41
resize.....................................................................................................................................................42
save-config............................................................................................................................................42
service-access...................................................................................................................................... 43
set......................................................................................................................................................... 43
setup..................................................................................................................................................... 44
show......................................................................................................................................................44
  show aaa............................................................................................................................................47
  show auxdv........................................................................................................................................ 49
  show date...........................................................................................................................................49
  show dns...........................................................................................................................................49
  show filter...........................................................................................................................................49
  show health.......................................................................................................................................50
  show high-availability.........................................................................................................................52
  show interface....................................................................................................................................52
  show key............................................................................................................................................53
  show license.......................................................................................................................................54
  show log-file.......................................................................................................................................54
    show log-file boot................................................................. show log-file FILE_NAME.......................... 55
    show log-file FILE_NAME stat.......................................... 58
    show log-file summary...................................................... 59
  show mfg-info.....................................................................................................................................59
  show np engine..................................................................................................................................60
  show np general statistics.................................................... 60
  show np mcfilt-rule-stats...................................................... 61
  show np protocol-mix.......................................................... 61
  show np reassembly............................................................. 62
show np rule-stats........................................................................................................................................62
show np softlinx.........................................................................................................................................63
show np tier-stats.......................................................................................................................................63
show quarantine-list................................................................................................................................64
show reports...........................................................................................................................................65
show service...........................................................................................................................................65
show slot................................................................................................................................................66
show sms................................................................................................................................................66
show snmp.................................................................................................................................................66
show ssl-inspection congestion..................................................................................................................67
show system connections..........................................................................................................................67
show system processes.............................................................................................................................68
show system queue-stats..........................................................................................................................69
show system statistics...............................................................................................................................69
show system usage..................................................................................................................................69
show system virtual-memory....................................................................................................................70
show system xms memory..........................................................................................................................70
show terminal..........................................................................................................................................71
show traffic-file.......................................................................................................................................71
show tse....................................................................................................................................................72
  show tse connection-table.......................................................................................................................73
show user-disk.........................................................................................................................................73
show users.................................................................................................................................................73
show version..........................................................................................................................................74
show virtual segments.............................................................................................................................74

sms..........................................................................................................................................................74
snapshot create.......................................................................................................................................75
snapshot list.............................................................................................................................................75
snapshot remove......................................................................................................................................76
snapshot restore.................................................................76

tcpdump...................................................................................76

tech-support-report............................................................77

traceroute................................................................................78

traceroute6.............................................................................78

user-disk...............................................................................78

Log configure commands.......................................................80

display..................................................................................80

email.....................................................................................81

log-file-size...........................................................................81

log-storage..........................................................................82

log-test................................................................................82

rotate....................................................................................83

Edit running configuration commands....................................84

Edit context commands.......................................................84

aaa.......................................................................................84

actionsets............................................................................85

autodv................................................................................85

blockedStreams.................................................................86

certificates.........................................................................87

debug...................................................................................87

delete...................................................................................88

display...............................................................................88

dns......................................................................................88

gen....................................................................................89

high-availability.................................................................90
interface .......................................................................................................................... 90
ips ......................................................................................................................................... 91
log ....................................................................................................................................... 92
notifycontacts .......................................................................................................................... 93
ntp ....................................................................................................................................... 93
reputation .............................................................................................................................. 94
security-policy-reset ............................................................................................................... 95
segmentX .............................................................................................................................. 95
services ................................................................................................................................. 96
snmp ..................................................................................................................................... 96
ssl-inspection ......................................................................................................................... 97
traffic-management ............................................................................................................... 98
virtual-segments .................................................................................................................. 98
Contexts and related commands ............................................................................................ 99
running-aaa Context Commands .......................................................................................... 99
ips{running-aaa}delete ........................................................................................................... 99
ips{running-aaa}display ......................................................................................................... 99
ips{running-aaa}ldap-group ................................................................................................. 100
ips{running-aaa}ldap-schema .............................................................................................. 100
ips{running-aaa}login ............................................................................................................ 100
ips{running-aaa}password .................................................................................................... 101
ips{running-aaa}radius-group .............................................................................................. 102
ips{running-aaa}remote-login-group .................................................................................... 102
ips{running-aaa}role ............................................................................................................ 102
ips{running-aaa}user ............................................................................................................ 102
ips{running-aaa}user-group ................................................................................................. 103
aaa debug ldap test-bind ....................................................................................................... 103
aaa debug ldap authenticate-user ........................................................................................ 104
aaa debug ldap lookup-user .................................................................................................. 104
running-aaa-ldap-group-X Context Commands .................................................................... 105
ips{running-aaa-ldap-group-mygroup1}base-dn................................................................. 105
ips{running-aaa-ldap-group-mygroup1}bind-dn................................................................. 106
ips{running-aaa-ldap-group-mygroup1}delete................................................................. 106
ips{running-aaa-ldap-group-mygroup1}port..................................................................... 106
ips{running-aaa-ldap-group-mygroup1}retries................................................................. 106
ips{running-aaa-ldap-group-mygroup1}server................................................................. 107
ips{running-aaa-ldap-group-mygroup1}timeout............................................................... 107
ips{running-aaa-ldap-group-mygroup1}tls....................................................................... 107
running-aaa-radius-group-X Context Commands.......................................................... 107
ips{running-aaa-radius-group-2}default-usergroup........................................................ 108
ips{running-aaa-radius-group-2}delete........................................................................... 108
ips{running-aaa-radius-group-2}auth-type..................................................................... 108
ips{running-aaa-radius-group-2}retries......................................................................... 109
ips{running-aaa-radius-group-2}server......................................................................... 109
running-actionsets Context Commands.......................................................................... 109
ips{running-actionsets}actionset.................................................................................... 109
ips{running-actionsets}rename....................................................................................... 109
running-actionsets-X Context Commands....................................................................... 110
ips{running-actionsets-myactionset1}action.................................................................... 110
ips{running-actionsets-myactionset1}allow-access......................................................... 110
ips{running-actionsets-myactionset1}bytes-to-capture................................................... 110
ips{running-actionsets-myactionset1}delete................................................................... 111
ips{running-actionsets-myactionset1}http-block............................................................ 111
ips{running-actionsets-myactionset1}http-redirect......................................................... 111
ips{running-actionsets-myactionset1}http-showdesc...................................................... 111
ips{running-actionsets-myactionset1}limit-quarantine.................................................... 112
ips{running-actionsets-myactionset1}packet-trace.......................................................... 112
ips{running-actionsets-myactionset1}priority.................................................................. 112
ips{running-actionsets-myactionset1}quarantine.............................................................. 112
ips{running-actionsets-myactionset1}tcp-reset.............................................................. 113
ips{running-actionsets-myactionset1}threshold
ips{running-actionsets-myactionset1}verbosity

running-autodv Context Commands
ips{running-autodv}calendar
ips{running-autodv}delete
ips{running-autodv}disable
ips{running-autodv}enable
ips{running-autodv}list
ips{running-autodv}periodic
ips{running-autodv}proxy
ips{running-autodv}proxy-password
ips{running-autodv}proxy-username
ips{running-autodv}update

running-autodv-periodic Context Commands
ips{running-autodv-periodic}day
ips{running-autodv-periodic}period
ips{running-autodv-periodic}time

running-blockedStreams Context Commands
ips{running-blockedStreams}flushallstreams
ips{running-blockedStreams}flushstreams
ips{running-blockedStreams}list

running-certificates Context Commands
ips{running-certificates}certificate
ips{running-certificates}ca-certificate
ips{running-certificates}delete
ips{running-certificates}display
ips{running-certificates}private-key

running-debug Context Commands
ips{running}debug

running-dns Context Commands
ips{running-dns}delete................................................................................................................... 121
ips{running-dns}domain-name........................................................................................................ 122
ips{running-dns}domain-search.................................................................................................... 122
ips{running-dns}name-server....................................................................................................... 122
ips{running-dns}proxy.................................................................................................................... 123
running-gen Context Commands.................................................................................................. 123
ips{running-gen}delete................................................................................................................... 123
ips{running-gen}ephemeral-port-range.......................................................................................... 123
ips{running-gen}host...................................................................................................................... 124
ips{running-gen}https..................................................................................................................... 124
ips{running-gen}ssh....................................................................................................................... 124
ips{running-gen}tls......................................................................................................................... 124
ips{running-gen}timezone.............................................................................................................. 125
running-high-availability Context Commands............................................................................. 125
ips{running-high-availability}disable............................................................................................... 125
ips{running-high-availability}enable............................................................................................... 126
ips{running-high-availability}encryption......................................................................................... 126
ips{running-high-availability}partner............................................................................................... 126
running-inspection-bypass Context Commands........................................................................... 126
ips{running-inspection-bypass-rule-myrule1}eth............................................................................ 129
ips{running-inspection-bypass-rule-myrule1}ip-proto.................................................................... 129
ips{running-inspection-bypass-rule-myrule1}vlan-id...................................................................... 130
running-interface Context Commands........................................................................................... 131
ips{running}interface nM................................................................................................................ 131
ips{running}interface mgmt............................................................................................................ 131
running-ips Context Commands.................................................................................................... 132
ips{running-ips}afc-mode............................................................................................................... 132
ips{running-ips}afc-severity............................................................................................................ 132
ips{running-ips}asymmetric-network.............................................................................................. 133
ips{running-ips}connection-table.................................................................................................... 133
running-ntp Context Commands......................................................................................................142
ips{running-ntp}delete....................................................................................................................143
ips{running-ntp}key........................................................................................................................ 143
ips{running-ntp}ntp.........................................................................................................................143
ips{running-ntp}polling-interval...................................................................................................... 144
ips{running-ntp}server....................................................................................................................144
running-rep Context Commands......................................................................................................144
ips{running-rep}delete....................................................................................................................144
ips{running-rep}group.................................................................................................................... 145
ips{running-rep}nxdomain-response..............................................................................................145
ips{running-rep}profile....................................................................................................................146
ips{running-rep}rename................................................................................................................. 146
running-rep-X (group X) Context Commands ..................................................................................147
ips{running-rep-1}delete................................................................................................................ 147
ips{running-rep-1}description.........................................................................................................147
ips{running-rep-1}domain.............................................................................................................. 147
ips{running-rep-1}ip........................................................................................................................148
running-rep-X (profile X) Context Commands................................................................................. 148
ips{running-rep-abc}action-when-pending..................................................................................... 148
ips{running-rep-abc}check-destination-address............................................................................ 148
ips{running-rep-abc}check-source-address................................................................................... 148
ips{running-rep-abc}delete.............................................................................................................149
ips{running-rep-abc}dns-except.....................................................................................................149
ips{running-rep-abc}filter................................................................................................................149
ips{running-rep-abc}ip-except........................................................................................................150
security-policy-reset..........................................................................................................................150
running-segmentX Context Commands...........................................................................................150
ips{running-segment0}description................................................................................................. 150
ips{running-segment0}high-availability..........................................................................................150
ips{running-segment0}link-down....................................................................................................151
ips{running-segment0}restart.........................................................................................................151
running-services Context Commands..........................................................................................151
ips{running-services}display......................................................................................................153
ips{running-services}service......................................................................................................153
running-services-X Context Commands....................................................................................153
ips{running-services-myservice1}delete..................................................................................153
ips{running-services-myservice1}port......................................................................................154
running-snmp Context Commands.............................................................................................154
ips{running-snmp}authtrap..........................................................................................................154
ips{running-snmp}community......................................................................................................155
ips{running-snmp}delete...............................................................................................................155
ips{running-snmp}engineID.........................................................................................................155
ips{running-snmp}snmp...............................................................................................................156
ips{running-snmp}trapdest..........................................................................................................156
ips{running-snmp}username.......................................................................................................157
running-sslinsp Context Commands........................................................................................158
ips{running-sslinsp}enable..........................................................................................................158
ips{running-sslinsp}log sslInspection.........................................................................................158
ips{running-sslinsp}profile.........................................................................................................159
ips{running-sslinsp}server..........................................................................................................160
running-traffic-management Context Commands......................................................................163
ips{running-trafmgmt}delete.......................................................................................................163
ips{running-trafmgmt}profile......................................................................................................164
ips{running-trafmgmt}rename.....................................................................................................165
running-virtual-segments Context Commands..........................................................................165
ips{running-vsegs}delete virtual-segment..................................................................................166
ips{running-vsegs}display..........................................................................................................166
ips{running-vsegs}rename virtual-segment................................................................................166
ips{running-vsegs}virtual-segment.............................................................................................166
running-virtual-segment Context Commands............................................................................167
ips{running-vsegs}bind.................................................................................................................. 168
ips{running-vsegs}delete bind........................................................................................................ 168
ips{running-vsegs}description........................................................................................................ 168
ips{running-vsegs}display.............................................................................................................. 168
ips{running-vsegs}dst-address...................................................................................................... 169
ips{running-vsegs}delete dst-address........................................................................................... 169
ips{running-vsegs-VSEG_NAME}ips-profile.................................................................................. 169
ips{running-vsegs-VSEG_NAME}delete ips-profile......................................................................... 169
ips{running-vsegs-VSEG_NAME}reputation-profile....................................................................... 170
ips{running-vsegs-VSEG_NAME}delete reputation-profile............................................................ 170
ips{running-vsegs-VSEG_NAME}ssl-profile.................................................................................. 170
ips{running-vsegs-VSEG_NAME}delete ssl-profile......................................................................... 171
ips{running-vsegs}move................................................................................................................ 171
ips{running-vsegs}src-address...................................................................................................... 171
ips{running-vsegs}delete src-address........................................................................................... 172
ips{running-vsegs}vlan-id............................................................................................................... 172
ips{running-vsegs}delete vlan-id................................................................................................... 172
running-vlan-translations Context Commands................................................................................. 173
ips{running-vlan-translations}........................................................................................................ 173
About this guide

The Threat Protection System (TPS) enables you to configure and manage the TPS device using the Command-line Interface (CLI).

This section covers the following topics:

- **Target Audience** on page 1
- **Related Documentation** on page 2
- **Document Conventions** on page 2
- **Customer Support** on page 3

Target audience

The intended audience includes technicians and maintenance personnel responsible for installing, configuring, and maintaining TippingPoint security systems and associated devices.

Users should be familiar with the following concepts:

- Basic networking
- Network security
- Routing
- TCP/IP
- UDP
- ICMP
- RADIUS
- TACACS+
- Ethernet
- Network Time Protocol (NTP)
- Secure Sockets Layer (SSL)
- Simple Network Time Protocol (SNTP)
- Simple Mail Transport Protocol (SMTP)
- Simple Network Management Protocol (SNMP)
Related documentation

A complete set of documentation for your product is available on the TippingPoint Threat Management Center (TMC) at: https://tmc.tippingpoint.com. The documentation generally includes installation and user guides, command-line interface (CLI) references, safety and compliance information, and release notes.

Conventions

This information uses the following conventions.

Typefaces

TippingPoint uses the following typographic conventions for structuring information.

<table>
<thead>
<tr>
<th>Convention</th>
<th>Element</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Bold font</strong></td>
<td>• Key names</td>
</tr>
<tr>
<td></td>
<td>• Text typed into a GUI element, such as into a box</td>
</tr>
<tr>
<td></td>
<td>• GUI elements that are clicked or selected, such as menu and list items, buttons, and check boxes. Example: Click <strong>OK</strong> to accept.</td>
</tr>
<tr>
<td><em>Italic font</em></td>
<td>Text emphasis, important terms, variables, and publication titles</td>
</tr>
<tr>
<td><strong>Monospace font</strong></td>
<td>• File and directory names</td>
</tr>
<tr>
<td></td>
<td>• System output</td>
</tr>
<tr>
<td></td>
<td>• Code</td>
</tr>
<tr>
<td></td>
<td>• Text typed at the command-line</td>
</tr>
<tr>
<td><strong>Monospace, italic font</strong></td>
<td>• Code variables</td>
</tr>
<tr>
<td></td>
<td>• Command-line variables</td>
</tr>
<tr>
<td><strong>Monospace, bold font</strong></td>
<td>Emphasis of file and directory names, system output, code, and text typed at the command line</td>
</tr>
</tbody>
</table>
Messages

Messages are special text that is emphasized by font, format, and icons.

⚠️ **Warning!** Alerts you to potential danger of bodily harm or other potential harmful consequences.

⚠️ **Caution:** Provides information to help minimize risk, for example, when a failure to follow directions could result in damage to equipment or loss of data.

**Note:** Provides additional information to explain a concept or complete a task.

**Important:** Provides significant information or specific instructions.

**Tip:** Provides helpful hints and shortcuts, such as suggestions about how to perform a task more easily or more efficiently.

Product support

Get support for your product by using any of the following options:

**Email support**

tippingpoint.support@trendmicro.com

**Phone support**

North America: +1 866 681 8324

International: See https://tmc.tippingpoint.com

New and changed information in this edition

The following additions and changes have been made for this edition:

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.0</td>
<td><strong>New features</strong></td>
</tr>
<tr>
<td></td>
<td>X-Forwarded-For and True Client IP technologies support – The TPS can collect a client's true IP address from the HTTP header of a packet that has passed through a web proxy if the HTTP header includes the XFF or TCIP field. This feature introduces the following new commands:</td>
</tr>
<tr>
<td></td>
<td>• ips client-ip enable</td>
</tr>
</tbody>
</table>
### Version

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>• `ips{running-ips}profile PROFILENAME client-ip enable</td>
</tr>
<tr>
<td>• `ips{running-ips}profile PROFILENAME http-context enable</td>
</tr>
</tbody>
</table>

Capture additional event information – TOS v4.2.0 and later provide the ability to identify the HTTP URI and hostname information associated with an event.

### Enhancements

- SSL Inspection provides the following enhancements:
  - New support for Perfect Forward Secrecy (PFS). SSL Inspection extends key exchange support to Ephemeral Elliptic Curve Diffie-Hellman with RSA signatures (ECDHE-RSA). ECDHE-RSA enables PFS support for inspection of encrypted SSL sessions. Prior to this release, SSL Inspection supported the RSA key exchange, which is the most common key exchange used for SSL today, but did not support PFS.
  - The number of supported ciphers has increased from 6 to 14.
  - Performance improvements significantly increase the maximum number of concurrent SSL sessions under inspection.
  - Enhanced support for RSA AES cipher suites to now include SHA256.
- You can now use the `chpasswd` command to change the password for your local user account. In previous releases, only a user with the SuperUser role (or a custom role that allows modification of local user data) could change local passwords. 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.

### Deprecated

- `persona-change` command
- `shutdown` command

Instead, use 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:
<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>◦ 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.</td>
</tr>
<tr>
<td></td>
<td>◦ 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.</td>
</tr>
</tbody>
</table>

**4.1.0 Enhancements**

- 2200T support.
- From the CLI, you can exit the edit configuration mode from any context, by using the `!` command. For example: `ips{running}!`
- The `halt` command allows you 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. To restart the device, remove power, wait 15 seconds, and then re-apply power.
- The `timezone` CLI command provides a new option, US, that allows you to set the time zone of the device to a standard time zone in the United States.

