<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>boot</td>
<td>18</td>
</tr>
<tr>
<td>chpasswd</td>
<td>19</td>
</tr>
<tr>
<td>clear</td>
<td>19</td>
</tr>
<tr>
<td>date</td>
<td>20</td>
</tr>
<tr>
<td>debug</td>
<td>20</td>
</tr>
<tr>
<td>delete</td>
<td>29</td>
</tr>
<tr>
<td>delete auxdv</td>
<td>29</td>
</tr>
<tr>
<td>display</td>
<td>30</td>
</tr>
<tr>
<td>display conf</td>
<td>30</td>
</tr>
<tr>
<td>display-config</td>
<td>31</td>
</tr>
<tr>
<td>edit</td>
<td>32</td>
</tr>
<tr>
<td>fips-mode-enable</td>
<td>33</td>
</tr>
<tr>
<td>halt</td>
<td>33</td>
</tr>
<tr>
<td>help</td>
<td>34</td>
</tr>
<tr>
<td>high-availability</td>
<td>34</td>
</tr>
<tr>
<td>keystore</td>
<td>36</td>
</tr>
<tr>
<td>list</td>
<td>37</td>
</tr>
<tr>
<td>log-configure</td>
<td>37</td>
</tr>
<tr>
<td>logout</td>
<td>37</td>
</tr>
<tr>
<td>master-key</td>
<td>38</td>
</tr>
<tr>
<td>ping</td>
<td>40</td>
</tr>
<tr>
<td>ping6</td>
<td>40</td>
</tr>
<tr>
<td>quarantine</td>
<td>41</td>
</tr>
<tr>
<td>reboot</td>
<td>41</td>
</tr>
<tr>
<td>reports</td>
<td>42</td>
</tr>
<tr>
<td>resize</td>
<td>42</td>
</tr>
<tr>
<td>save-config</td>
<td>42</td>
</tr>
<tr>
<td>service-access</td>
<td>43</td>
</tr>
<tr>
<td>set</td>
<td>43</td>
</tr>
<tr>
<td>setup</td>
<td>44</td>
</tr>
</tbody>
</table>
show ................................................................................................................................................... 44
show aaa ............................................................................................................................................ 47
show auxdv ...................................................................................................................................... 49
show date ........................................................................................................................................ 49
show dns ......................................................................................................................................... 49
show filter ........................................................................................................................................ 50
show health ..................................................................................................................................... 51
show high-availability ....................................................................................................................... 52
show inspection-bypass ..................................................................................................................... 53
show interface ................................................................................................................................. 54
show key .......................................................................................................................................... 54
show license .................................................................................................................................... 54
show log-file ..................................................................................................................................... 55
show log-file boot ............................................................................................................................ 55
show log-file FILE_NAME ............................................................................................................... 56
show log-file FILE_NAME stat ......................................................................................................... 59
show log-file summary ..................................................................................................................... 59
show mfg-info .................................................................................................................................. 59
show np engine ................................................................................................................................ 60
show np general statistics ............................................................................................................... 61
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 ......................................................................................................................... 65
show reports .................................................................................................................................... 65
show service ..................................................................................................................................... 65
show sflow ....................................................................................................................................... 66
show slot .......................................................................................................................................... 66
display................................................................................................................................................ 82
email................................................................................................................................................... 83
log-file-size......................................................................................................................................... 83
log-storage..........................................................................................................................................84
log-test................................................................................................................................................84
rotate.................................................................................................................................................. 85

Edit running configuration commands .............................................................................................86

Edit context commands .....................................................................................................................86

aaa...................................................................................................................................................86
actionsets.........................................................................................................................................86
autodv.............................................................................................................................................. 87
blockedStreams............................................................................................................................... 88
certificates........................................................................................................................................88
debug...............................................................................................................................................89
delete...............................................................................................................................................89
display..............................................................................................................................................89
dns................................................................................................................................................... 90
gen...................................................................................................................................................91
high-availability.................................................................................................................................92
interface............................................................................................................................................92
ips.................................................................................................................................................... 93
log.................................................................................................................................................... 94
notifycontacts...................................................................................................................................95
ntp.................................................................................................................................................... 96
reputation.........................................................................................................................................96
security-policy-reset.........................................................................................................................