**New features**

- SSL inspection profiles (2200T only)
- VLAN translation
- Best Effort mode (2200T only)
- Inspection bypass rules
- Inspection of tunneled traffic

**New commands**

- `tech-support-report`
- `ssl-inspection`
- `running-sslinsp context commands`
- `debug np ssl-clear`
- `debug np stats show npSslInspStats`
- `show ssl-inspection congestion`
<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.0.0</td>
<td>Initial publication</td>
</tr>
</tbody>
</table>

- `ips{running-vsegs-VSEG_NAME}ssl-profile`
- `running-inspection-bypass context commands`
- `running-vlan-translations context commands`
- `debug np best-effort`
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:

<table>
<thead>
<tr>
<th>Syntax Convention</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>UPPERCASE</td>
<td>Uppercase represents a user-supplied value.</td>
</tr>
<tr>
<td>(x)</td>
<td>Parentheses indicate a required argument.</td>
</tr>
<tr>
<td>[x]</td>
<td>Brackets indicate an optional argument.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Examples

The question mark displays help information:

```plaintext
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.

<table>
<thead>
<tr>
<th>Shortcut</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ENTER</strong></td>
<td>Runs the command.</td>
</tr>
<tr>
<td><strong>TAB</strong></td>
<td>Completes a partial command.</td>
</tr>
<tr>
<td><strong>?</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>!</strong></td>
<td>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></td>
</tr>
<tr>
<td><strong>UP ARROW</strong></td>
<td>Shows the previous command.</td>
</tr>
<tr>
<td><strong>DOWN ARROW</strong></td>
<td>Shows the next command.</td>
</tr>
<tr>
<td><strong>Ctrl + P</strong></td>
<td>Shows the previous command.</td>
</tr>
<tr>
<td><strong>Ctrl + N</strong></td>
<td>Shows the next command.</td>
</tr>
<tr>
<td><strong>Ctrl + L</strong></td>
<td>Clears the screen, does not clear history.</td>
</tr>
</tbody>
</table>
### Shortcut

<table>
<thead>
<tr>
<th>Shortcut</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ctrl + A</td>
<td>Returns to the start of the command you are typing.</td>
</tr>
<tr>
<td>Ctrl + E</td>
<td>Goes to the end of the command you are typing.</td>
</tr>
<tr>
<td>Ctrl + U</td>
<td>Cuts the whole line to a special clipboard.</td>
</tr>
<tr>
<td>Ctrl + K</td>
<td>Cuts everything after the cursor to a special clipboard.</td>
</tr>
<tr>
<td>Ctrl + Y</td>
<td>Pastes from the special clipboard used by Ctrl + U and Ctrl + K.</td>
</tr>
</tbody>
</table>

### Hierarchical context

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

<table>
<thead>
<tr>
<th>Prompt</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ips{}</td>
<td>Displays the top-level root mode. This context is displayed when you first log in to the CLI.</td>
</tr>
<tr>
<td>ips{}edit</td>
<td>Enters the edit configuration mode.</td>
</tr>
<tr>
<td>ips{running}</td>
<td>Displays the configuration mode by changing the prompt to running. This indicates you will be making changes to the running configuration.</td>
</tr>
<tr>
<td>ips{running}display</td>
<td>Views the current configuration and any changes.</td>
</tr>
<tr>
<td>ips{running}commit</td>
<td>Commits changes to the running configuration.</td>
</tr>
<tr>
<td>ips{}log-configure</td>
<td>Enters the log-configure context to access the log configuration mode.</td>
</tr>
</tbody>
</table>
### Prompt

<table>
<thead>
<tr>
<th>Prompt</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ips{log-configure}</code></td>
<td>Displays the log configuration mode.</td>
</tr>
<tr>
<td><code>ips{log-configure}help</code></td>
<td>Displays list of valid commands and syntax usage.</td>
</tr>
<tr>
<td><code>ips{running}exit</code></td>
<td>Leaves the current configuration mode.</td>
</tr>
<tr>
<td><code>ips{running}!</code></td>
<td>Leaves the configuration mode from any context and returns to the top-level root mode.</td>
</tr>
</tbody>
</table>

### 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.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>help</code> or <code>?</code></td>
<td>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).</td>
</tr>
<tr>
<td><code>help commandname</code></td>
<td>Displays syntax for a command.</td>
</tr>
<tr>
<td><code>commandname?</code></td>
<td>Displays the options for a command. For example, <code>ping ?</code>.</td>
</tr>
<tr>
<td><code>string?</code></td>
<td>Shows the commands or keywords that match the string. For example, <code>s?</code>.</td>
</tr>
</tbody>
</table>

### Command modes

The TPS uses a hierarchical menu structure. Within this structure, commands are grouped by functional area within one of three command modes:
<table>
<thead>
<tr>
<th>Command Mode</th>
<th>Description/Example</th>
</tr>
</thead>
</table>
| Root               | When you first log in to the device, you enter the top of the hierarchy, the root mode.  
|                    | ips{}                                                                               |
| Edit               | Enters the edit mode.                                                                |
|                    | ips{running}                                                                        |
| Log Configuration  | Enters the log configuration mode.                                                   |
|                    | ips{log-configure}                                                                  |

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:

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

To change the host name, type:

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

For a list of root commands and their usage see Root commands on page 19.

**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.

```plaintext
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.

```plaintext
ips{running}exit
```

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

```plaintext
ips{running}exit
```

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

```plaintext
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 on page 19.
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.

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>save-config</td>
<td>Copy the Running configuration to the Startup configuration.</td>
</tr>
</tbody>
</table>

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]

Example

ips{running-aaa-user-myuser1}display

# USER ID
user myuser1

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* on page 12.

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
dns
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
<table>
<thead>
<tr>
<th>Command</th>
<th>Context</th>
</tr>
</thead>
<tbody>
<tr>
<td>segmentX</td>
<td>Enter Segment context</td>
</tr>
<tr>
<td>services</td>
<td>Enter services context</td>
</tr>
<tr>
<td>snmp</td>
<td>Enter SNMP context</td>
</tr>
<tr>
<td>traffic-management</td>
<td>Enter traffic-management profile context</td>
</tr>
<tr>
<td>virtual-segments</td>
<td>Enter virtual-segments context</td>
</tr>
</tbody>
</table>

ips{running}commit
ips{running}exit
ips{}

## help
Displays help information.

### Syntax
help [full|COMMAND]

### Example
ips{running}help log
Enter log context
Syntax: log
log Enter log context
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`

**boot**

Lists software packages and rollback to a previous version.

**Syntax**

`boot (list-image|rollback)`

**Example**

`ips{}boot list-image`

<table>
<thead>
<tr>
<th>Index</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1.0.0.3935</td>
</tr>
<tr>
<td>1</td>
<td>1.0.0.2923</td>
</tr>
<tr>
<td>2</td>
<td>1.0.0.3932</td>
</tr>
</tbody>
</table>
Oldest Index is 2
Factory Reset Index is 3

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

Example

Enter the chpasswd command and the name of the local user, user01, to change the password. You are prompted to enter and confirm the new password.

ips{}chpasswd user01
Enter new password: *********
Confirm new password: *********

clear

Clears system stats, logs, locked users, or packet traces.

Syntax

clear connection-table (blocks|trusts)
clear log-file (audit|fwAlert|fwBlock|ipsAlert|ipsBlock|quarantine|reputationAlert|reputationBlock|system|visibility|vpn)
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]

Example
gerps{}clear log-file audit

Example
gerps{}clear users fred

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

Example
gerps{}date 071718202013.59 (sets date to July 17 2013 6:20PM 59 seconds)

debug

Most debug commands should be used only when you are instructed to do so by technical support.
Syntax

default

Valid entries at this position are:

aaa                 aaa debug options
autoDV              Access automatic Digital Vaccine (AutoDV) functions
busy-wait           Wait for UDM
core-dump           Enable or disable core dumps
echo                Echo text to console
factory-reset       Factory Reset
force-obe           Forces re-run of OBE on the next reset
ini-cfg             .ini values
np                  Network processor
reputation          Reputation utilities
show                Show current .ini values
snapshot            Manage system snapshots
UDM                 UDM debug options

Examples

See the following examples for more information about debug commands.

debug factory-reset

debug factory-reset

WARNING!!!

This command WILL reset this device to factory default configuration.
This will remove all network and security configuration, user accounts
log files, snapshots and applied software upgrades

You will NOT be able to recover any of this data from the device after
this command has been confirmed

After the factory reset completes, the device will automatically
reboot and display the OBE

Warning: Type the word 'COMMIT' to continue: COMMIT

debug np best-effort options

Best Effort mode protects latency-sensitive applications by not inspecting packets if the latency introduced
by inspecting them exceeds the configured threshold. When the latency reaches the specified threshold,
permitted traffic is not inspected until latency falls to the user-defined recovery percentage. When
performing SSL inspection, the latency measure and relief only apply on inspection, and do not apply to the SSL and TCP proxy connections.

Best Effort mode is supported on the 2200T TPS only.

Subcommands

The `debug np best-effort` command uses the following subcommands.

<table>
<thead>
<tr>
<th>Subcommand</th>
<th>Description</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enables Best Effort mode.</td>
<td><code>debug np best-effort enable [-queue-latency &lt;microseconds&gt;] [-recover-percent &lt;percent&gt;]</code></td>
</tr>
<tr>
<td>disable</td>
<td>Disables Best Effort mode.</td>
<td><code>debug np best-effort disable</code></td>
</tr>
</tbody>
</table>

Options

The `debug np best-effort` command uses the following options.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>-queue-latency</td>
<td>Defines the latency threshold at which Best Effort mode is entered. The default is 1000 microseconds.</td>
<td><code>debug np best-effort enable -queue-latency &lt;microseconds&gt;</code></td>
</tr>
<tr>
<td>-recover-percent</td>
<td>Defines the recovery percentage at which Best Effort mode is exited. The default is 20%; if the latency threshold is 1000 microseconds, the device exits Best Effort mode when latency drops to 200 microseconds (20% of 1000).</td>
<td><code>debug np best-effort enable -recover-percent &lt;percent&gt;</code></td>
</tr>
</tbody>
</table>

`debug np mcfilt-regex options`

Microfilter regular expression statistics.
debug np regex [clear|show option]

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear</td>
<td>Clears regular expression statistics.</td>
</tr>
<tr>
<td>show average</td>
<td>Sorts and displays network processor information based on average time.</td>
</tr>
<tr>
<td>show count</td>
<td>Specifies the number of entries to display. Default: 10</td>
</tr>
<tr>
<td>show evaluations</td>
<td>Sorts and displays network processor information based on the number of evaluations.</td>
</tr>
<tr>
<td>show matches</td>
<td>Sorts and displays network processor information based on the number filter matches.</td>
</tr>
<tr>
<td>show maximum</td>
<td>Sorts and displays network processor information by maximum time. Default: The default display if you do not specify another option.</td>
</tr>
<tr>
<td>show total</td>
<td>Sorts and displays network processor information by total time.</td>
</tr>
</tbody>
</table>

debug np regex options

Regular expression statistics.

depth np regex [clear|show option]

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear</td>
<td>Clears regular expression statistics.</td>
</tr>
<tr>
<td>show average</td>
<td>Sorts and displays network processor information based on average time.</td>
</tr>
<tr>
<td>show count</td>
<td>Specifies the number of entries to display.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>default</td>
<td>Default: 10</td>
</tr>
<tr>
<td>show evaluations</td>
<td>Sorts and displays network processor information based on the number of evaluations.</td>
</tr>
<tr>
<td>show matches</td>
<td>Sorts and displays network processor information based on the number filter matches.</td>
</tr>
<tr>
<td>show maximum</td>
<td>Sorts and displays network processor information by maximum time. Default: The default display if you do not specify another option.</td>
</tr>
<tr>
<td>show total</td>
<td>Sorts and displays network processor information by total time.</td>
</tr>
</tbody>
</table>

**debug np stats options**

Show/clear engine statistics.

d debug np stats [clear|help|show]

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear</td>
<td>Clears regular expression statistics.</td>
</tr>
<tr>
<td>help</td>
<td>Lists available statistics tables.</td>
</tr>
<tr>
<td>show</td>
<td>Shows system information.</td>
</tr>
</tbody>
</table>

**Note:** When an active session is closed, the session count is decremented. If the session count was already set to zero by the clear command, then the session count incorrectly appears as a very large number.

**debug np stats show npSslInspStats Example**

The following example displays potential culprits of SSL inspection:

ips{}debug np stats show npSslInspStats

Connections:
clientConnections = 1 ; Number of client connections
clientConnectionFailures = 0 ; Number of client connection failures
serverConnections = 1 ; Number of server connections
serverConnectionFailures = 0 ; Number of server connection failures
refusedConnections = 9 ; Number of refused sessions

Sessions:
activeSessions = 0 ; Number of active sessions
inspectedSessions = 1 ; Number of inspected sessions
blockedSessions = 0 ; Number of blocked sessions
trustedSessions = 0 ; Number of trusted sessions
flushTrustedSessions = 0 ; Number of flushed trusted sessions
shuntedSessions = 0 ; Number of shunted sessions
blockedMaxSslConnections = 0 ; Number of blocked sessions due to max conn limit
allowedMaxSslConnections = 0 ; Number of allowed sessions due to max conn limit

Renegotiation:
renegotiationServerSide = 1 ; Number of renegotiations initiated by the server
renegotiationClientSide = 2 ; Number of renegotiations initiated by the client
renegotiationProxy = 0 ; Number of renegotiations initiated by the proxy

Certificate Requests:
clientCertificateRequests = 0 ; Number of client certificates requested by server

Other:
mbufFails = 0 ; Number of failures to get a free message buffer

debug np congestionx Example

The following example displays potential culprits of network congestion:

ips{}debug np congestionx
Device Bypassed Dropped Out of
--------- ----------- --------- ----------
BCOM 0          0       1447
NIC Ingress 0 893353197360 111669151015
CPU Ingress 0          0       1448
CPU Egress 0          0       1448
NIC Egress 0 0 111669151015
System RL 0          1448

debug np diagx Example

The following example displays diagnostic information:

ips{} debug np diagx -details
Switch (packet flow from top left counterclockwise)

  1A 0 0
Bypass 0 0
Uplink 0 0 RX Dropped 0 RX Pause 0

Processor
  CPU A 0 0
  Engine 0 0
Dropped               0
Blocked               0
Policy RL               0
System RL               0

Time since last snapshot: 1 minute, 12 seconds

dbg np regex Example

The following example sorts the network processor information based on the average time:

ips{}debug np regex show average

<table>
<thead>
<tr>
<th>Filter</th>
<th>CRC</th>
<th>Flag</th>
<th>Max(us)</th>
<th>Avg(us)</th>
<th>Evals</th>
<th>Matches</th>
<th>Total(us)</th>
</tr>
</thead>
<tbody>
<tr>
<td>3179</td>
<td>0x0f7b8828</td>
<td>P</td>
<td>795</td>
<td>768</td>
<td>4</td>
<td>0</td>
<td>3073</td>
</tr>
<tr>
<td>4062</td>
<td>0xaf664079</td>
<td>PS</td>
<td>595</td>
<td>466</td>
<td>4</td>
<td>4</td>
<td>1866</td>
</tr>
<tr>
<td>5995</td>
<td>0xed3a9991</td>
<td>R</td>
<td>308</td>
<td>234</td>
<td>4</td>
<td>0</td>
<td>938</td>
</tr>
<tr>
<td>10762</td>
<td>0xf4a09e9d</td>
<td>P</td>
<td>614</td>
<td>169</td>
<td>8</td>
<td>0</td>
<td>1350</td>
</tr>
<tr>
<td>6413</td>
<td>0xbea34771</td>
<td>R</td>
<td>114</td>
<td>109</td>
<td>2</td>
<td>0</td>
<td>218</td>
</tr>
<tr>
<td>10777</td>
<td>0xe602fe470</td>
<td>R</td>
<td>417</td>
<td>105</td>
<td>55</td>
<td>0</td>
<td>5750</td>
</tr>
<tr>
<td>6416</td>
<td>0xbb3d4b462</td>
<td>R</td>
<td>102</td>
<td>102</td>
<td>1</td>
<td>0</td>
<td>102</td>
</tr>
<tr>
<td>6417</td>
<td>0xe65b97c0b</td>
<td>R</td>
<td>98</td>
<td>98</td>
<td>1</td>
<td>0</td>
<td>98</td>
</tr>
<tr>
<td>6356</td>
<td>0x4b09bc88</td>
<td>R</td>
<td>103</td>
<td>85</td>
<td>4</td>
<td>0</td>
<td>341</td>
</tr>
<tr>
<td>6662</td>
<td>0x96decebfe</td>
<td>P</td>
<td>130</td>
<td>80</td>
<td>18</td>
<td>0</td>
<td>1439</td>
</tr>
</tbody>
</table>

dbg np ssl-clear Example

The debug np ssl-clear command clears any "stale" sessions and forces clients to reconnect. This is a useful troubleshooting tool for features that have a session state. The following example terminates any SSL sessions that are proxied by the 2200T and clears the sessions information from the LSM:

ips{}debug np ssl-clear

dbg np stats Example

The following example displays system information:

ips{}debug np stats help

<table>
<thead>
<tr>
<th>udmAggStats</th>
<th>(CP only)</th>
<th>UDM Aggregation Statistics</th>
</tr>
</thead>
<tbody>
<tr>
<td>cpMiscStats</td>
<td>(CP only)</td>
<td>Control Plane Miscellaneous Stats</td>
</tr>
<tr>
<td>npMetadataStats</td>
<td>(DP only)</td>
<td>Event Metadata Statistics</td>
</tr>
<tr>
<td>npIrrStats</td>
<td></td>
<td>NetPal Inverted Reroute Stats</td>
</tr>
<tr>
<td>npMicrofilterStats</td>
<td>(DP only)</td>
<td>NetPal Microfilter Statistics</td>
</tr>
<tr>
<td>npHttpresponseStats</td>
<td>(DP only)</td>
<td>HTTP Response Statistics</td>
</tr>
<tr>
<td>dpalStats</td>
<td>(CP only)</td>
<td>DPAL counters</td>
</tr>
<tr>
<td>asFlowControlStats</td>
<td></td>
<td>Action Set Flow Control Stats</td>
</tr>
<tr>
<td>fqStats</td>
<td>(DP only)</td>
<td>FlowQueue Stats</td>
</tr>
<tr>
<td>npScanSweepMemStats</td>
<td></td>
<td>NetPal Scan/Sweep Memory Stats</td>
</tr>
<tr>
<td>npScanSweepStats</td>
<td></td>
<td>NetPal Scan/Sweep Statistics</td>
</tr>
</tbody>
</table>
dpsIpcClassStats
npZlibStats
sleuthPatterns (CP only)
ruleStatsStats
dpsIpcConv
npTrafficCaptureStats
dpsIpcRpcStats (CP only)
dpwdStats (CP only)
dpsIpcCPStats
lwipStats (DP only)
dpsIpcStats
snakeStats
npTurboSimLfhStats (DP only)
npQuarantineActionLfhStats (DP only)
npQuarantineAqciLfhStats (DP only)
npQuarantineStats
npSynProxyStats (DP only)
npIpReputationIpStats (CP only)
npIpReputationRequestStats (CP only)
npIpReputationCallbackStats (DP only)
npDnsReputationStats (DP only)
npIpReputationStats (DP only)
npHreStats (DP only)
npSoftLinxStats (DP only)
trhaStats (CP only)
npTcpStateStats (DP only)
rlStats (DP only)
npHCDSpStats (DP only)
npIPDgrams (DP only)
npZoneStats (DP only)
npTelnetStats (DP only)
npSnmpStats (DP only)
npSmtpStats (DP only)
npSmbStats (DP only)
npRpcStats (DP only)
npMsrpcStats (DP only)
npOspfStats (DP only)
npImapStats (DP only)
npHttpStats (DP only)
aphStats (DP only)
npFtpStats (DP only)
npDnsStats (DP only)
udmCbStats
npTTStats

dpsIpc per-class stats
NetPal Zlib Statistics
Sleuth pattern table stats
stats about rule stats
dpsIpc Conversion stats
NetPal traffic capture stats
dpsIpcRpc Stats
DP Watchdog Statistics
XLRC's ECC Stats
XLRB's ECC Stats
XLRA's ECC Stats
ECC Stats
Timing Subsystem
dpsIpc CP Stats
lwip Stats
dpsIpc Stats
Snake Stats
Turbo Simulator LF Hash Stats
Quarantine Action LF Hash Stats
Quarantine AQCI LF Hash Stats
NetPal Quarantine Packet Stats
NetPal SYN Proxy Statistics
IP Reputation command IPC Stats
(null)
IP Reputation Callback Stats
DNS Reputation Statistics
IP Reputation Statistics
Rule Statistics
NetPal SOFTLINX Statistics
TRHA Statistics
TCP State module stats.
Policy Rate Limiter Statistics
NetPal HardCode Statistics
(null)
ZoneStats
TELNET Decode Statistics
SNMP Decode Statistics
SMTP Decode Statistics
SMB Decode Statistics
RPC Decode Statistics
MS-RPC Decode Statistics
OSPF Decode Statistics
IMAP Decode Statistics
HTTP Decode Statistics
ahp Stats
FTP Decode Statistics
DNS Decode Statistics
UDM Callback Statistics
NetPal Trust Table Stats
npCTStats                                NetPal Connection Table Statistics  
pcbStats                    (DP only)    PCB Stats  
rxStats                     (DP only)    Rx Stats  
threadFwdStats              (DP only)    NetPal Parse Packet Statistics  
npHardCodeStats             (DP only)    HardCode Packet Statistics  
npFilterStatsInst           (DP only)    (null)  
npReparseStatsInst          (DP only)    NetPal Non-ingress Parse Packet Stats  
npParseStatsInst            (DP only)    NetPal Parse Packet Statistics  
npTcpReas                   (DP only)    TCP Reassembly Statistics  
npReasIpv6                  (DP only)    IPv6 Reassembly Statistics  
npReas                      (DP only)    IPv4 Reassembly Statistics  
dpk                         (DP only)    Data Plane Stats  
triv                                     Sample stats  
ips{}debug np stats show trhaStats  
TRHA:                        
    trhaSend = 0    ; trhaSend  
    trhaReceive = 0 ; trhaReceive  
    trhaDropped = 0 ; trhaDropped  
Host Communication:         
    hostCommSend = 0  ; hostCommSend  
    hostCommReceive = 0 ; hostCommReceive  
    hostCommDropped = 0 ; hostCommDropped  
Delay:                      
    delayTotal = 0 ; delayTotal  
    delayCount = 0 ; delayCount  

**debug np port Example**

The following example displays system information:

ips{}debug np port show  
PORT status:  
Local Device 0 (switch in NORMAL mode)  

Port  Bcm  Num  Admin Status Speed AutoNeg Pause Mode MTU Medium SP MMU cells  
enet1  ge1  3 Disabled DOWN 1Gbps auto  - GMII 1526 Fiber 0 0  
enet2  ge0  2 Disabled DOWN 1Gbps auto  - GMII 1526 Fiber 0 0  
enet3  ge3  5 Disabled DOWN 1Gbps auto  - GMII 1526 Fiber 0 0  
enet4  ge2  4 Disabled DOWN 1Gbps auto  - GMII 1526 Fiber 0 0  
enet5  ge5  7 Disabled DOWN 1Gbps auto  - GMII 1526 Fiber 0 0  
enet6  ge4  6 Disabled DOWN 1Gbps auto  - GMII 1526 Fiber 0 0  
enet7  ge7  9 Disabled DOWN 1Gbps auto  - GMII 1526 Fiber 0 0  
enet8  ge6  8 Disabled DOWN 1Gbps auto  - GMII 1526 Fiber 0 0  
enet9  ge9  11 Enabled UP 1Gbps auto none SGMII 1526 Copper 0 0  
enet10 ge8  10 Enabled UP 1Gbps auto none SGMII 1526 Copper 0 0  
enet11 ge11 13 Enabled UP 1Gbps auto none SGMII 1526 Copper 0 0  
enet12 ge10 12 Enabled UP 1Gbps auto none SGMII 1526 Copper 0 0  
enet13 ge13 15 Disabled DOWN  - auto  - SGMII 1526 Copper 0 0
enet14  ge12 14   Disabled  DOWN   -  auto      -   SGMII  1526 Copper  0   0
enet15  ge15 17   Enabled   UP     1Gbps  auto    none  SGMII  1526 Copper  0   0
enet16  ge14 16   Enabled   UP     1Gbps  auto    none  SGMII  1526 Copper  0   0
uplnk0  xe0  26   Uplink   UP    10Gbps  none    none  XGMII 16356  Fiber  0   0
uplnk1  xe1  27   Uplink   UP    10Gbps  none    none  XGMII 16356  Fiber  0   0
uplnk2  xe2  28   Uplink   DOWN  10Gbps  none      -   XGMII 16356  Fiber  0   0
uplnk3  xe3  29   Uplink   DOWN  10Gbps  none      -   XGMII 16356  Fiber  0   0
ips{}debug np port diags 1A
Port:     enet1 (uport 1; port 3)
Enable state:   Disabled
Link status:    DOWN
Laser status:   SFP absent and laser off
Linkscan mode:  SW
Auto-negotiated: (no link)
Port ability:   fd = 100MB,1000MB
                 hd = <none>
                 intf = gmii
                 medium = <none>
                 pause = pause_tx,pause_rx,pause_asymm
                 lb = none,MAC,PHY
                 flags = autoneg
Advertised ability:   fd = 1000MB
                 hd = <none>
                 intf = <none>
                 medium = <none>
                 pause = <none>
                 lb = <none>
                 flags = <none>
STP mode:         Forward
Learn mode:        FWD
Untag priority mask:  0
Multicast flood (pfm):  FloodNone
Interface:         GMII
Max_frame size:    1526
MDIX mode:         ForcedNormal, Normal
Medium:            Fiber

dump show settings Example

The dump show settings command provides an overview your debug configuration. In the following example, best-effort mode is enabled.

ips{}debug show settings
Core dumps:   Disabled
Best Effort:  Enabled
Snapshot Version:  Ignore
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

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]

Example

ips{running-aaa-user-myuser1}display

# USER ID

user myuser1

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

Example

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

Example

Displays SSL configuration.

ips{}display conf running ssl-inspection
# SSL INSPECTION STATEMENTS
disable
# SSL SERVERS
server "swdevts4b"
  ip address 10.1.2.78/32
detection-port 443
detection-port 999
decrypted-service http
cipher-suite RSA-3DES-EDE-CBC-SHA1
cipher-suite RSA-AES128-CBC-SHA1
cipher-suite RSA-AES256-CBC-SHA1
protocol TLSv1.0
protocol TLSv1.1
protocol TLSv1.2
certificate swdevts4b
logging
tcp-reset
exit
server "swdevts4b_server"
  ip address 10.1.2.2/32
detection-port 443
detection-port 999
decrypted-service http
cipher-suite RSA-3DES-EDE-CBC-SHA1
cipher-suite RSA-AES128-CBC-SHA1
cipher-suite RSA-AES256-CBC-SHA1
protocol TLSv1.0
protocol TLSv1.1
protocol TLSv1.2
certificate swdevts4b_cert
logging
tcp-reset
exit

# SSL PROFILES
profile "swdevts4b"
policy "swdevts4b"
   enable
   server "swdevts4b"
exit
exit

profile "swdevts4b_profile"
policy "swdevts4b_policy"
   enable
   server "swdevts4b_server"
exit
exit

# LOG SERVICE
log sslInspection "Management Console" ALL
log sslInspection "Remote System Log" ALL

display-config

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

Syntax

display-config (start|running)

Example

ips{}display-config start

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 on page 12.
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
- `segmentX` Enter Segment context
- `services` Enter services context
- `snmp` Enter SNMP context
- `traffic-management` Enter traffic-management profile context
- `virtual-segments` Enter virtual-segments context

ips{running}commit
ips{running}exit
ips{}

**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

Example

ips{}halt

You are about to halt the device.

Make sure you have Committed all your changes and Saved them if you wish these changes to be applied when the device is restarted.

WARNING: Are you sure you want to halt the system (y/n) [n]:

help

Displays help information.

Syntax

help [full|COMMAND]

Example

ips{running}help log

Enter log context

Syntax: log

log Enter log context

high-availability

Enters high-availability context mode.

Syntax

high-availability force (fallback|normal)

high-availability zero-power (bypass-ips|normal)

Example

ips{running}high-availability

Valid entries at this position are:
force        Set intrinsic HA state manually
zero-power   Configure high-availability zero-power state
ips{running}high-availability force
Valid entries at this position are:
  fallback   Set intrinsic HA state to fallback mode
  normal     Set intrinsic HA state to normal
ips{running}high-availability force fallback enable|disable
ips{running}high-availability zero-power
Valid entries at this position are:
  bypass-ips Configure high-availability zero-power state to bypass-ips
  normal      Configure high-availability zero-power state to normal
ips{running}high-availability zero-power bypass-id enable|disable

## 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 via 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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ips{running-certificates}private-key</code> on page 120</td>
<td>Import the private key from your web server into the local keystore on the device.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td><code>ips{running-certificates}certificate</code> on page 117</td>
<td>Import the certificate from your web server into the local keystore on the device.</td>
</tr>
<tr>
<td><code>ips{running-sslinsp}server</code> on page 160</td>
<td>Add an SSL server to the device with the same security settings as your web server, and assign the corresponding certificate and private key.</td>
</tr>
</tbody>
</table>

**list**

Displays traffic capture file list.

**Syntax**

```
list traffic-file
```

**Example**

```
ips{}list traffic-file
```

**log-configure**

Enters log configuration context.

**Syntax**

```
log-configure
```

**Example**

```
ips{}log-configure
ips{log-configure}help
ips{log-configure}show log-file summary
```

**logout**

Logs you out of the system.

**Syntax**

```
logout
```
### master-key

Set the system master key to encrypt the system keystore. The system keystore retains data, such as device certificates and private keys. If you are planning to persist private keys on the device, always secure the system keystore. By default, the system keystore is not encrypted.

If the master key is already set, you can skip this step.

When the system master key is set, you can choose to also encrypt any data on the user disk (external CFast). For more information, see `user-disk` on page 78.

⚠️ **Caution:** When the external CFast is encrypted, changing or clearing the system master key erases all traffic logs, snapshots, and packet capture data on the removable user disk. For information about securing the external CFast, see the *Local Security Manager User Guide* or the `user-disk` command in the *Command Line Interface Reference*.

Enter an option to set the master key:

- **passphrase** – This option prompts you to enter a passphrase to secure the system keystore.

  **Note:** This option allows you to restore a snapshot of this device, which includes the keystore, to a different device that is configured with the same master key. If you misplace this passphrase, you can restore a snapshot of this device to a different device, but the keystore is not restored. You must also reset the keystore using the `master-key clear reset-keystore` command.

  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-specific-key** – This option generates a passphrase to secure the keystore to this device.

  **Note:** This option allows you to restore a snapshot, which includes the keystore, to the same device. If necessary, you can restore a snapshot with a device-generated key to a different device, but the keystore is not restored. You must also reset the keystore to its initial state using the `master-key clear reset-keystore` command. After you reset the keystore, import any private keys and, for SSL inspection, edit SSL servers to use the new private keys.

**Syntax**

```
master-key (clear [reset-keystore]|set [device-specific-key|passphrase])
```
Example

Set the system master key with your own passphrase to encrypt the system keystore. Existing data in the system keystore is encrypted:

```bash
ips{}master-key set passphrase
WARNING: Master key will be set to a passphrase and used to encrypt the keystore and user disk.
Do you want to continue (y/n)? [n]: y
    Enter Master Key    : ****************
    Re-enter Master Key: ****************
Success: Master key has been set.
```

Example

Set the system master key with a device-specific key to encrypt the system keystore. Existing data in the system keystore is encrypted:

```bash
ips{}master-key set device-specific-key
WARNING: Master key will be set to a device specific key and used to encrypt the keystore and user disk. Keystore data in snapshots created with the device specific key can only be restored to this device.
Do you want to continue (y/n)? [n]: y
    Success: Master key has been set to device specific key.
```

Example

Clear the master key to remove encryption from the system keystore and the external user disk. If you clear a device-specific key, data in the system keystore is preserved but keystore data in snapshots created with the previous key is unrecoverable.

```bash
ips{}master-key clear
WARNING: Clearing the master key will remove encryption from the keystore and user disk.
WARNING: User disk encryption is enabled. Clearing the master key will erase all existing data on the user disk and disable user disk encryption.
WARNING: This device is currently using a device specific key. Changing this key will make keystore data in snapshots created with the previous key non-recoverable.
Do you want to continue (y/n)? [n]: y
Success: Master key has been cleared.
WARNING: Keystore and user disk are no longer encrypted.
```

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)]

Example

ips{}ping 192.168.1.1
ping using mgmt port
PING 192.168.1.1 (192.168.1.1): 56 data bytes
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 vrfid=500 time=0.4 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 vrfid=500 time=0.1 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=64 vrfid=500 time=0.1 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=64 vrfid=500 time=0.1 ms
--- 192.168.1.1 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.1/0.1/0.4 ms

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)]

Example

ips{}ping6 100:0:0:0:0:0:0:1
ping using mgmt port
PING 100:0:0:0:0:0:0:1 (100:0:0:0:0:0:0:1): 56 data bytes
64 bytes from 100:0:0:0:0:0:0:1: icmp_seq=1 ttl=64 vrfid=0 time=0.3 ms
64 bytes from 100:0:0:0:0:0:0:1: icmp_seq=2 ttl=64 vrfid=0 time=0.1 ms
64 bytes from 100:0:0:0:0:0:0:1: icmp_seq=3 ttl=64 vrfid=0 time=0.1 ms
64 bytes from 100:0:0:0:0:0:0:1: icmp_seq=4 ttl=64 vrfid=0 time=0.1 ms
--- 100:0:0:0:0:0:0:1 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.1/0.1/0.3 ms
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

Example
quarantine add 1.1.1.1 Block (Actionset Block's quarantine feature should be enabled)
quarantine remove 1.1.1.1
quarantine list
quarantine empty

Related commands
show quarantine-list on page 64

reboot

Reboots the system. Specify a full system restart with the full option.

Syntax
reboot [full]

Example
ips{}reboot
WARNING: Are you sure you want to reboot the system (y/n) [n]:

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

Example
ips{}reports enable cpu
ips{}reports reset cpu
WARNING: Are you sure you want to reset cpu reports (y/n)? [n]:

Related commands
show reports on page 65

resize

Resizes the terminal.

Syntax
resize

save-config

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

Tip: 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. Note when run from a context, this command does not commit your pending changes to the Running configuration.

Syntax
save-config

Examples
Copies the Running configuration to the Startup configuration. Note that in order to run this command from the top-level prompt, you must commit or discard your pending configuration changes.
ips{}save-config
WARNING: Saving will apply this configuration at the next system start. Continue (y/n)? [n]:

The following example copies the Running configuration to the Startup configuration without exiting the configuration mode. Any pending context configuration changes are preserved.

ips{running-sslinsp}!save-config

WARNING: Saving will apply this configuration at the next system start. Continue (y/n)? [n]:

**Related commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>commit on page 16</td>
<td>Commit your pending changes to the Running configuration.</td>
</tr>
</tbody>
</table>

**service-access**

Enables or disables service access.

**Syntax**

service-access (enable|disable)

**Example**

ips{}service-access enable
Serial: X-NGF-S1020F-GENERIC-001
Salt: Zk0lenyg
ips{}service-access disable

**set**

Configures an item.

**Syntax**

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

ips{}set cli filtering rule auto-comment
ips{}set cli filtering rule no-auto-comment

setup

Runs the setup wizard.

Syntax

setup

show

View current system configuration, status, and statistics.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show aaa on page 47</td>
<td>Show AAA information.</td>
</tr>
<tr>
<td>show auxdv on page 49</td>
<td>Show the AuxDV package.</td>
</tr>
<tr>
<td>show date on page 49</td>
<td>Show the current router date and time.</td>
</tr>
<tr>
<td>show dns on page 49</td>
<td>Show Domain Name Service.</td>
</tr>
<tr>
<td>show filter on page 49</td>
<td>Show filter information.</td>
</tr>
<tr>
<td>show health on page 50</td>
<td>Show health information.</td>
</tr>
<tr>
<td>show high-availability on page 52</td>
<td>Show high-availability status.</td>
</tr>
<tr>
<td>show interface on page 53</td>
<td>Show network interface.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td><code>show key</code> on page 54</td>
<td>Show local server SSH key information.</td>
</tr>
<tr>
<td><code>show license</code> on page 54</td>
<td>Show the license number and status.</td>
</tr>
<tr>
<td><code>show log-file</code> on page 54</td>
<td>Show the log files.</td>
</tr>
<tr>
<td><code>show log-file boot</code> on page 55</td>
<td>Show the boot file.</td>
</tr>
<tr>
<td><code>show mfg-info</code> on page 59</td>
<td>Show manufacturing information.</td>
</tr>
<tr>
<td><code>show np engine</code> on page 60</td>
<td>Show net processor statistics.</td>
</tr>
<tr>
<td><code>show np general statistics</code> on page 60</td>
<td>Show general network processor information.</td>
</tr>
<tr>
<td><code>show np mcfilt-rule-stats</code> on page 61</td>
<td>Show microfilter rules, number of flows, successful matches.</td>
</tr>
<tr>
<td><code>show np protocol-mix</code> on page 61</td>
<td>Show network processor protocol-level statistics.</td>
</tr>
<tr>
<td><code>show np reassembly</code> on page 62</td>
<td>Show network processor reassembly statistics.</td>
</tr>
<tr>
<td><code>show np rule-stats</code> on page 62</td>
<td>Show network processor rules, number of flows, successful matches.</td>
</tr>
<tr>
<td><code>show np softlinx</code> on page 63</td>
<td>Show network processor softlinx statistics.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>show np tier-stats on page 63</td>
<td>Show network processor throughput and utilization for each tier.</td>
</tr>
<tr>
<td>show quarantine-list on page 64</td>
<td>Show quarantine list information.</td>
</tr>
<tr>
<td>show reports on page 65</td>
<td>Show status of data collection for reports.</td>
</tr>
<tr>
<td>show service on page 65</td>
<td>Show network service information.</td>
</tr>
<tr>
<td>show sms on page 66</td>
<td>Show status of SMS control.</td>
</tr>
<tr>
<td>show snmp on page 66</td>
<td>Show SNMP information.</td>
</tr>
<tr>
<td>show system connections on page 67</td>
<td>Show active socket information.</td>
</tr>
<tr>
<td>show system processes on page 68</td>
<td>Show system processes.</td>
</tr>
<tr>
<td>show system queue-stats on page 69</td>
<td>Show internal queue stats.</td>
</tr>
<tr>
<td>show system statistics on page 69</td>
<td>Show system-wide protocol-related statistics.</td>
</tr>
<tr>
<td>show system usage on page 69</td>
<td>Show system usage.</td>
</tr>
<tr>
<td>show system virtual-memory on page 70</td>
<td>Show system virtual memory.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td><code>show system xms memory</code> on page 70</td>
<td>Show xms memory usage.</td>
</tr>
<tr>
<td><code>show terminal</code> on page 71</td>
<td>Show terminal settings.</td>
</tr>
<tr>
<td><code>show traffic-file</code> on page 71</td>
<td>Show network traffic from file.</td>
</tr>
<tr>
<td><code>show tse</code> on page 72</td>
<td>Show threat suppression engine information.</td>
</tr>
<tr>
<td><code>show user-disk</code> on page 73</td>
<td>Show user-disk statistics.</td>
</tr>
<tr>
<td><code>show users</code> on page 73</td>
<td>Show users information.</td>
</tr>
<tr>
<td><code>show version</code> on page 74</td>
<td>Show device version information.</td>
</tr>
<tr>
<td><code>show virtual segments</code> on page 74</td>
<td>Show virtual segment configuration.</td>
</tr>
</tbody>
</table>

### show aaa

**Syntax**

`show aaa capabilities USER`

`show aaa capabilities fred`

<table>
<thead>
<tr>
<th>ID</th>
<th>NAME</th>
<th>STATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ALL</td>
<td>full</td>
</tr>
<tr>
<td>2</td>
<td>SECURITY</td>
<td>full</td>
</tr>
<tr>
<td>7</td>
<td>SERVICES</td>
<td>full</td>
</tr>
<tr>
<td>9</td>
<td>INSPECTIONPROFILES</td>
<td>full</td>
</tr>
<tr>
<td>10</td>
<td>IPS</td>
<td>full</td>
</tr>
<tr>
<td>11</td>
<td>REPUTATION</td>
<td>full</td>
</tr>
<tr>
<td>12</td>
<td>TRAFFICMGMT</td>
<td>full</td>
</tr>
</tbody>
</table>
15 ACTIONSETS full
16 SYSTEM full
17 SMSMANAGED full
18 MANAGEMENT full
19 DNS full
20 IPFILTERS full
21 UPGRADE full
22 NOTIFICATION full
23 LOGGING full
24 HIGHAVAILABILITY full
25 HACONFIGURATION full
26 HASTATE full
27 SNMP full
28 TIME full
29 full
30 UPDATE full
31 PACKAGES full
32 AUTODV full
33 SNAPSHOT full
34 USERAUTH full
35 LOCALUSER full
36 USERGROUP full
37 ROLES full
38 RADIUS full
39 LDAP full
41 GENERAL full
42 X509CERT full
53 REPORTING full
54 LOG full
56 IPSLOG full
57 REPUTATIONLOG full
59 SYSTEMLOG full
60 AUDITLOG full
61 SECURITYREPORTS full
62 NETWORKREPORTS full
63 DEBUGTOOLS full
64 REBOOT full
65 SHUTDOWN full
66 SERVICEACCESS full
67 NETWORK full
68 INTERFACES full
69 SEGMENTS full
83 COMPACTFLASH full
84 CUSTOMCATEGORIES full
87 DEBUGNP full
88 DEBUGREPUTATION full
90 DATASECURITY full
91 OBE full
92 QUARANTINELOG full
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]

Example

ips{}show date
Sun Sept 15 04:29:59 2013 GMT
ips{}show date gmt
ips{}show date
Wed Aug 21 14:51:16 2013 America/Los_Angeles

show dns

Syntax

show dns

Example

ips{}show dns
# DNS PROXY
Proxy Disabled
# STATIC DNS
# DYNAMIC V4 DNS
# DYNAMIC V6 DNS

show filter

Displays the filters.

Syntax

show filter [XFILTERNUMBER | UDVFILTERNUMBER]
Example

show filter 10129
#10129: HTTP: Microsoft Word Memory Corruption Vulnerability
2 instances found
(Default Policy) Config: enabled  AFC: enabled
Category: vulnerabilities
TestProfile Config: enabled  AFC: enabled
Override: Block + Notify + Trace
show filter 6519
#6519: P2P: Skype Initial Login Request
1 instance found
(Application Policy) Config: enabled  AFC: enabled
Category: peer2peer
show filter 100
#0100: TFN: UDP Flood Command Acknowledgement (General)
1 instance found
(Default Policy) Config: enabled  AFC: enabled
Category: exploits
show filter 1000
#Error: Invalid filter number.
show filter 7002
#7002: TCP: Host Sweep
2 instances found
(Default Policy) Config: disabled  AFC: enabled
Category: reconprobing
threshold: 100
timeout: 300
MyTestProfile Config: enabled  AFC: enabled
Category: reconprobing
threshold: 100
timeout: 300
exception: 192.168.1.1 192.168.1.5
exception: 10.10.1.1 10.10.1.5

show health

Shows health information.

Syntax

show health

Example

ips{}show health
CPU Usage:
  Management cores: 16% used
  Health: Normal
  Data cores: 0% used
  Health: Normal

Port Links:
  Ports: 0 down
  Health: Normal

Memory:
  Current use in %: 74.5
  Current use in GBytes: 5.72
  Total capacity in GBytes: 7.68
  Health: Normal
  Warning threshold: 90 %
  Critical threshold: 95 %

SAL Restarts:
  Current: 0 restarts during the period
  Health: Normal

Disk Usage:
  /var/config: 12.8% used
  Current use in GBytes: 0.07
  Total capacity in GBytes: 0.54
  Health: Normal
  Warning threshold: 90 %
  Critical threshold: 95 %
  /var/records: 2.8% used
  Current use in GBytes: 0.01
  Total capacity in GBytes: 0.38
  Health: Normal
  Warning threshold: 90 %
  Critical threshold: 95 %
  /user: 1.9% used
  Current use in GBytes: 0.07
  Total capacity in GBytes: 3.62
  Health: Normal
  Warning threshold: 90 %
  Critical threshold: 95 %

Temperature:
  System: 24.6 degrees (C)
  Health: Normal
  Warning threshold: 62 degrees (C)
  Critical threshold: 68 degrees (C)
  CPU0: 42.0 degrees (C)
  Health: Normal
  Warning threshold: 62 degrees (C)
  Critical threshold: 68 degrees (C)

Fan Tachometer:
  Rear fan far from power supply: 6709 rpm
  Health: Normal
Warning threshold: 2550 rpm
Critical threshold: 2100 rpm
Rear fan in the center: 6717 rpm
    Health: Normal
Warning threshold: 2550 rpm
Critical threshold: 2100 rpm
Rear fan near power supply: 6608 rpm
    Health: Normal
Warning threshold: 2550 rpm
Critical threshold: 2100 rpm
Inside CPU fan near edge of board: 6295 rpm
    Health: Normal
Warning threshold: 2550 rpm
Critical threshold: 2100 rpm
Inside CPU fan near BCM heat sink: 6128 rpm
    Health: Normal
Warning threshold: 2550 rpm
Critical threshold: 2100 rpm
PSU Status:
    Power Supply Status: Present, Status not available
        Health: Normal
PSU Voltages:

<table>
<thead>
<tr>
<th>Rail</th>
<th>Voltage (V)</th>
<th>Health</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU0_VCORE</td>
<td>1.21</td>
<td>Normal</td>
</tr>
<tr>
<td>CPU0_PVDDQ_DDR</td>
<td>1.52</td>
<td>Normal</td>
</tr>
<tr>
<td>AVCC</td>
<td>3.38</td>
<td>Normal</td>
</tr>
<tr>
<td>3VCC</td>
<td>3.36</td>
<td>Normal</td>
</tr>
<tr>
<td>+3.30V</td>
<td>3.34</td>
<td>Normal</td>
</tr>
<tr>
<td>+5.00V</td>
<td>5.04</td>
<td>Normal</td>
</tr>
<tr>
<td>+12.00V</td>
<td>12.19</td>
<td>Normal</td>
</tr>
<tr>
<td>VSBB3</td>
<td>3.36</td>
<td>Normal</td>
</tr>
<tr>
<td>VBAT</td>
<td>3.31</td>
<td>Normal</td>
</tr>
</tbody>
</table>
HA status:
    Status: HA is disabled, and HA link is down
        Health: Normal

**show high-availability**

**Syntax**

`show high-availability`

**Example**

`ips{}show high-availability`

    HA Status
    --------
Intrinsic HA state: Normal
Zero-power HA state: Normal
Transparent HA state: Not Connected

Related Commands

high-availability force (active|passive)

high-availability segment force (normal|fallback)

show interface

Syntax

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

Example

ips{}show interface ha
Interface ha
MAC Address 00:10:f3:2c:81:df
Admin State Yes
Link Down
Speed 10Mbps
Auto Negotiate Enabled
Duplex Half
MTU 9216

ips{}show interface mgmt
Interface mgmt
IP Address A.B.C.D/24
IPv6 Address fe80::210:f3ff:fe2c:81de/64 (Link Local)
MAC Address 00:10:f3:2c:81:de
Admin State Yes
Link Up
Speed 1000Mbps
Auto Negotiate Enabled
Duplex Full
MTU 1500

ips{}show interface bridge1
Interface bridge1
IPv6 Address fe80::210:f3ff:fe2c:81e2/64 (Link Local)
MAC Address 00:10:f3:2c:81:e2
Admin State Yes
Link Up
MTU 1500
show key

Shows local server SSH key.

Syntax

show key

Example

ips{}show key

show license

Syntax

show license

Example

ips{}show license

License: 5.0.0.46

<table>
<thead>
<tr>
<th>Feature</th>
<th>Status</th>
<th>Permit</th>
<th>Expiration</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>License</td>
<td>OK</td>
<td>Allow</td>
<td>9/30/2015</td>
<td></td>
</tr>
<tr>
<td>Update TOS</td>
<td>OK</td>
<td>Allow</td>
<td>9/30/2015</td>
<td></td>
</tr>
<tr>
<td>Update DV</td>
<td>OK</td>
<td>Allow</td>
<td>9/30/2015</td>
<td></td>
</tr>
<tr>
<td>MalwareAuxDv</td>
<td>OK</td>
<td>Allow</td>
<td>9/30/2015</td>
<td></td>
</tr>
<tr>
<td>Auxiliary DV:ScadaAux</td>
<td>OK</td>
<td>Allow</td>
<td>9/30/2015</td>
<td></td>
</tr>
<tr>
<td>Auxiliary DV:Other</td>
<td>OK</td>
<td>Allow</td>
<td>9/30/2015</td>
<td></td>
</tr>
<tr>
<td>ReputationDV</td>
<td>OK</td>
<td>Allow</td>
<td>9/30/2015</td>
<td></td>
</tr>
<tr>
<td>SSL Inspection</td>
<td>OK</td>
<td>Allow</td>
<td>9/30/2015</td>
<td></td>
</tr>
<tr>
<td>Throughput Upgrade</td>
<td>Info</td>
<td>Deny</td>
<td>Never</td>
<td>Not licensed to use this feature.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Feature</th>
<th>Active</th>
<th>After Reboot</th>
</tr>
</thead>
<tbody>
<tr>
<td>Throughput Upgrade</td>
<td>20000 Mbps</td>
<td>No change</td>
</tr>
<tr>
<td>SSL Inspection</td>
<td>Allow</td>
<td>No change</td>
</tr>
</tbody>
</table>

show log-file

The following log files are available:

- system
- audit
- boot

54
• 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.

Example

ips{} show log-file audit more
  2013-07-05 ...(log info is displayed)
  2013-07-05 ...
  ...
  :q
ips{} show log-file boot search nocase ethernet7 count 7
ips{} show log-file boot search invert ethernet7 count 3
ips{} show log-file boot search ethernet7 count 2
ADDRCONF(NETDEV_UP): ethernet7: link is not ready
device ethernet7 entered promiscuous mode

Example

To tail the last 5 lines of the boot log file:

ips{} show log-file boot tail 5
  bridge1: port 8(ethernet7) entering disabled state
  bridge1: port 8(ethernet7) entering disabled state
  ADDRCONF(NETDEV_UP): ethernet7: link is not ready
device ethernet8 left promiscuous mode
device ethernet7 left promiscuous mode

show log-file FILE_NAME

Syntax

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

Threat Protection System Command Line Interface Reference
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]

**Example**

ips{}show log ipsAlert

**Example**

ips{}show log quarantine

**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

**Example**

ips{}show log ipsBlock stat
Display limited to 500 lines...
show log-file summary

**Syntax**

show log-file summary [verbose]

**Example**

```markdown
ips{}show log-file summary

File            Total      First      Last     Allocated  Used  Location
Entries    Entry      Entry
--------------- ---------  ---------  -------- ---------- ----  ------
system            2902     1          2902     174.32 MB     0% internal
audit             411      1          411      174.32 MB     0% internal
ipsAlert          0        0          0        350.11 MB     0% ramdisk
ipsBlock          0        0          0        350.11 MB     0% ramdisk
reputationAlert   0        0          0        175.06 MB     0% ramdisk
reputationBlock   0        0          0        175.06 MB     0% ramdisk
quarantine        0        0          0        175.06 MB     0% ramdisk
```

**show mfg-info**

Shows manufacturing information.

**Syntax**

show mfg-info

**Example**

```markdown
ips{}show mfg-info
device34{}show mfg-info

ECO Version                : 40AA
Manufacturer S/N           : TBBC10021827
PCBA Assembly Date         : 01/11/2012
Chassis Version            : 00
Mfg System Revision        : A905
Base Unit P/N              : 5066-2732
Base Unit Revision         : A1
Number of MACs             : 12
MAC Address                : 00:10:F3:2C:81:DE
Mgmt Port MAC Address      : 00:10:F3:2C:81:DE
ethernet1 MAC Address      : 00:10:F3:2C:81:E2
Base Unit S/N              : PR2AFQY003
Internal Disk Model        : 4GB SATA Flash Drive
```
Internal Disk S/N          : 11001420994500582125
External Disk Model        : 4GB SATA Flash Drive
External Disk S/N          : 00224192122400702578
BIOS Version               : Z513-021
IPM Version                : 1.d (working)

**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

**Example**

ips{}show np engine packet
  Packet Statistics:
  Rx packets OK             =             275263890
  Rx packets dropped        =                     0
  Rx packets dropped no pcb =                     0
  Tx packets OK             =             275262516
  Tx packets dropped        =                  1374
  Tx packets dropped no pcb =                     0
  Rx bytes OK               =           14864242660
  Tx bytes OK               =           16515754024

**show np general statistics**

Shows general network processor information.

**Syntax**

show np general statistics

**Example**

ips{}show np general statistics

  General Statistics:
  Incoming             =      0
  Outgoing             =      0
  Dropped              =      0
  Interface discards   =      0
show np mcfilt-rule-stats

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

Syntax

show np mcfilt-rule-stats

Example

ips{}show np mcfilt-rule-stats

<table>
<thead>
<tr>
<th>Filter</th>
<th>Flows</th>
<th>Success</th>
<th>% Total</th>
<th>% Success</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total number of flows: 0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

show np protocol-mix

Syntax

show np protocol-mix

Example

ips{}show np protocol-mix

Network Traffic Protocol Statistics:

<table>
<thead>
<tr>
<th>EthType:</th>
<th>Packets</th>
<th>Bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>=</td>
<td>=</td>
</tr>
<tr>
<td>EthType:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ARP</td>
<td>289096</td>
<td>17363292</td>
</tr>
<tr>
<td>IP</td>
<td>75851320</td>
<td>16817451395</td>
</tr>
<tr>
<td>IPv6</td>
<td>110966</td>
<td>91605367</td>
</tr>
<tr>
<td>Other</td>
<td>47087</td>
<td>31256790</td>
</tr>
<tr>
<td>IPv4 in IPv4</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>IPv4</td>
<td>75851320</td>
<td>16817451395</td>
</tr>
<tr>
<td>IPv6</td>
<td>110966</td>
<td>91605367</td>
</tr>
<tr>
<td>Other</td>
<td>9010</td>
<td>5444502</td>
</tr>
<tr>
<td>IPv4 in IPv4</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>IPv4 in IPv4</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>IPv4 in IPv4</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>IPv4 in IPv4</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
show np reassembly

Syntax

show np reassembly (ip|tcp)

Example

ips{}show np reassembly ip
    Summary:
    Frags incoming = 0
    Frags kept = 0
    Frags outgoing = 0
    Frags passed thru = 0
    Frags dropped (duplicate) = 0
    Frags recently reassembled = 0
    Frags dropped (other) = 0
    Dgrams completed = 0

show np rule-stats

Syntax

show np rule-stats

Example

ips{}show np rule-stats
    Filter  Flows  Success %Total %Success
    6281    9     0    21    0.00
    6310    9     0    21    0.00
    633     8     3    19   37.50
    5337    8     0    19    0.00
show np softlinx

Syntax

show np softlinx

Example

ips{}show np softlinx
SoftLinx Statistics:
Matched both softlinx and a rule = 0
Matched softlinx, but not a rule = 0
Matched a rule, but not softlinx = 0
Sleuth inspected packets = 0
Sleuth matched packets = 0
Matched HW (Sleuth) but notsoftLinx = 0
Sleuth gave up = 0
Sleuth bypassed = 0
Sleuth bypassed zero payload length = 0
Sleuth overflow = 0
Matched nothing = 281567607
Linx rules created = 0
Linx rules deleted = 0
Discarded by the softlinx = 0
Total packets sent to softlinx = 80
Embedded Trigger matches = 0
Engine Trigger matches = 0
Trigger matches = 0
False pkt matches = 80
Good pkt matches = 0
SoftLinx trigger match roll over = 0
Highest flow based trigger match = 0

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

Example

ips{}show np tier-stats
<table>
<thead>
<tr>
<th>Tier 1 (Physical Ports):</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rx Mbps                  = 261.7 (1,250.0)</td>
</tr>
<tr>
<td>Tx Mbps                  = 270.4 (1,248.6)</td>
</tr>
<tr>
<td>Rx Packets/Sec           = 31,054.0 (111,814.0)</td>
</tr>
<tr>
<td>Tx Packets/Sec           = 45,279.0 (111,682.0)</td>
</tr>
<tr>
<td>Utilization              = 23.7% (100.0%)</td>
</tr>
<tr>
<td>Ratio to next tier       = 100.0% [0.0%]</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Tier 2 (Software Fastpath):</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rx Mbps                     = 261.7 (838.2)</td>
</tr>
<tr>
<td>Rx Packets/Sec              = 31,054.0 (74,982.0)</td>
</tr>
<tr>
<td>Tx trust packets/sec        = 0.0 (0.0)</td>
</tr>
<tr>
<td>Utilization                 = 23.7% (76.2%)</td>
</tr>
<tr>
<td>Ratio to next tier          = 100.0% [99.6%]</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Tier 3 (IPS Engine Fastpath):</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rx Mbps                       = 261.7 (836.4)</td>
</tr>
<tr>
<td>Rx Packets/Sec                = 31,054.0 (74,781.0)</td>
</tr>
<tr>
<td>Tx trust packets/sec          = 0.0 (0.0)</td>
</tr>
<tr>
<td>Utilization                   = 23.7% (76.0%)</td>
</tr>
<tr>
<td>Ratio to next tier            = 0.0% (0.0%)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Tier 4 (IPS Engine Slowpath):</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rx Mbps                       = 0.0 (0.0)</td>
</tr>
<tr>
<td>Rx Packets/Sec                = 0.0 (2.0)</td>
</tr>
<tr>
<td>Rx due to:</td>
</tr>
<tr>
<td>Trigger match                 = 0.0% (0.0%)</td>
</tr>
<tr>
<td>Reroute                       = 0.0% (50.0%)</td>
</tr>
<tr>
<td>TCP sequence                  = 0.0% (0.0%)</td>
</tr>
<tr>
<td>Protocol decode               = 0.0% (0.0%)</td>
</tr>
<tr>
<td>Utilization                   = 0.0% (0.0%)</td>
</tr>
<tr>
<td>Ratio to deep                 = 0.0% (0.0%)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Tier 5 (SSL Inspection):</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rx Mbps                       = 252.7 (257.7)</td>
</tr>
<tr>
<td>Rx Packets/Sec                = 21,823.0 (22,256.0)</td>
</tr>
<tr>
<td>Utilization                   = 22.9% (23.4%)</td>
</tr>
</tbody>
</table>

show quarantine-list

Syntax
show quarantine-list

Example
ips{}show quarantine-list

IP Reason

show reports

Shows the status of the data collection for reports.

Syntax
show reports

Example
ips{}show reports
CPU Utilization: enabled
Disk Utilization: enabled
Fan Speed: enabled
Memory Utilization: enabled
Network Bandwidth: enabled
Rate Limiter: enabled
Temperature: enabled
Traffic Profile: enabled

show service

Shows the state of all the services.

Syntax
show service

Example
ips{}show service
Service SSH is active
Service HTTPS is active
Service SNMP is inactive
Service DNS-PROXY is inactive
Service NTP is inactive
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

Example

ips{}show slot
#############################
# SLOT INFO                  #
#############################
Slot 1
  State        : Empty
  Module Type  : Empty
Slot 2
  State        : Empty
  Module Type  : Empty

show sms

Syntax

show sms

Example

ips{}show sms
Device is not under SMS control

show snmp

Syntax

show snmp

Example

ips{}show snmp
#SNMP Status
  Enabled : Yes
  Version : 2c, 3
  Engine ID  : 0x800029ee030010f327fe2e
  Auth. Traps : Yes
System Name           : S8020F
System Object ID      : .1.3.6.1.4.1.10734.1.9.7
System ID             : TPS
System Contact        : Administrator
System Location       : Data Center

#SNMP Trap Sessions
Host                  : A.B.C.D
Version               : 3
Port                  : 162
Security Name         : trap
Level                 : authPriv
Authentication        : SHA
Privacy               : AES
Inform                : Yes

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

Example

ips{}show ssl-inspection congestion
SSL connection rate: 3.15 conn/sec
SSL current connections: 152 of max 100000 connections
SSL congested action: Pass

show system connections

Syntax

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

Example

ips{}show system connections ipv4
Active Internet connections (servers and established)
vrfid Proto Recv-Q Send-Q Local Address Foreign Address State
 0  tcp  0    0 127.0.0.1:60000 0.0.0.0:* LISTEN
 0  tcp  0    0 127.0.0.1:616  0.0.0.0:* LISTEN

Example
ips{}show system connections unix
Active UNIX domain sockets (servers and established)

<table>
<thead>
<tr>
<th>Proto</th>
<th>RefCnt</th>
<th>Flags</th>
<th>Type</th>
<th>State</th>
<th>I-Node</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>unix</td>
<td>2</td>
<td>[ACC]</td>
<td>STREAM</td>
<td>LISTENING</td>
<td>40709</td>
<td>/var/tmp/apache2/logs/fcgidsock/7095.0</td>
</tr>
<tr>
<td>unix</td>
<td>2</td>
<td>[ACC]</td>
<td>STREAM</td>
<td>LISTENING</td>
<td>3871</td>
<td>/var/tmp/segmentdsock</td>
</tr>
<tr>
<td>unix</td>
<td>2</td>
<td>[ACC]</td>
<td>STREAM</td>
<td>LISTENING</td>
<td>2080</td>
<td>/var/run/nscd/socket</td>
</tr>
<tr>
<td>unix</td>
<td>2</td>
<td>[ACC]</td>
<td>STREAM</td>
<td>LISTENING</td>
<td>379</td>
<td>@/com/ubuntu/upstart</td>
</tr>
<tr>
<td>unix</td>
<td>2</td>
<td>[ACC]</td>
<td>STREAM</td>
<td>LISTENING</td>
<td>16968</td>
<td>/var/run/xms.default</td>
</tr>
<tr>
<td>unix</td>
<td>2</td>
<td>[ ]</td>
<td>DGRAM</td>
<td></td>
<td>16970</td>
<td>/tmp/.server.socketname</td>
</tr>
<tr>
<td>unix</td>
<td>2</td>
<td>[ ]</td>
<td>DGRAM</td>
<td></td>
<td>17575</td>
<td>@/tmp/.has_xmsd</td>
</tr>
<tr>
<td>unix</td>
<td>2</td>
<td>[ACC]</td>
<td>STREAM</td>
<td>LISTENING</td>
<td>1436</td>
<td>/usr/local/var/syslog-ng.ctl</td>
</tr>
</tbody>
</table>

Example

ips{}show system connections sctp

ASSOC SOCK STY SST ST HBKT ASSOC-ID TX_QUEUE RX_QUEUE UID INODE LPORT RPORT
LADDRS <-> RADDRS HBINT INS OUTS MAXRT T1X T2X RTXC VRF

show system processes

Syntax

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

Example

ips{}show system processes brief

```
  top - 02:23:22 up 5:08, 2 users, load average: 16.20, 16.23, 16.16
  Tasks: 349 total, 6 running, 343 sleeping, 0 stopped, 0 zombie
  Cpu(s): 37.8% us, 2.4% sy, 0.0% ni, 52.8% id, 0.0% wa, 0.0% hi, 6.9% si
  Mem: 28681276k total, 10367048k used, 18314228k free, 100416k buffers
  Swap: 0k total, 0k used, 0k free, 1638220k cached

   PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM   TIME+ COMMAND
3656 root      20   0   11.1g  4.6g  3.7g R  1200 16.7  3691:24   n0
3731 root      20   0   0    0    0  R  100  0.0  307:25.33 dpvi-task3
3730 root      20   0   0    0    0  R  980.0 303:42.33 dpvi-task2
3729 root      20   0   0    0    0  R  960.0 300:14.52 dpvi-task1
2941 root      20   0  84516 3976 2852 R  2  0.0  4:18.44 syslog-ng
4436 root      20   0   0    0    0  D  2  0.0  1:44.56 fpm-nfct-hf-tas
4216 root      20   0  21496 1112 772 D  0  0.0  0:21.46 sensormond
17380root     20   0  13084 1292 800 R  0  0.0  0:00.01 top
```
**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]
```

**Example**

```
ips{}show system statistics
Valid entries at this position are:
<Enter> Execute command
fast-path Fast path statistics
management Show protocol-related information for management and HA interfaces
non-zero Only non-zero counters
show system statistics management
Valid entries at this position are:
<Enter> Execute command
inet Statistics of V4 family
inet6 Statistics of V6 family
ipv4 IPv4 statistics
ipv6 IPv6 statistics
icmpv4 ICMPv4 statistics
icmpv6 ICMPv6 statistics
igmp IGMP statistics
tcpv4 TCPv4 statistics
tcpv6 TCPv6 statistics
udpv4 UDPv4 statistics
udpv6 UDPv6 statistics
ipsecv4 IPsec IPv4 statistics
ipsecv6 IPsec IPv6 statistics
sctp SCTP statistics
non-zero Only non-zero counters
```

**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]
```

**Example**

```
ips{} show system usage update 12
```

**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
```

**Example**

```
ips{} show system virtual-memory
```

**show system xms memory**

Shows xms memory statistics.
Syntax

show system xms memory (all| SERVICE)

Example

ips{}show system xms memory snmp
xmsd memory usage :
+ Service: snmp
    + snmp: 840 Bytes
      Maximum amounts: 840 Bytes
      Calls to alloc : 1 times
+ Service: misc
    + miscellaneous: 1663 Bytes
      Maximum amounts: 1864 Bytes
      Calls to alloc : 10 times
    + xmlMem: 3696468 Bytes
      Maximum amounts: 5032841 Bytes
      Calls to alloc : 19441 times

show terminal

Shows terminal type information.

Syntax

show terminal

Example

ips{}show terminal

============
Terminal configuration:
type tpterm
columns 164
lines 46

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

Example

ips{}show traffic-file myfilename

show tse

Shows threat suppression engine information.

Syntax

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

Example of connection-table blocks

ips{}show tse connection-table blocks
Blocked connections: 1 of 1 shown.

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Src/Dest IP</th>
<th>Port</th>
<th>Src/Dest IP</th>
<th>Port</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
<td>10.1.3.1</td>
<td>36051</td>
<td>10.1.3.2</td>
<td>44</td>
<td>6551: TCP: IPS Test Filter</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Virtual Segment ID</th>
<th>In Interface</th>
<th>Out Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>segment6 (A &gt; B)</td>
<td>unknown</td>
<td>unknown</td>
</tr>
</tbody>
</table>

Example of rate-limit

ips{}show tse rate-limit
Rate limit streams: 1 of 1 shown.

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Src/Dest IP</th>
<th>Port</th>
<th>Src/Dest IP</th>
<th>Port</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
<td>10.1.3.1</td>
<td>36052</td>
<td>10.1.3.2</td>
<td>44</td>
<td>6551: TCP: IPS Test Filter</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Virtual Segment ID</th>
<th>In Interface</th>
<th>Out Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>segment6 (A &gt; B)</td>
<td>unknown</td>
<td>unknown</td>
</tr>
</tbody>
</table>

Example of ssl-inspection

ips{}show tse ssl-inspection
SSL Inspected Sessions: 1 of 1 shown.
<table>
<thead>
<tr>
<th>Client IP</th>
<th>Port</th>
<th>Interface</th>
<th>Proto</th>
<th>Cipher</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1.3.1</td>
<td>42523</td>
<td>5B</td>
<td>TLSv1.2</td>
<td>TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384</td>
</tr>
<tr>
<td>Server IP</td>
<td>Port</td>
<td>Interface</td>
<td>Proto</td>
<td>Cipher</td>
</tr>
<tr>
<td>10.1.3.2</td>
<td>443</td>
<td>5A</td>
<td>TLSv1.2</td>
<td>TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384</td>
</tr>
</tbody>
</table>

**show tse connection-table**

**Syntax**

```none
show tse connection-table TYPE
```

**Example**

This example displays the basic IPS state synchronization by viewing the connection table on the active and passive device.

```none
ips{}show tse connection-table blocks
```

**Second device**

```none
ips{}show tse connection-table blocks
```

The ‘TRHA’ indicates this is a connection created by state synchronization.

**show user-disk**

**Syntax**

```none
show user-disk
```

**Example**

```none
ips{}show user-disk
```

**External User Disk**

<table>
<thead>
<tr>
<th>Status:</th>
<th>Mounted</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption:</td>
<td>None</td>
</tr>
<tr>
<td>Capacity:</td>
<td>3952263168 bytes</td>
</tr>
<tr>
<td>Used:</td>
<td>784158720 bytes</td>
</tr>
<tr>
<td>Free:</td>
<td>2907357184 bytes</td>
</tr>
</tbody>
</table>

**show users**

**Syntax**

```none
show users [locked|ip-locked]
```
Example

ips{}show users
USER        IDLE    INTERFACE  LOGIN                IPADDRESS        TYPE
myadminuser  00:00   SSH        2013-07-19 23:42:56 198.51.100.139   LOCAL

show version

Syntax

show version

Example

ips{}show version
    Serial: X-TPS-2200T-STLAB-0057
    Software: 4.1.0.4401 Build Date: "Dec 18 2015 16:51:29"
    Development [28892M]
    Digital Vaccine: 3.2.0.8790
    Reputation DV: N/A
    Model: 2200T (IPS)
    HW Serial: PR49A2J041
    HW Revision: 2200
    Failsafe: 1.3.0.7751
    Throughput: 1000 Mbps
    System Boot Time: Tue Dec 22 16:22:52 2015
    Uptime: 00:11:05

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
Example

ips{}sms unmanage
ips{}sms must-be-ip 192.168.1.1

Related commands

*show sms* on page 66

### 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

**Example**

```
ips{}snapshot create s_041713
```

### snapshot list

**Syntax**

```
snapshot list
```

**Example**

```
ips{}snapshot list
```

<table>
<thead>
<tr>
<th>Name</th>
<th>Date</th>
<th>OS Version</th>
<th>DV</th>
</tr>
</thead>
<tbody>
<tr>
<td>s_041713</td>
<td>Wednesday, April 17 2013</td>
<td>1.0.0.3913</td>
<td>3.2.0.15172</td>
</tr>
<tr>
<td>Version</td>
<td>Model</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Restore</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>440T</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
snapshot remove

Syntax
snapshot remove

Example
ips{}snapshot remove s_041713
Success

snapshot restore

Restores system from saved snapshot.

Syntax
snapshot restore NAME

Example
ips{}snapshot restore s_041713
Success

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 1-100000000]] [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

Example
ips{}tcpdump mgmt count 2
ips{}tcpdump bridge0 record mycapturefile count 100 proto tcp without udp pcap "dst port 443" background
**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 RADIUS 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]
```

**Usage**

```
ips{}tech-support-report include-snapshot exclude-traffic-logs
Do you wish to run the report now (y/n)? [n]: y
Generating Tech Support Report. This may take a moment...
Tech Support Report successfully created and may be exported via the LSM.
```
NOTE: this report will persist after a device reboot.

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 [from X::X:X]

Example

ips{}traceroute 192.168.140.254
traceroute: Warning: ip checksums disabled
traceroute to 192.168.140.254 (192.168.140.254), 30 hops max, 46 byte packets
1 192.168.140.254 (192.168.140.254) 0.256 ms 0.249 ms 0.233 ms

traceroute6

Trace IPv6 network routes.

Example

ips{}traceroute6 192.168.140.1

user-disk

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

If the system master key is set, you can also use this command to encrypt the external CFast. By default, the external CFast is not encrypted. For information about setting the system master key, see `master-key` on page 38.

To enable the device to automatically mount the external CFast at boot, the user disk must be seated properly during initial installation, or you must format and mount the disk.

⚠️ Caution: If you change the encryption status of the external CFast, the external CFast automatically formats and any existing data on the disk is erased.

The external CFast can also be encrypted and decrypted from the LSM at System > Settings > Data Security.

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

Example

Unmount the external user disk.

ips{}user-disk unmount
WARNING: Unmounting the external user disk will disable snapshot and packet capture, and traffic related logs will be stored in memory only.
Do you want to continue (y/n)? [n]: y
Success: User disk unmounted.

Example

Mount the external disk and enable the device to automatically mount the disk on boot.

ips{}user-disk mount
Note: The external user disk will be used for snapshots, packet captures and traffic related logs. The external user disk will be automatically mounted on rebooted.
Do you want to continue (y/n)? [n]: y
Success: User disk mounted.

Example

Format the disk.

ips{}user-disk format
WARNING: This action will erase all existing data on the external user disk!
Do you want to continue (y/n)? [n]: y
Success: User disk format completed.

Example

Enable encryption on the external disk.

ips{}user-disk encryption enable
WARNING: Changing the encryption status of the user disk will erase all traffic log, snapshot, and packet capture data on the disk.
Do you want to continue (y/n)? [n]: y
Success: User disk encryption enabled.

Related commands

show user-disk on page 73
master-key on page 38
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]

ips{log-configure}display
# LOG EMAIL SETTINGS
email set sleepSeconds   300
email set maxRequeue     2016
# LOG ROTATE SETTINGS
rotate set sleepSeconds   600
rotate set defaultFiles   5
rotate set defaultCheckRecords 500
rotate set rotateMsgSeverity info
rotate set maxFileSize    100 MB
# LOG FILE DISK ALLOCATION
log-storage external 90%
log-storage ramdisk 25%
# LOG FILE ALLOCATION SETTINGS
# INTERNAL DISK
log-file-size system          50%
log-file-size audit           50%
#    ----
#    Total 100%
# EXTERNAL DISK (USER-DISK)
log-file-size ipsAlert        30%
log-file-size ipsBlock        30%
log-file-size reputationAlert 15%
log-file-size reputationBlock 15%
log-file-size quarantine      10%
#    ----
#    Total 100%
email

Allows you to set logging email daemon parameters.

Syntax

e-mail set sleepSeconds SLEEPSEC
e-mail set maxRequeue MAXREQUEUE
e-mail delete (sleepSeconds|maxRequeue)

Example

ips{log-configure}email set sleepSeconds 600
ips{log-configure}email delete sleepSeconds
ips{log-configure}email set maxRequeue 1
ips{log-configure}email delete 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

Example

ips{log-configure}log-file-size system 50
ips{log-configure}log-file-size audit 60
ERROR: This would over allocate (110%) the Internal log disk!
log-storage

Sets local log file allocation of external CFast disk space. Usage value can range from 50 to 99 percent.

Syntax

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

Example

ips{log-configure}log-storage external 90

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
Example

ips{log-configure}log-test logID 1 msg "my test message for logging"
ips{log-configure}log-test all

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

Example

ips{log-configure}rotate set sleepSeconds 10
ips{log-configure}rotate set visibility Files 5 Records 500
ips{log-configure}rotate delete visibility
ips{log-configure}rotate set defaultCheckRecords 500
ips{log-configure}rotate set defaultFiles 5
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.

This section is divided as follows:

- **Edit context commands** on page 84
- **Contexts and related commands** on page 99

## Edit context commands

**aaa**

aaa
ips{}edit
ips{running}aaa
ips{running-aaa}help
ips{running-aaa}display user fred xml
<?xml version="1.0"?>
<record>
<index>
<user>fred</user>
</index>
<parameters>
<password>$password$</password>
<epoch>1373049840</epoch>
</parameters>
</record>
ips{running-aaa}

**Related Commands**

`running-aaa Context Commands` on page 99
actionsets

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

Example

ips{}edit
ips{running}actionsets
ips{running-actionsets}help

Example

ips{running-actionsets}actionset myactionset
ips{running-actionsets-myactionset}help
ips{running-actionsets-myactionset}?
Valid entries at this position are:

<table>
<thead>
<tr>
<th>entry</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>action</td>
<td>Set action type, available value: permit, rate-limit, block, trust</td>
</tr>
<tr>
<td>allow-access</td>
<td>Allow quarantined host to access defined IP</td>
</tr>
<tr>
<td>bytes-to-capture</td>
<td>Set bytes to capture for packet trace</td>
</tr>
<tr>
<td>contact</td>
<td>Add a notify contact</td>
</tr>
<tr>
<td>delete</td>
<td>Delete file or configuration item</td>
</tr>
<tr>
<td>display</td>
<td>Display file or configuration item</td>
</tr>
<tr>
<td>help</td>
<td>Display help information</td>
</tr>
<tr>
<td>http-block</td>
<td>Set quarantine option to block HTTP traffic</td>
</tr>
<tr>
<td>http-custom</td>
<td>Set or clear HTTP custom text display option</td>
</tr>
<tr>
<td>http-redirect</td>
<td>Set redirect URL for HTTP redirect option</td>
</tr>
<tr>
<td>http-showdesc</td>
<td>Set or clear HTTP show desc display option</td>
</tr>
<tr>
<td>http-showname</td>
<td>Set or clear HTTP show name display option</td>
</tr>
<tr>
<td>limit-quarantine</td>
<td>Add IP for limit quarantine</td>
</tr>
<tr>
<td>limit-rate</td>
<td>Set the rate value for rate-limit action</td>
</tr>
<tr>
<td>no-quarantine</td>
<td>Add IP for no quarantine</td>
</tr>
<tr>
<td>nonhttp-block</td>
<td>Set quarantine option to block non-HTTP traffic</td>
</tr>
<tr>
<td>packet-trace</td>
<td>Enable/disable packet trace option</td>
</tr>
<tr>
<td>priority</td>
<td>Set packet trace priority</td>
</tr>
<tr>
<td>quarantine</td>
<td>Set quarantine option, available value: no, immediate, threshold</td>
</tr>
<tr>
<td>tcp-reset</td>
<td>Set tcp reset option for block action, can be disable, source, dest or both</td>
</tr>
<tr>
<td>threshold</td>
<td>Set quarantine threshold value</td>
</tr>
<tr>
<td>verbosity</td>
<td>Set packet trace verbosity</td>
</tr>
</tbody>
</table>

autodv

Enters Auto Digital Vaccine context mode.
Syntax

autodv

ips{running}autodv
Entering Immediate Commit Feature. Changes take effect immediately.
ips{running-autodv}help
Valid commands are:
calendar
delete proxy
delete proxy-password
delete proxy-username
disable
display
enable
help [full|COMMAND]
list
periodic
proxy ADDR port PORT
proxy-password PASSWD
proxy-username USER
update
ips{running-autodv}? 
Valid entries at this position are:
calendar Enter Calendar Style
delete Delete file or configuration item
disable Disable service
display Display file or configuration item
enable Enable service
help Display help information
list List Installed DVs
periodic Enter Periodic Style
proxy Configure proxy
proxy-password Proxy password
proxy-username Proxy username
update Update AutoDV

blockedStreams

Enters blockedStreams context mode.

Syntax

blockedStreams

Example

ips{running}blockedStreams
ips{running-blockedStreams}help
Valid commands are:
flushallstreams
flushstreams
help [full|COMMAND]
list

certificates
Enters certificates context mode.

Syntax
certificates

Example
ips{running}certificates
ips{running-certificates}help
Valid commands are:
  ca-certificate CANAME
  cert-request CERTREQUEST [key-size SIZE]
  certificate CERTNAME
  delete ca-certificate (all|CANAME)
  delete cert-request (all|CERTREQUEST)
  delete certificate (all|CERTNAME)
  display cert-request CERTNAME
  display certificate CERTNAME [pem|text]
  display [default] ca-certificate CANAME [pem|text]
  help [full|COMMAND]
  private-key CERTNAME
  reload default-ca-list

debug
Enters debug context mode.

Syntax
debug

debug

Example
ips{running}debug
ips{running-debug}help
Valid commands are:
  display [xml]
  help [full|COMMAND]
  sysrq enable|disable
delete

Deletes file or configuration item.

**Syntax**

delete interface

**Example**

ips{running}delete interface vrrpvXgY

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

**Example**

ips{running}dns
ips{running-dns}help

Valid commands are:

delete domain-name
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
domain-name NAME
domain-search primary NAME
help [full|COMMAND]
name-server A.B.C.D|X:X::X:X
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
proxy enable|disable
ips{running-dns}?

Valid entries at this position are:
delete Delete file or configuration item
domain-name Configure domain name
domain-search Configure domain search
help Display help information
name-server Configure DNS server
proxy Configure proxy
proxy Enable or disable proxy

gen

Enters general context mode.

Syntax

gen

Example

ips{running}gen
ips{running-gen}help

Valid commands are:
# System commands
timezone (GMT|(REGION CITY))
# Manage context
display [xml]
# Other commands
arp A.B.C.D INTERFACE MAC
auto-restart enable|disable
delete arp all|(ENTRY INTERFACE)
delete host NAME|all
delete ndp all|(ENTRY INTERFACE)
ephemeral-port-range default|(LOWRANGE HIGHRANGE)
forwarding ipv4|ipv6 enable|disable
help [full|COMMAND]
host NAME A.B.C.D|X:X::X:X
https enable|disable
ssh enable|disable
xmsd remote (port PORT [address A.B.C.D])|disable
ips{running-gen}?
Valid entries at this position are:
arp Configure static ARP entry
auto-restart Enable/disable automatic restart on detection of critical
    problem
delete Delete file or configuration item
display Display general context
ephemeral-
    port-range Set the range of the ephemeral port (default is 32768-61000)
forwarding Enable or disable IPv4/IPv6 forwarding
help Display help information
host Configure static address to host name association
https Enable or disable WEB server configuration
ssh Enable or disable ssh service
timezone Display or configure time zone

high-availability

Enters high-availability context mode.

Syntax

high-availability

Example

ips{running}high-availability
ips{running-high-availability}help
Valid commands are:
    enable|disable
    encryption (passphrase PASSPHRASE)|enable|disable
    help [full|COMMAND]
    partner SERIAL
ips{running-high-availability}?
Valid entries at this position are:
    disable Disable TRHA
    enable Enable TRHA
    encryption Apply encryption hash
    help Display help information
    partner Serial number of the partner

interface

Enters interface context mode. The X represents a number to be entered, such as ethernet2.

Syntax

# Enter context
interface ethernetX
interface mgmt
Example

ips{running}interface ethernet2
ips{running-ethernet2}?
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

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

Example

ips{running}ips
Entering Immediate Commit Feature. Changes take effect immediately.
ips{running-ips}help
Valid commands are:
  # Enter context
display-categoryrules
  # Other commands
afc-mode AFCMODE
afc-severity SEVERITY
asymmetric-network enable|disable
client-ip enable|disable
connection-table TIMEOUTTYPE SECONDS
delete profile XPROFILENAME
deployment-choices
display
gzip-decompression enable|disable
help [full|COMMAND]
http-encoded-resp (accelerated|inspect url-nrc STATUS)|ignore
http-mode enable|disable
ids-mode IDSMODE
profile PROFILENAME
quarantine-duration DURATION
rename profile XPROFILENAME NEWPROFILENAME
ips{running-ips}?
Valid entries at this position are:

- **afc-mode**                AFC mode
- **afc-severity**            AFC severity
- **asymmetric-network**      Asymmetric network mode
- **connection-table**        Connection table timeout
- **delete**                  Delete a profile
- **deployment-choices**      Get deployment choices
- **display**                 Display all ips configuration and profiles
- **display-categoryrules**   Display category rules for all profiles
- **gzip-decompression**      GZIP decompression mode
- **help**                    Display help information
- **http-encoded-resp**       Inspection of encoded HTTP responses
- **http-mode**               HTTP mode
- **ids-mode**                IDS mode
- **profile**                 Create/enter a IPS profile
- **quarantine-duration**     Quarantine duration
- **rename**                  Rename a profile

**log**

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

**Syntax**

log

**Example**

ips{running}log
ips{running-log}display

# LOG SERVICES
log system "Management Console" notice
#log audit "Management Console" ALL

# TRAFFIC LOGS
log quarantine "Management Console" ALL

# SUB-SERVICES
sub-system INIT info
sub-system XMS notice
sub-system TOS info
sub-system HTTPD notice
sub-system LOGIN notice
sub-system COROSYNC notice
sub-system CRMADMIN none

# PERFORMANCE PROTECTION
logging-mode conditional threshold 1% period 600
**notifycontacts**

Enters notify contacts context mode.

**Syntax**

```
notifycontacts
```

**Example**

```
ips{running}notifycontacts
Entering Immediate Commit Feature. Changes take effect immediately.
ips{running-notifycontacts}help
Valid commands are:
    contact CONTACTNAME
    contact NEWNAME email
    contact NEWNAME snmp COMMUNITY IP [PORT]
    delete EMAILSETTING
    delete contact XCONTACTNAME
    display
    email-from-address EMAIL
    email-from-domain DOMAIN
    email-server IP
    email-threshold THRESHOLD
    email-to-default-address EMAIL
    help [full|COMMAND]
    rename contact XCONTACTNAME NEWNAME
ips{running-notifycontacts}?
Valid entries at this position are:
    contact                    Create or edit a notify contact
    delete                    Delete file or configuration item
    display                   Display all available contacts
    email-from-address        From email address
    email-from-domain         From domain name
    email-server              Set mail server IP
    email-threshold           Set email threshold
    email-to-default-address  Default to email address
    help                      Display help information
    rename                    Rename contact with new name
```

**ntp**

Enters notify contacts context mode.

**Syntax**

```
ntp
```
**Example**

ips{running}ntp
ips{running-ntp}help
Valid commands are:
delete key all|ID
delete server all|HOST
help [full|COMMAND]
key (1-65535) VALUE
ntp enable|disable
polling-interval SECONDS
server dhcp|NAME [key ID] [prefer]
ips{running-ntp}?
Valid entries at this position are:
delete Delete file or configuration item
help Display help information
key Configure NTP authentication key
ntp Enable or disable NTP
polling-interval Configure minimum polling interval
server Configure remote NTP server

**reputation**

Enters Reputation context mode.

**Syntax**

reputation

**Example**

ips{running}reputation
Entering Immediate Commit Feature. Changes take effect immediately.
ips{running-rep}help
Valid commands are:
delete group USERGROUP
delete profile XPROFILENAME
display
group USERGROUP
help [full|COMMAND]
nxdomain-response enable|disable
profile PROFILENAME
rename group USERGROUP NEWUSERGROUP
rename profile XPROFILENAME NEWPROFILENAME
ips{running-rep}?
Valid entries at this position are:
delete Delete file or configuration item
display Display all reputation profiles and groups
security-policy-reset

Resets IPS security policy to the default values.

Syntax

security-policy-reset

Example

ips{running}security-policy-reset
WARNING!!!
This command WILL reset more of the IPS configuration than you may intend.
This will remove all user-configured security configuration from the device,
including virtual segments and profiles.
You will NOT be able to recover any of this data from the IPS after this
command has been confirmed.
This command will also commit any pending configuration changes to the device
and copy the running configuration to the start config.
Warning: Type the word 'COMMIT' to continue:

segmentX

Enters Segment context mode. The X represents a segment number, for example segment0.

Syntax

segmentX

Example

ips{running}segment2
ips{running-segment2}help
Valid commands are:
  # Enter context
  high-availability mode
  link-down breaker [wait-time WAIT-TIME]
  link-down hub
  link-down wire [wait-time WAIT-TIME]
  restart
  # Other commands
  description TEXT
  help [full|COMMAND]
ips{running-segment0}?
Valid entries at this position are:
  description          Enter description for the segment
  help                 Display help information
  high-availability    Intrinsic HA Layer 2 Fallback action
  link-down            Link down synchronization mode
  restart              Restart both Ethernet ports of segment

services

Enters services context mode.

Syntax

services

Example

ips{running}services
Entering Immediate Commit Feature. Changes take effect immediately.
ips{running-services}help
Valid commands are:
  display
  help [full|COMMAND]
  service SERVICE
ips{running-services}?  
Valid entries at this position are:
  display              Display all services
  help                 Display help information
  service              Edit a service

snmp

Enters SNMP context mode.

Syntax

snmp

Example

ips{running}snmp
ips{running-snmp}help
Valid commands are:
  authtrap enable|disable
  community COMMUNITY SOURCE
  delete community COMMUNITY|all
  delete trapdest (HOST ver VERSION)|all
  delete username (USERNAME|all)
help [full|COMMAND]
snmp enable|disable
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 PRIVPROTO [PRIVPASS] [inform]
username USERNAME
username USERNAME authtype AUTHTYPE AUTHPASS
username USERNAME authtype AUTHTYPE AUTHPASS privproto PRIVPROTO [PRIVPASS]
ips{running-snmp}?
Valid entries at this position are:
authtrap Configure SNMP authentication failure trap
community Configure SNMP read-only community
delete Delete file or configuration item
gineID Configure SNMPv3 engine ID
help Display help information
snmp Enable or disable SNMP
trapsession Configure a trap/inform
username Configure SNMPv3 USM read-only user

ssl-inspection

Enters SSL inspection context mode.

Syntax

ssl-inspection

Example

ips{running}ssl-inspection
ips{running-sslinsp}help
Valid commands are:
delete log sslInspection CONTACT-NAME
delete profile (all|PROFILE_NAME)
delete server (all|SERVER_NAME)
enable|disable
help [full|COMMAND]
log sslInspection CONTACT-NAME [ALL|none]
profile PROFILE_NAME
rename profile PROFILE_NAME NEW_PROFILE_NAME
rename server SERVER_NAME NEW_SERVER_NAME
server SERVER_NAME

Related commands
### Command

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>certificates</td>
<td>Store security certificates and private keys on the TPS as device certificates.</td>
</tr>
<tr>
<td>virtual-segments</td>
<td>Assign an SSL inspection profile to a virtual segment.</td>
</tr>
</tbody>
</table>

### traffic-management

Enters traffic-management profile context.

**Syntax**

```
traffic-management
```

**Example**

```
ips{running}traffic-management
ips{running-trafmgmt}help
```

Valid commands are:

- # Manage context
  - display
- # Other commands
  - delete profile TRAFPROFNAME
  - help [full|COMMAND]
  - profile NEWTRAFPROFNAME
  - profile TRAFPROFNAME
  - rename profile TRAFPROFNAME NEWTRAFPROFNAME

```
ips{running-trafmgmt}?
```

Valid entries at this position are:

- delete Delete file or configuration item
- display Display traffic-management profiles context
- help Display help information
- profile Create/enter traffic-management profile context
- rename Rename traffic-management profile

### virtual-segments

Enters virtual-segments context.

**Syntax**

```
virtual-segments
```
Example

```plaintext
ips{running}virtual-segments
ips{running-vsegs}help
Valid commands are:
  delete virtual-segment VSEGNAME
  help [full|COMMAND]
  rename virtual-segment VSEGNAME NEWVSEGNAME
  virtual-segment NEWVSEGNAME
  virtual-segment VSEGNAME
```

**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**

```plaintext
delete ldap-group (LDAPNAME|all)
delete radius-group (RADIUSNAME|all)
delete role (ROLE|all)
delete user (USER|all)
delete user-group (USERGROUP|all)
```

Enter the delete subcommand and delete the LDAP group named "group1":

```plaintext
ips{running-aaa}delete ldap-group group1
ips{running-aaa}delete radius-group group1
ips{running-aaa}delete role myrole1
ips{running-aaa}delete user myuser1
ips{running-aaa}delete user-group group1
```

**ips{running-aaa}display**

Display configuration.

**Syntax**

```plaintext
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 user USER [xml]
display usergroup USERGROUP [xml]

Example

ips{running-aaa}display ldap-group group1
ips{running-aaa}display ldap-schema active-directory
ips{running-aaa}display login-settings
ips{running-aaa}display password-settings
ips{running-aaa}display radius-group group1
ips{running-aaa}display remote-login-group
ips{running-aaa}display role superuserRole
ips{running-aaa}display user myuser1
ips{running-aaa}display usergroup group1

ips{running-aaa}ldap-group

Configure LDAP group. Maximum number of groups is two.

Syntax

ldap-group LDAPNAME

Example

ips{running-aaa}ldap-group mygroup

ips{running-aaa}ldap-schema

Configure LDAP schema.

Syntax

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

Example

ips{running-aaa}ldap-schema custom
ips{running-aaa-ldap-schema-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
Configure login settings
Syntax: login maximum-attempts LOGINATTEMPTS
       login failure-action FAILURE-ACTION
       login lockout-period DURATION
       login cli-inactive-timeout [MINUTES]
       login lsm-inactive-timeout [MINUTES]
       login Configure login settings
       maximum-attempts Configure login maximum attempts
       LOGINATTEMPTS login maximum-attempts number. Range is 1-10
       failure-action Configure action for login failure
       FAILURE-ACTION Action to be performed when login is failed
       Possible values for FAILURE-ACTION are:
       lockout-disable Disable the account and lockout the IP address
       lockout Lockout the account and IP address for the
       lockout-period
       audit Notify in audit log each failed login exceeding
       maximum-attempts
       lockout-period Configure login lockout period
       DURATION login lockout-period in minutes. Range is 1-1440 minutes
       cli-inactive-timeout Configure time at which a CLI session is terminated due
       to inactivity
       MINUTES Inactive timeout in minutes. Range is 5-180. Default
       is 15
       lsm-inactive-timeout Configure time at which an LSM session is terminated
       due to inactivity

ips{running-aaa}password
Configure password settings.

Syntax

password quality (basic|maximum|none)
password expiry-time (10d|20d|30d|45d|60d|90d|6m|1y)
password expiry-action (force-change|notify-user|disable-account)
Example

```plaintext
ips{running-aaa}password quality maximum
ips{running-aaa}password expiry-time 30d
ips{running-aaa}password expiry-action force-change
```

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

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

**Syntax**

```plaintext
radius-group RADIUSNAME
```

**Example**

```plaintext
ips{running-aaa}radius-group group1
```

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

Configure LDAP or RADIUS group to use for administrative login.

**Syntax**

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

**Example**

```plaintext
ips{running-aaa}remote-login-group administrator group1
```

**ips{running-aaa}role**

Configure an access role.

**Syntax**

```plaintext
role ROLE [OLDROLE]
```

**Example**

```plaintext
ips{running-aaa}role myrole1
```

**ips{running-aaa}user**

Configure a name identified user.

**Syntax**

```plaintext
user NAME
```
Example

ips{running-aaa}user myuser1

ips{running-aaa}user-group

Configure a name identified usergroup.

Syntax

user-group GROUPNAME

Example

ips{running-aaa}user-group group1

**aaa debug ldap test-bind**

This command tests the configuration to bind to the LDAP servers configured for network or administrative logins. It tries each server in the LDAP group in sequence. If the bind to a server is not successful, it attempts a sequence of diagnostic checks to determine the connectivity issue. These include DNS, ping and TCP connectivity checks.

**Certificate Usage**

- All commands use the certificate information from the system configured certificates.
- If an LDAP group is configured to enable `tls require-valid-server-cert`, the certificate needs to be trusted. You can set this with the `vpn ipsec trust` CLI command or in the LSM, in the Trusted Certificate Authorities section of the VPN IPsec page.

**Syntax**

deploy aaa ldap test-bind [admin | network]

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin</td>
<td>Tests connectivity to the LDAP group configured for administrative login.</td>
</tr>
<tr>
<td>network</td>
<td>Tests connectivity to the LDAP group configured for network login.</td>
</tr>
</tbody>
</table>

**Example**

ips{} debug aaa ldap test-bind network
Using following configuration:
LDAP group 'foobar'
Management network
   Server 1.2.3.4: SUCCESS
   Server 2.3.4.5: SUCCESS

aaa debug ldap authenticate-user

Prompts for the user's password to verify that the user can authenticate. Apart from this, the remainder of the command's behavior is identical to the lookup-user command.

Syntax

dump aa acl debug ldap authenticate-user [admin | network ] username

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin</td>
<td>Authenticates the user using the LDAP group configured for administrative login.</td>
</tr>
<tr>
<td>network</td>
<td>Authenticates the user using the LDAP group configured for network login.</td>
</tr>
</tbody>
</table>

Example

The following examples uses the administrative login group to test a user's administrative role. The WARNING indicates the user is not a member of the administrative group:

```shell
ips{}debug aaa ldap authenticate-user admin user1
Enter password: *******
Using the following configuration:
   LDAP group 'ldapgroup'
   Management port network
   Server: 10.20.4.55
Result: Success
User DN: CN=user1,CN=Users,DC=AD01-AC,DC=local
User LDAP group membership:
   CN=Domain Admins,CN=Users,DC=AD01-AC,DC=local
WARNING: User 'user1' is not a member of a user group or administrative role, therefore cannot login to the administrative interface
```

aaa debug ldap lookup-user

Looks up an individual user on the LDAP server to determine the user's group membership and administrative role; it does not perform an authentication so the user's password is not required.
You can use this command to diagnose user-based policy or administrative login problems after you determine that the device can successfully bind to all of the LDAP servers in the configured LDAP group.

This command binds to the first LDAP server in the group and queries the server for the user. It then returns the groups and roles that the user is a member of or an appropriate error. You can then cross-check this information against the IPS policy and administrative login configuration.

**Syntax**

```plaintext
ips{}debug aaa ldap lookup-user [admin | network ] username
```

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin</td>
<td>Looks up the user using the LDAP group configured for administrative login.</td>
</tr>
<tr>
<td>network</td>
<td>Looks up the user using the LDAP group configured for network login.</td>
</tr>
</tbody>
</table>

**Example**

```plaintext
ips{}debug aaa ldap lookup-user admin user1
```

Using the following configuration:

- LDAP group 'ldapgroup'
- Management port network

User LDAP group membership:
- Server 10.20.4.55

Result: Success

User DN: CN=user1,CN=Users,DC=AD01-AC,DC=local

User LDAP group membership:
- CN=Domain Admins,CN=Users,DC=AD01-AC,DC=local

User Group membership:
- administrator

Admin Role membership:
- administratorRole

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

Immediate Commit Feature. Changes take effect immediately.

```plaintext
ips{running-aaa-ldap-group-mygroup1}base-dn
```

Configure base distinguished name (DN).
Syntax
base-dn DN

Example
ips{running-aaa}ldap-group mygroup1
ips{running-aaa-ldap-group-mygroup1}base-dn DC=example,DC=com

ips{running-aaa-ldap-group-mygroup1}bind-dn
Configure bind distinguished name (DN).

Syntax
bind-dn DN

Example
ips{running-aaa-ldap-group-mygroup1}bind-dn CN=admin,
OU=People,DC=example,DC=com

ips{running-aaa-ldap-group-mygroup1}delete
Delete file or configuration item.

Syntax
delete server (ADDRESS|all)

Example
ips{running-aaa-ldap-group-mygroup1}delete server 192.168.1.1

ips{running-aaa-ldap-group-mygroup1}port
Configure LDAP port.

Syntax
port <0-65535>

Example
ips{running-aaa-ldap-group-mygroup1}port 389

ips{running-aaa-ldap-group-mygroup1}retries
Configure server(s) retries.

Syntax
retries RETRY

Example
ips{running-aaa-ldap-group-mygroup1}retries 3

ips{running-aaa-ldap-group-mygroup1}server
Configure LDAP server address.

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

Example
ips{running-aaa-ldap-group-mygroup1}server 192.168.1.1 priority 1
ips{running-aaa-ldap-group-mygroup1}server 192.168.1.2 priority 2

ips{running-aaa-ldap-group-mygroup1}timeout
Configure timeout.

Syntax
timeout SECONDS

Example
ips{running-aaa-ldap-group-mygroup1}timeout 10

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)

Example
ips{running-aaa-ldap-group-mygroup1}tls enable
ips{running-aaa-ldap-group-mygroup1}tls require-valid-server-cert enable
ips{running-aaa-ldap-group-mygroup1}tls start-tls enable

running-aaa-radius-group-X Context Commands
Immediate Commit Feature. Changes take effect immediately.
ips{running-aaa-radius-group-2}default-usergroup

Default usergroup.

Syntax

default-usergroup GROUP|none

Example

ips{running-aaa}radius-group 2
ips{running-aaa-radius-group-2}default-usergroup administrator

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

Delete file or configuration item.

Syntax

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

Example

ips{running-aaa-radius-group-2}delete server 192.168.1.1

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

Example

ips{running-aaa}radius-group 2
ips{running-aaa-radius-group-2}auth-type PEAP/EAP-MSCHAPv2

Related commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ips{running-certificates}ca-certificate on page 118</td>
<td>Import a CA certificate.</td>
</tr>
</tbody>
</table>
ips{running-aaa-radius-group-2}retries

Configure server retries.

**Syntax**

retries (0-3)

**Example**

ips{running-aaa-radius-group-2}retries 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]

**Example**

ips{running-aaa-radius-group-2}server 192.168.1.1 1812 password mysecret priority 1 timeout 10 nas-id 1
ips{running-aaa-radius-group-2}server 192.168.1.7 1812 password mysecret priority 2 timeout 10 nas-id 1

**running-actionsets Context Commands**

Immediate Commit Feature. Changes take effect immediately.

ips{running-actionsets}actionset

Enter an action set context with defined name.

**Syntax**

actionset ACTIONSETNAME

**Example**

ips{running}actionsets
ips{running-actionsets}actionset myactionset1

ips{running-actionsets}rename

Rename action set.

**Syntax**
rename actionset ACTIONSETNAME NEWACTIONSETNAME

Example
ips{running-actionsets}rename actionset myactionset1 myactionset2

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)

Example
ips{running-actionsets}actionset myactionset1
ips{running-actionsets-myactionset1}action rate-limit

ips{running-actionsets-myactionset1}allow-access
Allow quarantined host to access defined IP.
Syntax
allow-access DESTIP

Example
ips{running-actionsets-myactionset1}allow-access 192.168.1.1

ips{running-actionsets-myactionset1}bytes-to-capture
Set bytes to capture for packet trace.
Syntax
bytes-to-capture BYTES

Example
ips{running-actionsets-myactionset1}bytes-to-capture 6144
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

Example
ips{running-actionsets-myactionset1}delete allow-access 192.168.1.1
ips{running-actionsets-myactionset1}delete contact mycontact1
ips{running-actionsets-myactionset1}delete limit-quarantine 192.168.1.1
ips{running-actionsets-myactionset1}delete no-quarantine 192.168.1.1

ips{running-actionsets-myactionset1}http-block
Set quarantine option to block HTTP traffic.

Syntax
http-block

Example
ips{running-actionsets-myactionset1}http-block

ips{running-actionsets-myactionset1}http-redirect
Set redirect URL for HTTP redirect option.

Syntax
http-redirect URL

Example
ips{running-actionsets-myactionset1}http-redirect https://www.example.com

ips{running-actionsets-myactionset1}http-showdesc
Set or clear HTTP show description display option.

Syntax
http-showdesc (enable|disable)
Example

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

ips{running-actionsets-myactionset1}limit-quarantine
Add IP for limit quarantine.

Syntax
limit-quarantine SOURCEIP

Example

ips{running-actionsets-myactionset1}limit-quarantine 192.168.1.1

ips{running-actionsets-myactionset1}packet-trace
Configure packet trace option.

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

Example

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

ips{running-actionsets-myactionset1}priority
Set packet trace priority.

Syntax
priority PRIORITY

Example

ips{running-actionsets-myactionset1}priority medium

ips{running-actionsets-myactionset1}quarantine
Set quarantine option. Available options: no, immediate, threshold.

Syntax
quarantine QUARANTINETYPE

Example

ips{running-actionsets-myactionset1}quarantine immediate
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)

Example

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

ips{running-actionsets-myactionset1}threshold
Set quarantine threshold value.

Syntax

threshold (2-10000) (1-60)

Example

ips{running-actionsets-myactionset1}threshold 200 5

ips{running-actionsets-myactionset1}verbosity
Set packet trace verbosity.

Syntax

verbosity (partial|full)

Example

ips{running-actionsets-myactionset1}verbosity full

running-autodv Context Commands
Immediate Commit Feature. Changes take effect immediately.

ips{running-autodv}calendar
Enter Calender Style.

Syntax

calendar

Example
ips{running-autodv}calendar

ips{running-autodv}delete
Delete file or configuration item.

Syntax
delete proxy
delete proxy-password
delete proxy-username

Example
ips{running-autodv}delete proxy-password
ips{running-autodv}delete proxy-username
ips{running-autodv}delete proxy

ips{running-autodv}disable
Disable service.

Syntax
disable

Example
ips{running-autodv}disable

ips{running-autodv}enable
Enable service.

Syntax
enable

Example
ips{running-autodv}enable

ips{running-autodv}list
List Installed DVs.

Syntax
list

Example
ips{running-autodv}list
version 3.2.0.8458

ips{running-autodv}periodic
Enter Periodic Style.

Syntax
periodic

Example
ips{running-autodv}periodic

ips{running-autodv}proxy
Configures a proxy server.

Syntax
proxy ADDR port PORT

Example
ips{running-autodv}proxy 172.16.254.1 port enet1

ips{running-autodv}proxy-password
Sets a password for a proxy server.

Syntax
proxy-password PASSWD

Example
ips{running-autodv}proxy-password X5uth#pxy

ips{running-autodv}proxy-username
Sets a password for a proxy server.

Syntax
proxy-username USER

Example
ips{running-autodv}proxy-username user1
ips\{running-autodv\}update
Update AutoDV.

Syntax
update

Example
ips\{running-autodv\}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)

Example
ips\{running-autodv-periodic\}day Sunday

ips\{running-autodv-periodic\}period
Set number of days between update checks.

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

Example
ips\{running-autodv-periodic\}period 1

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
Example
ips{running-autodv-periodic}time 21:00

**running-blockedStreams Context Commands**

Immediate Commit Feature. Changes take effect immediately.

**ips{running-blockedStreams}flushallstreams**
Flush All Reports.

**Syntax**
flushallstreams

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

**ips{running-blockedStreams}flushstreams**
Flush reports.

**Syntax**
flushstreams

**Example**
ips{running-blockedStreams}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 2200T 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
```

**Example**

Import the certificate contents from your web server into a device certificate named `mycertname`.

```
ips{running-certificates}certificate mycertname
Please enter the PEM encoded certificate contents (including BEGIN CERTIFICATE and END CERTIFICATE lines):
-----BEGIN CERTIFICATE-----
.
.
.
-----END CERTIFICATE-----
```

**Related commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ips{running-certificates}private-key</code> on page 120</td>
<td>Import the private key from your web server into the local keystore on the 2200T device.</td>
</tr>
<tr>
<td><code>ips{running-sslinsp}server</code> on page 160</td>
<td>Add an SSL server to the 2200T device with the same security settings as your web server, and assign the corresponding certificate and private key.</td>
</tr>
</tbody>
</table>

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

Add CA certificate.

**Syntax**

```
ca-certificate CANAME
```

**Example**

```
ips{running-certificates}ca-certificate myCAname
Please enter the PEM encoded CA certificate contents
```
(including BEGIN CERTIFICATE and END CERTIFICATE lines):

```plaintext
-----BEGIN CERTIFICATE-----
SoIDQTCCAqoCCQiEcSvKsrhKTANBgkqhkiG9w0BAQQFADBQMswCQYDVQQGEwJB
VTETMBAECAUECMKU29tZToGZzEhMB8GA1UEChMYeSW50ZXJuZXQxVz02Z230
cyQdKg8TheRkMB4XDTA5MDQxNzE3MDUxNhloDTA5MDQxNzE3MDUxNlowbDEwM4A4G
A1UEBhMHV5rbsb93jEQA4GAIUECMHMHV5rbm93jEQA4GAIUEBxMHV5rbm93jEQA4GAIUEBxMHV5rbsb93jEQA4GAIUEAxMH
V5rbm93jEQA4GAIUEBwXgEsBgcqhjkjO0AQBMIIBHwKBgQD9f0BHXUSKLfsSpwu70h
9hG3UjzvRADDhj+Ap1EmaUvDQCJR+1k9j6v8x1ujDy25tVbNeBO4AdNG/y/zM3c
a5LopaSfn+gEexAiwk+7qdf+t8Yb+Dtx58aophUPBPu9t9FPHsMCNQVTWhaRMvZ1
864rYdcq7/IlAxmd0UqBwxIvAQJdqUI8VlwxMspK5qRhlAvwWbz1AoGBAPfhoIXW
mz3ey7yrXDaV7151K+7+jrgqvlXTAs9B4JnUVlXjrrRUUW/mcQcQgYCB0SRZxI+hM
KBYTt88JMozIpuE8PnqLVHyNKOCjrh4rs6Z1kW6jfwv6lTVi8fTieqEkO8y8k86o
UZCJqIPf4VrlnwaSi2ZegHtVJWQBTPTv+z0kqA4GEAAKaBdDNS53gXgLBNqXzf5AIs
npdKIHcP6LOmaueQM2X9p5IWe8n95T19pUEozSAsKbV235WFqagaIhxkXM7d
D/huz80xy3pF5EzAEGhZlanL2GF6UL79z0ZTH17E1y2y1r881/fboIP21ug
Nq9TR7Th0yOy9dfwftwoKSEXemSMA0GCSQGSIb3DQEBBAA4GBAIzQr3OK9J9zq+wh
ZFKLd0S7pNhZ8Hb07voEGtu5SfSPbzikm079FYAg+U0rvIrHq12DkSPHOxO0A9
P1SrOjQgU6A2+VTRBk2TJB32/Zng/hTDUQkyyj11skdmafaS1b99Ss07SPu6VDB
z6PBzfoWwKx3X21Ysk/gF9p07z
-----END CERTIFICATE-----
```

**ips** (`running-certificates` deleted)

Delete file or configuration item.

**Syntax**

`delete ca-certificate (all|CANAME)`

**Example**

```plaintext
ips{running-certificates}delete ca-certificate myCAname
```

**ips** (`running-certificates` displayed)

Display file or configuration item.

**Syntax**

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

**Example**

```plaintext
ips{running-certificates}display # CERTIFICATE AUTHORITIES
ca-certificate myCAname
-------BEGIN CERTIFICATE-------
SoIDQTCaQoCCQiEcSvKsrhKTBgkqhkiG9w0BAQQFADBQMswCQYDVQQGEwJB ...
```

Threat Protection System Command Line Interface Reference
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 2200T 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

Example

Import the private key from your web server into the 2200T and assign it to its corresponding mycertname device certificate. Note that if a private key is encrypted, you are automatically prompted to provide the passphrase.

ips{running-certificates}private-key mycertname
Please enter the PEM encoded private key contents (including BEGIN PRIVATE KEY and END PRIVATE KEY lines):
-----BEGIN DSA PRIVATE KEY-----
.
.
.
-----END DSA PRIVATE KEY-----

Related commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>ips{running-certificates}certificate</em> on page 117</td>
<td>Import the certificate from your web server into the local keystore on the 2200T device.</td>
</tr>
<tr>
<td><em>ips{running-sslinsp}server</em> on page 160</td>
<td>Add an SSL server to the 2200T device with the same security settings as your web server, and assign the corresponding certificate and private key.</td>
</tr>
</tbody>
</table>
running-debug Context Commands

Immediate Commit Feature. Changes take effect immediately.

ips{running}debug

Configure the sysrq state. Disabled by default.

Syntax

ips{running}debug
ips{running-debug}

Valid entries at this position are:

- display: Display file or configuration item
- help: Display help information
- sysrq: Enable or disable sysrq support

Example

ips{running-debug}sysrq enable

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)
delete proxy cache cleaning interval
delete proxy cache forwarder (all|A.B.C.D|X::X::X)
delete proxy cache maximum negative ttl
delete proxy cache maximum ttl
delete proxy cache size

Example

ips{running-dns}delete proxy cache ?

Valid entries at this position are:

- cleaning: Delete cleaning
- forwarder: Delete forwarder
maximum Delete maximum
size Delete size
ips{running-dns}delete domain-search tertiary
ips{running-dns}delete domain-search secondary
ips{running-dns}delete domain-search primary

**ips{running-dns}domain-name**
Immediate Commit Feature. Changes take effect immediately. Configure domain name.

**Syntax**
domain-name NAME

**Example**
ips{running-dns}domain-name americas

**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

**Example**
ips{running-dns}domain-search primary example.com
ips{running-dns}domain-search secondary example.org
ips{running-dns}domain-search tertiary example.edu

**ips{running-dns}name-server**
Configure DNS server.

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

**Example**
ips{running-dns}help name-server
Configure DNS server
Syntax: name-server A.B.C.D|X:X::X:X
A.B.C.D IPv4 address
X:X::X:X IPv6 address
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

Example

ips{running-dns}proxy enable

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)

Example

ips{running-gen}delete host myhost

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
HIGHRANGE Value of the last port

Example

ips{running-gen}ephemeral-port-range default
ips{running-gen}ephemeral-port-range 32768 61000
ips{running-gen}host

Configure static address to host name association.

**Syntax**

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

**Example**

ips{running-gen}host myhost 192.168.1.1
ips{running-gen}host myhost 100:0:0:0:0:0:0:1

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 on page 124 for more information.

**Syntax**

https (enable|disable)

**Example**

ips{running-gen}https enable

ips{running-gen}ssh

**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 on page 124 for more information.

**Syntax**

ssh (enable|disable)

**Example**

ips{running-gen}ssh enable

ips{running-gen}tls

**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)
```

**Example**

```
ips{running-gen}tls TLSv1.0 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)
```

**Example**

```
ips{running-gen}timezone America Chicago
ips{running-gen}timezone GMT
```

**running-high-availability Context Commands**

Create or enter a high-availability context.

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

Disables HA.

**Syntax**

```
disable
```

**Example**

The following example disables HA on the local device:

```
ips{running-high-availability}disable
```
**ips{running-high-availability}enable**
Enables high-availability on the local device.

**Syntax**
```
enable
```

**Example**
The following example enables HA on the local device.
```
ips{running-high-availability}enable
```

**ips{running-high-availability}encryption**
Applies encryption hash for a passphrase.

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

**Example**
```
ips{running-high-availability}encryption passphrase mypassphrase enable
```

**ips{running-high-availability}partner**
Specifies the serial number of the HA partner.

**Syntax**
```
partner SERIAL
```

**Example**
```
ips{running-high-availability}partner X-TPS-440T-DEV-2963
```

**running-inspection-bypass Context Commands**
Enables, disables, or removes inspection bypass rules. Inspection bypass rules direct traffic through the TippingPoint 440T and 2200T 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.

<table>
<thead>
<tr>
<th>Inspection bypass rule</th>
<th>Resulting number of port-VLAN rule combinations</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4 traffic on TCP 1556 with untagged traffic or a particular VLAN ID</td>
<td>1</td>
</tr>
<tr>
<td>IPv6 traffic on TCP 1556 with untagged traffic or a particular VLAN ID</td>
<td>2</td>
</tr>
<tr>
<td>IPv4 traffic on TCP 1556 with VLAN 10 – 100</td>
<td>90</td>
</tr>
<tr>
<td>IPv6 traffic on TCP 1556 with VLAN 10 – 100</td>
<td>180</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>For a</th>
<th>Maximum (approximate) number of port-VLAN rule combinations</th>
</tr>
</thead>
<tbody>
<tr>
<td>440T</td>
<td>1200 when bypassing IPv4 or IPv6 traffic</td>
</tr>
<tr>
<td>2200T</td>
<td>5500 when bypassing IPv4 traffic</td>
</tr>
<tr>
<td></td>
<td>3000 when bypassing IPv6 traffic</td>
</tr>
</tbody>
</table>

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`

Example
When you edit or create an inspection bypass rule, the context changes to that rule. For example, create an inspection bypass rule named myrule1 by entering the following command.

ips{running-inspection-bypass}rule myrule1

From the context of an inspection bypass rule, type help and press Enter for a list of commands.

ips{running-inspection-bypass-rule-myrule1}help

Valid commands are:
- clear-stats
- delete dst-address
- delete dst-port
- delete ip-proto
- delete ports
- delete src-address
- delete src-port
- delete vlan-id
- display [xml]
- dst-address A.B.C.D|A.B.C.D/M|X:X::X:X|X:X::X:X/M
- dst-port PORTNUM
- dst-port range MINPORTNUM MAXPORTNUM
- enable|disable
- eth ETYPE_OPTION|ETYPE_VALUE
- help [full|COMMAND]
- ip-proto PROTO_OPTION|PROTO_VALUE
- ports PORTNAME( PORTNAME){0,16}
- src-address A.B.C.D|A.B.C.D/M|X:X::X:X|X:X::X:X/M
- src-port PORTNUM
- src-port range MINPORTNUM MAXPORTNUM
- vlan-id none
- vlan-id VLANID
- vlan-id range MINVLANID MAXVLANID

Or, type help command for help on a particular command.

ips{running-inspection-bypass-rule-myrule1}help eth

Enter an ethernet type for inspection bypass rule

Syntax: eth ETYPE_OPTION|ETYPE_VALUE
eth          Enter an ethernet type
ETYPE_OPTION Enter eth type for inspection bypass rule

Possible values for ETYPE_OPTION are:
- ip          Ethernet option ip (default)
- notip       Ethernet option notip (all non-ip ethernet types)
- ipv4        Ethernet option ipv4
- ipv6        Ethernet option ipv6
ETYPE_VALUE  Ethernet hex value (e.g. 0x0806 for ARP, maximum 0xFFFF)
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.

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

**Example**

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

```plaintext
ips{running-inspection-bypass-rule-myrule1}help eth
Enter an ethernet type for inspection bypass rule
```

**Syntax:** `eth ETYPE_OPTION|ETYPE_VALUE`

- **eth** Enter an ethernet type
- **ETYPE_OPTION** Enter eth type for inspection bypass rule

Possible values for **ETYPE_OPTION** are:

- ip Ethernet option ip (default)
- notip Ethernet option notip (all non-ip ethernet types)
- ipv4 Ethernet option ipv4
- ipv6 Ethernet option ipv6
- **ETYPE_VALUE** Ethernet hex value (e.g. 0x0806 for ARP, maximum 0xFFFF)

**Example**

Edit an inspection bypass rule and enter the `eth notip` command to not inspect non-IP traffic. Then, type `display` and press Enter to view your change.

```plaintext
ips{running-inspection-bypass-rule-myrule1}eth notip
device171{running-inspection-bypass-rule-myrule1}display
rule  "myrule1"
#Rule settings#
  #id         1
  enable
  eth        notip
exit
```

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.
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)
```

Example

Edit an inspection bypass rule and enter ip-proto udp to not inspect UDP traffic.

```
ips{running-inspection-bypass-rule-myrule1}ip-proto udp
device171{running-inspection-bypass-rule-myrule1}display
rule          "myrule1"
#Rule settings#
#id         1
    enable
    eth     ip
    ip-proto udp

exit
```

```
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.

Example

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
```
Example

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.

```plaintext
ips{running-inspection-bypass-rule-myrule1}vlan-id none
device171{running-inspection-bypass-rule-myrule1}display
rule "myrule1"
#Rule settings#
    #id   1
    enable
    eth   ip
    vlan-id none
exit
```

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**

```plaintext
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

**Example**

```plaintext
ips{running}interface 1A
ips{running-1A}physical-media auto-neg
```

**ips{running}interface mgmt**

Enters context for configuring management settings.

**Syntax**

```plaintext
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

Example

ips{running-mgmt}physical-media 100half

running-ips Context Commands
Immediate Commit Feature. Changes take effect immediately.

ips{running-ips}afc-mode
Configures AFC mode.

Syntax

afc-mode AFCMODE

Example

ips{running-ips}afc-mode ?
Valid entries at this position are:
automatic   Automatic AFC mode
manual      Manual AFC mode

ips{running-ips}afc-severity
Configures AFC severity level.

Syntax

afc-severity SEVERITY

Example

ips{running-ips}afc-severity ?
Valid entries for SEVERITY:
critical    Critical severity
critical    Critical severity
error       Error severity
info        Info severity
warning     Warning severity
ips{running-ips}asymmetric-network

Configures asymmetric network mode.

Syntax

asymmetric-network enable | disable

Example

ips{running-ips}asymmetric-network enable

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

Example

ips{running-ips}connection-table trust-timeout 60

ips{running-ips}delete

Allows you to delete a profile.

Syntax

delete profile XPROFILENAME

Example

ips{running-ips}delete profile myprofile

ips{running-ips}deployment-choices

Lists deployment choices.

Syntax

deployment (Aggressive|Core|Default|Edge|Perimeter)
### Example

ips{running-ips}deployment-choices

<table>
<thead>
<tr>
<th>Name</th>
<th>Description:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>&quot;Recommended for general deployment.&quot;</td>
</tr>
<tr>
<td>Aggressive</td>
<td>&quot;Offers a more aggressive security posture that may require tuning based upon specific application protocol usage.&quot;</td>
</tr>
<tr>
<td>Core</td>
<td>&quot;Recommended for deployment in the network core.&quot;</td>
</tr>
<tr>
<td>Edge</td>
<td>&quot;Recommended for deployment in a Server Farm/DMZ.&quot;</td>
</tr>
<tr>
<td>Hyper-Aggressive</td>
<td>&quot;Offers our most aggressive security posture that will require performance and false positive tuning based on usage.&quot;</td>
</tr>
<tr>
<td>Perimeter</td>
<td>&quot;Recommended for deployment at an Internet entry point.&quot;</td>
</tr>
</tbody>
</table>

### 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

**Example**

ips{running-ips}display-categoryrules
category "Streaming Media" enabled actionset "Recommended"
category "Identity Theft" enabled actionset "Recommended"
category "Virus" enabled actionset "Recommended"
category "Spyware" enabled actionset "Recommended"
category "IM" enabled actionset "Recommended"
category "Network Equipment" enabled actionset "Recommended"
category "Traffic Normalization" enabled actionset "Recommended"
category "P2P" enabled actionset "Recommended"
category "Vulnerabilities" enabled actionset "Recommended"
category "Exploits" enabled actionset "Recommended"
category "Reconnaissance" enabled actionset "Recommended"
category "Security Policy" enabled actionset "Recommended"
ips{running-ips}gzip-decompression
Sets GZIP decompression mode.

Syntax

gzip-decompression (enable|disable)

Example

ips{running-ips}gzip-decompression enable

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

Example

ips{running-ips}http-encoded-resp accelerated

ips{running-ips}http-mode
Configures HTTP mode, which allows all TCP ports to be treated as HTTP ports for inspection purposes.

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]

Example

ips{running-ips}profile myprofile
ips{running-ips-myprofile}client-ip enable
ips{running-ips-myprofile}http-context enable
ips{running-ips}quarantine-duration

Sets quarantine duration.

Syntax

quarantine-duration DURATION
DURATION value between 1 to 1440 minutes

Example

ips{running-ips}quarantine-duration 60

ips{running-ips}rename

Renames a profile.

Syntax

rename profile PROFILENAME NEWPROFILENAME

Example

ips{running-ips}rename profile myprofile yourprofile

running-ips-X Context Commands

Immediate Commit Feature. Changes take effect immediately.

ips{running-ips-1}categoryrule

Enters categoryrule context.

Syntax

categoryrule

Example

ips{running-ips-1}categoryrule
ips{running-ips-1-categoryrule}
ips{running-ips-1-categoryrule} ?
Valid entries at this position are:
category Custom category keyword
display Display category rules for profile
help Display help information
ips{running-ips-1-categoryrule}display
categoryrule
category "Network Equipment" enabled actionset "Recommended"
category "IM" enabled actionset "Recommended"
ips{running-ips-1}delete

Delete file or configuration item.

**Syntax**

delete filter FILTERNUMBER
FILTERNUMBER Existing filter number

**Example**

ips{running-ips-1}delete filter 9

ips{running-ips-1}description

Edit description for a profile.

**Syntax**

description DESCRIPTION

**Example**

ips{running-ips-1}description "my description"

ips{running-ips-1}filter

Creates or enters a filter context.

**Syntax**

filter FILTERNUMBER

**Example**

ips{running-ips-1}filter 200
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]
```

**Example**

```
ips{running-log}delete log-option ?
Valid entry at this position is:
  xmsd   Delete xmsd log-options
ips{running-log}delete log-option xmsd all
```

**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
```

**Example**

```
ips{running-log}log audit mycontactname ALL
```
ips{running-log}log quarantine mycontactname none
ips{running-log}log system mycontactname info

**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)

Example

```
ips{running-log}logging-mode conditional threshold 5.0 period 620
```

**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

Example

```
ips{running-log}sub-system LOGIN alert
```

**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]

Example
ips{running-notifycontacts}contact mycontact1 email
ips{running-notifycontacts}contact mycontact1 snmp mysecret 192.168.1.1

ips{running-notifycontacts}delete
Delete a contact or an email setting.

Syntax
delete contact XCONTACTNAME
delete EMAILSETTING

Example
ips{running-notifycontacts}delete contact mycontact1
WARNING: Are you sure you want to delete this contact (y/n)? [n]: y

ips{running-notifycontacts}email-from-address
From email address.

Syntax
eemail-from-address EMAIL

Example
ips{running-notifycontacts}email-from-address someone@example.com

ips{running-notifycontacts}email-from-domain
From domain name.

Syntax
eemail-from-domain DOMAIN

Example
ips{running-notifycontacts}email-from-domain example.com

ips{running-notifycontacts}email-server
Set mail server IP.
email-server IP

Example
ips{running-notifycontacts}email-server 123.45.67.890

ips{running-notifycontacts}email-threshold
Set email threshold per minute

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

Example
ips{running-notifycontacts}email-threshold 1

ips{running-notifycontacts}email-to-default-address
Default to email address.

Syntax
email-to-default-address EMAIL

Example
ips{running-notifycontacts}email-to-default-address mycontact@example.com

ips{running-notifycontacts}rename
Rename contact with new name.

Syntax
rename contact XCONTACTNAME NEWNAME

Example
ips{running-notifycontacts}rename contact mycontact1 mycontact2

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

**Example**

ips{running-ntp}delete key 1
ips{running-ntp}delete key all
ips{running-ntp}delete server all
ips{running-ntp}delete server 192.168.1.1

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)

**Example**

ips{running-ntp}key 1 myauthkey

ips{running-ntp}ntp

Enable or disable NTP service.

**Syntax**

ntp (enable|disable)

**Example**

ips{running-ntp}ntp enable
**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
```

**Example**

```
ips{running-ntp}polling-interval 16
```

**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
```

**Example**

```
ips{running-ntp}server 192.168.1.1 key 1 prefer
```

**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:
```

---

144

Threat Protection System Command Line Interface Reference
Threat Protection System Command Line Interface Reference

```
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>group</td>
<td>Reputation group</td>
</tr>
<tr>
<td>profile</td>
<td>Delete reputation profile</td>
</tr>
</tbody>
</table>

**Example**

```
ips{running-rep}delete group myrepgroup
WARNING: Are you sure you want to delete reputation group (y/n)? [n]: y
ips{running-rep}delete profile myrepprofile
WARNING: Are you sure you want to delete profile (y/n)? [n]: y

**ips{running-rep}group**

Create or enter reputation group context.

**Syntax**

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

**Example**

```
ips{running-rep}group myrepgroup
ips{running-rep-myrepgroup}
ips{running-rep-myrepgroup}help
Valid commands are:
delete domain DOMAINNAME
delete ip SOURCEIP
description DESCRIPTION
display
domain NEWDOMAINNAME
help [full|COMMAND]
ip SOURCEIP
```

**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)
```

**Example**

```
ips{running-rep}nxdomain-response enable
ips{running-rep}display
reputation
nxdomain-response enable
####################################
```
# REPUTATION GROUPS  #
#*******************************************************************************
#*******************************************************************************
# REPUTATION PROFILES  #
#*******************************************************************************
profile "Default Reputation Profile"
  # PROTECTION SETTINGS
  check-source-address enable
  check-destination-address enable
  action-when-pending permit
  # IP REPUTATION EXCEPTIONS
  # DNS REPUTATION EXCEPTIONS
  # REPUTATION FILTERS

exit
exit

ips{running-rep}profile

Create or enter reputation profile context.

Syntax

profile PROFILENAME

Example

ips{running-rep}profile myprofile
ips{running-rep-myprofile}help
Valid commands are:
CHECK-ADDRESS ACTION
action-when-pending ACTION
delete dns-except DOMAINNAME
delete filter ALLGROUPNAME
delete ip-except SOURCEIP DESTINATIONIP
display
dns-except NEWDOMAINNAME
filter ALLGROUPNAME( enable [threshold [XACTIONSETNAME]]){( disable)
help [full|COMMAND]
ip-except SOURCEIP DESTINATIONIP

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

Example

ips{running-rep}rename profile oldname newname

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

Example

ips{running-rep-1}delete domain example.com
ips{running-rep-1}delete ip 192.168.1.1
ips{running-rep-1}delete ip 100:0:0:0:0:0:0:0/64

ips{running-rep-1}description

Add a description to the reputation group.

Syntax

description DESCRIPTION

Example

ips{running-rep-1}description "Rep Group 1"

ips{running-rep-1}domain

New domain name.

Syntax

domain NEWDOMAIN

Example

ips{running-rep-1}domain example.com
ips{running-rep-1}ip

Syntax
ip IPADDRESS

Example
ips{running-rep-1}ip 123.45.67.890

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)

Example
ips{running-rep-abc}check-destination-address enable

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

Example
ips{running-rep-abc}check-source-address enable
**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)
```

**Example**

```
ips{running-rep-abc}delete dns-except example.com
ips{running-rep-abc}delete filter "myrepgroup"
ips{running-rep-abc}delete ip-except 192.168.1.1 192.168.2.2
ips{running-rep-abc}delete ip-except 2001:2:0:0:0:0:0:0/48 2001:db8:0:0:0:0:0:0/32
```

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

DNS domain exception.

**Syntax**

```
dns-except DOMAINNAME
```

**Example**

```
ips{running-rep-abc}dns-except example.com
```

**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

**Example**

```
ips{running-rep-abc}filter "myrepgroup" enable
ips{running-rep-abc}filter "myrepgroup" enable 0 "Block + Notify"
```
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`

Example

`ips{running-rep-abc}ip-except 192.168.1.1 192.168.2.2`

`ips{running-rep-abc}ip-except 2001:2:0:0:0:0:0:0/48 2001:db8:0:0:0:0:0:0/32`

security-policy-reset

Resets the IPS security policy to the default values.

Syntax

`security-policy-reset`

running-segmentX Context Commands

Immediate Commit Feature. Changes take effect immediately.

ips{running-segment0}description

Apply segment description.

Syntax

`description TEXT`

Example

`ips{running-segment0}description "my ethernet segment"`

ips{running-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
Example

ips{running-segment0}high-availability permit

ips{running-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

Example

ips{running-segment0}link-down wire wait-time 30

ips{running-segment0}restart

Restart both ethernet ports of segment.

Syntax

restart

Example

ips{running-segment0}restart

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)

**Example**

```
ips{running-services}display service myservice2
ips{running-services}display service all
```

**ips**(running-services)**service**

Edit a service.

**Syntax**

service SERVICENAME

**Example**

```
ips{running-services}service myservice1
```

**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

Example

ips{running-services-myservice1}delete icmp any
ips{running-services-myservice1}delete icmpv6 any
ips{running-services-myservice1}delete port udp 53
ips{running-services-myservice1}delete port tcp all
ips{running-services-myservice1}delete protocol 6
ips{running-services-myservice1}delete service http
ips{running-services-myservice1}delete service dns

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

Example

ips{running-services-myservice1}port tcp 80 to 88

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)

Example

ips{running-snmp}authtrap enable
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

Example

ips{running-snmp}community mycommunity default

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

Example

ips{running-snmp}delete community mycommunity
ips{running-snmp}delete community all
ips{running-snmp}delete trapsession 192.168.1.1 ver 3
ips{running-snmp}delete trapsession all

ips{running-snmp}engineID

Configure SNMPv3 engine ID.

Syntax

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

Example

ips{running-snmp}engineID 0x800012ef0302a11aab33f4
**ips{running-snmp}snmp**

Enable or disable SNMP.

**Syntax**

snmp (enable|disable)

**Example**

ips{running-snmp}snmp enable

**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
Example

```sh
trapdest snmpserver.example.com ver 2c mycommunity inform
trapdest 192.168.1.1 port 162 ver 2c mycommunity
trapdest 192.168.1.1 port 162 ver 3 mysnmpusername level
authNoPriv authtype SHA mysnmpassword inform
trapdest 100:0:0:0:0:0:0:1 ver 3 mysnmpusername level
authNoPriv authtype SHA mysnmpassword inform
```

**ips{running-snmp}username**

Configure SNMPv3 USM read-only user.

**Syntax**

```sh
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

**Example**

```sh
username mysnmpusername level noAuthNoPriv
username mysnmpusername level authNoPriv authtype SHA mysnmpassword
username mysnmpusername level authPriv authtype SHA mysnmpassword privproto AES mysnmpprivpassword
```
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. However, the IPS will not inspect secure sessions.

**Example**

Use the `help` command to display information about the `ssl-insp` context.

```plaintext
ips{running-sslinsp}help
Valid commands are:
delete log sslInspection CONTACT-NAME
delete profile (all|PROFILE_NAME)
delete server (all|SERVER_NAME)
disable
enable
help [full|COMMAND]
log sslInspection CONTACT-NAME [ALL|none]
profile PROFILE_NAME
rename profile PROFILE_NAME NEW_PROFILE_NAME
rename server SERVER_NAME NEW_SERVER_NAME
server SERVER_NAME
```

**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 2200T must be licensed for SSL inspection. Use the LSM to verify the SSL inspection license.

**Syntax**

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

**Example**

Enable SSL inspection to begin inspecting SSL sessions.

```plaintext
ips{running-sslinsp}enable
```

**ips{running-sslinsp}log sslInspection**

Use the `log sslInspection` command to save SSL inspection logging information to a particular notification contact. By default, the 2200T saves SSL inspection log information to the "Management
The "Console" notification contact which is available for display from the LSM and is found in the `sslInspection.log` on the 2200T.

**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` on page 160 for more information.

### Syntax

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

### Example

Save SSL inspection logging information to the remote system log servers that are configured in the Remote System Log notification contact.

```
isps{running-sslinsp}log sslInspection "Remote System Log"  ALL
```

**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.

### Syntax

```
[delete] profile PROFILENAME
```

### Example

Create a profile named myprofile.

```
isps{running-sslinsp}profile myprofile
```

The context changes to the myprofile subcontext.

For information about the available commands in the subcontext, type the help command and press Enter.

```
isps{running-sslinsp-myprofile}help
```

Valid commands are:

- delete description
- delete policy all|POLICYNAME
- description TEXT
- display [xml]
- help [full|COMMAND]
- policy NEWPOLICYNAME
policy POLICYNAME
rename policy POLICYNAME NEWPOLICYNAME

(Required) Add a policy named mypolicy to the profile.

ips{running-sslinsp-myprofile}policy mypolicy

The context changes to the mypolicy policy.

(Required) Assign an SSL inspection server named mysslserver to the policy. Note that the SSL server specifies the range of server IP addresses you want to protect along with your SSL server configuration details.

ips{running-sslinsp-myprofile-mypolicy}server mysslserver

(Optional) 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. In the following example, the server policy does not inspect inbound encrypted traffic between mysslserver and client IP addresses within the range of 10.7.0.1/24.

ips{running-sslinsp-myprofile-mypolicy}ip-exception
  src-address 10.7.0.1/24

Related commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ips{running-certificates}certificate</td>
<td>on page 117 Import the certificate from your web server into the local keystore on the device.</td>
</tr>
<tr>
<td>ips{running-certificates}private-key</td>
<td>on page 120 Import the private key from your web server into the local keystore on the device.</td>
</tr>
<tr>
<td>ips{running-vsegs-VSEG_NAME}ssl-profile</td>
<td>on page 170 Update the virtual segment to assign the SSL inspection profile.</td>
</tr>
<tr>
<td>ips{running-sslinsp}server</td>
<td>on page 160 Add an SSL server with its assigned security certificate and private key.</td>
</tr>
</tbody>
</table>

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.

**Syntax**

```
[delete] server SERVERNAME
```

**Example**

Add an SSL server named *myserver* with TLS protocols and cipher suites automatically configured.

```
ips{running-sslinsp}server myserver
```

The context changes to the `running-sslinsp-server-myserver` subcontext.

**Tip:** 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. For more information about the available commands in the subcontext, type `help` and press Enter.

```
ips{running-sslinsp-server-myserver}help
```

Valid commands are:

- `certificate SERVERCERT`
- `cipher-suite all|(protocol SSL-PROTOCOL)|CIPHER-SUITE`
- `compression enable|disable`
- `decrypted-service SERVICENAME`
- `delete cipher-suite all|(protocol SSL-PROTOCOL)|CIPHER-SUITE`
- `delete description`
- `delete detection-port (all|PORT [to LAST-PORT])`
- `delete ip address( all|A.B.C.D/M)`
- `delete protocol all|SSL-PROTOCOL [auto-delete-ciphers]`
- `delete rekey-interval`
- `description TEXT`
- `detection-port PORT [to PORT]ex`
- `display [xml]`
- `help [full|COMMAND]`
- `ip address( A.B.C.D|A.B.C.D/M)`
- `logging enable|disable`
- `protocol all|SSL-PROTOCOL [auto-add-ciphers]`
- `rekey-interval INTERVAL`
- `tcp-reset enable|disable`

Type `display` and press Enter to view the settings for the SSL server.

```
ips{running-sslinsp-server-myserver}display
```

```
server "myserver"
  detection-port 443
  decrypted-service http
```
protocol TLSv1.0
protocol TLSv1.1
protocol TLSv1.2
cipher-suite TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
cipher-suite TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
cipher-suite TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
cipher-suite TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
cipher-suite TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
cipher-suite TLS_RSA_WITH_3DES_EDE_CBC_SHA
cipher-suite TLS_RSA_WITH_AES_128_CBC_SHA
cipher-suite TLS_RSA_WITH_AES_128_CBC_SHA256
cipher-suite TLS_RSA_WITH_AES_256_CBC_SHA
cipher-suite TLS_RSA_WITH_AES_256_CBC_SHA256
logging disable
compression disable
tcp-reset enable
exit

Note that by default, the IP address and device certificate for the server are not defined, and must be specified separately. For information about changing a particular setting, enter `help` and press Enter.

(Required) 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.

```plaintext
ips{running-sslinsp-server-myserver}ip address 192.168.1.0/24
```

(Required) Specify the **device certificate** that the 2200T uses to decrypt and encrypt HTTP traffic across the specified range of server IP addresses. This setting is required. Make sure that the corresponding private key is assigned to the device certificate.

```plaintext
ips{running-sslinsp-server-myserver}certificate mycertificate
display
```

Type `display` and press Enter to view the updated IP address and certificate for the SSL server.

```plaintext
ips{running-sslinsp-server-myserver}display
```

```
service "myserver"
ip address 192.168.0.1/24
detection-port 443
decrypted-service http
protocol TLSv1.0
protocol TLSv1.1
protocol TLSv1.2
cipher-suite TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
cipher-suite TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
cipher-suite TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
cipher-suite TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
cipher-suite TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
cipher-suite TLS_RSA_WITH_3DES_EDE_CBC_SHA
cipher-suite TLS_RSA_WITH_AES_128_CBC_SHA
cipher-suite TLS_RSA_WITH_AES_128_CBC_SHA256
cipher-suite TLS_RSA_WITH_AES_256_CBC_SHA
```
cipher-suite TLS_RSA_WITH_AES_256_CBC_SHA256
logging disable
compression disable
tcp-reset enable
exit

Related commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ips{running-certificates}certificate on page 117</td>
<td>Import the certificate from your web server into the local keystore on the device.</td>
</tr>
<tr>
<td>ips{running-certificates}private-key on page 120</td>
<td>Import the private key from your web server into the local keystore on the device.</td>
</tr>
<tr>
<td>ips{running-vseg-VSEG_NAME}ssl-profile on page 170</td>
<td>Update the virtual segment to assign the SSL inspection profile.</td>
</tr>
<tr>
<td>ips{running-sslinsp}profile on page 159</td>
<td>Assign the SSL server to an SSL inspection profile.</td>
</tr>
</tbody>
</table>

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

Example

ips{running-trafmgmt}delete mytrafmgmt-profile
ips{running-trafficmgmt}profile

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

Syntax

```
profile NEWTRAFFPROFNAME
profile TRAFPROFNAME
```

Examples

```
ips{running-trafficmgmt}profile MyTrafficProfile
ips{running-trafficmgmt-MyTrafficProfile}
```

Valid entries at this position are:

```
delete               Delete a traffic-management filter
description          Update traffic-management profile description
display              Display file or configuration item
help                 Display help information
rename               Rename traffic-management filter
traffic-filter       Traffic-management filter
```

```
ips{running-trafficmgmt-MyTrafficProfile}help
```

Valid commands are:

```
delete traffic-filter all|TRAFFILTERNAME
description DESCRIPTION
display
help [full|COMMAND]
rename traffic-filter TRAFFILTERNAME NEWTRAFFILTERNAME
traffic-filter NEWTRAFFILTERNAME
traffic-filter TRAFFILTERNAME
```

```
ips{running-trafficmgmt-MyTrafficProfile}traffic-filter MyTrafficFilter
ips{running-trafficmgmt-MyTrafficProfile-MyTrafficFilter}
```

Valid entries at this position are:

```
action     Set traffic-management filter action to block
disable    Disable a traffic-management filter
display    Display file or configuration item
enable     Enable a traffic-management filter
help       Display help information
ip         Set source and destination addresses for a traffic-management filter
move       Move traffic-management filter priority position
protocol   Set traffic-management filter protocol
```

```
ips{running-trafficmgmt-MyTrafficProfile-MyTrafficFilter}help
```

Valid commands are:

```
action block|allow|trust|(rate-limit RATELIMITACTION)
display
enable|disable
help [full|COMMAND]
ip ipv4 [src-address IPV4-SRC-CIDR] [dst-address IPV4-DST-CIDR]
```
ip ipv6 [src-address IPV6-SRC-CIDR] [dst-address IPV6-DST-CIDR]
moves after TRAFFILTERNAME
move before TRAFFILTERNAME
move to position VALUE
protocol any [ip-fragments-only]
protocol tcp|udp [src-port SRCPORT] [dst-port DSTPORT]
protocol icmp [type ICMPTYPE] [code ICMP_CODE]

**ips{running-trafmgmt}rename**

Rename traffic-management profile.

**Syntax**

```
rename profile TRAFPROFNAME NEWTRAFPROFNAME
```

**Example**

```
ips{running-trafmgmt}rename profile http-traffic-profile web-traffic-profile
```

**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.

**Syntax**

```
ips{running}virtual-segments
```

Valid entries at this position are:

- `delete virtual-segment` Delete file or configuration item
- `rename virtual-segment` Rename virtual-segment
- `virtual-segment` Create or enter virtual-segment context
- `display` Display file or configuration item

**Notes**

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

```plaintext
delete virtual-segment VSEGNAME
```

**Example**

```plaintext
ips{running-vsegs}delete virtual-segment "segment1 (A > B)"
```

**ips{running-vsegs}display**
Display file or configuration item.

**Syntax**

```plaintext
display {xml}
```

**ips{running-vsegs}rename virtual-segment**
Rename the virtual segment. Each virtual segment name must be unique.

**Syntax**

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

**Example**

```plaintext
ips{running-vsegs}rename virtual-segment "segment1 (A > B)" "seg 1"
```

**ips{running-vsegs}virtual-segment**
Create or enter virtual-segment context.

**Syntax**

```plaintext
virtual-segment VSEGNAME
virtual-segment NEWVSEGNAME
```
Example

ips{running-vsegs}virtual-segment "segment1 (A > B)"

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}virtual-segment
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
- ips-profile: Virtual segment ips profile
- move: Move virtual segment priority position
- reputation-profile: Virtual segment reputation profile
- src-address: Add source address to a virtual segment
- ssl-profile: Virtual segment SSL profile
- traffic-profile: Virtual segment traffic-management profile
- vlan-id: 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.
- 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**

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

**Example**

```plaintext
ips{running-vsegs}bind in-port 1A out-port 1B
```

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

Delete a port-pair association from this virtual segment.

**Syntax**

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

**Example**

```plaintext
ips{running-vsegs}delete bind in-port 1A out-port 1B
```

**ips{running-vsegs}description**

Add or edit the description of a virtual segment.

**Syntax**

```plaintext
description TEXT
```

**Example**

```plaintext
ips{running-vsegs}description "virtual segment for ips profile"
```

**ips{running-vsegs}display**

Display file or configuration item.

**Syntax**

```plaintext
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.

Example

ips{running-vsegs}dst-address 192.168.1.0/24

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`.

Example

ips{running-vsegs}dest-address fe80:5555::73

ips{running-vsegs-VSEG_NAME}ips-profile

Associate an existing IPS security profile with this virtual segment.

Syntax

ips-profile PROFILENAME

Example

ips{running-vsegs}virtual-segment v1
ips{running-vsegs-v1}ips-profile "Default, 44.0"

ips{running-vsegs-VSEG_NAME}delete ips-profile

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

delete ips-profile PROFILENAME

Example

ips{running-vsegs}virtual-segment v1
ips{running-vsegs-v1}delete ips-profile "Default, 44.0"

ips{running-vsegs-VSEG_NAME}reputation-profile

Associate an existing reputation profile with this virtual segment.

Syntax

reputation-profile PROFILENAME

Example

ips{running-vsegs}virtual-segment v1
ips{running-vsegs-v1}reputation-profile Default__REP,4

ips{running-vsegs-VSEG_NAME}delete reputation-profile

Delete an existing reputation profile associated with this virtual segment.

Syntax

delete reputation-profile PROFILENAME

Example

ips{running-vsegs}virtual-segment v1
ips{running-vsegs-v1}delete reputation-profile Default__REP,4

ips{running-vsegs-VSEG_NAME}ssl-profile

Edit the virtual segment to assign an SSL inspection profile.

Syntax

ssl-profile PROFILENAME

Example

ips{running-vsegs}virtual-segment v1
ips{running-vsegs-v1}ssl-profile webprofile

Related commands
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ips{running-ssлинsp}profile</code> on page 159</td>
<td>Create an SSL-inspection profile.</td>
</tr>
</tbody>
</table>

**ips{running-vsegs-VSEG_NAME}delete ssl-profile**

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

**Syntax**

delete ssl-profile PROFILENAME

**Example**

ips{running-vsegs}virtual-segment vl
ips{running-vsegs-v1}delete ssl-profile webprofile

**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.

**Example**

ips{running-vsegs}description "virtual segment for ips profile"

**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.

**Example**

```bash
ips{running-vsegs}src-address 2001:eeb8::/64
```

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

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

**Syntax**

```bash
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`.

**Example**

```bash
ips{running-vsegs}src-address 2001:eeb8::/64
```

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

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

**Syntax**

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

Valid IDs can range from 1–4094. You can configure a maximum of 512 VLAN IDs.

**Example**

```bash
ips{running-vsegs}vlan-id range 301 304
```

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

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

**Syntax**

```bash
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.

Example

```bash
ips{running-vsegs}delete vlan-id range 301 304
```

**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**

```bash
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.

**Usage**

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

**Examples**

Add a VLAN translation for inbound TCP traffic on port 120 to port 1A of the device where the tagged traffic is updated to have a VLAN tag of 240:

```bash
ips{running-vlan-translations}add-translation 1A 120 240
```

Display the currently defined VLAN translations:

```bash
ips{running-vlan-translations}display
#  VLAN TRANSLATION  #
add-translation 1A 120 240
```

Remove a VLAN translation for inbound TCP traffic on port 120 from port 1A of the device:

```bash
ips{running-vlan-translations}delete-translation 1A 120
```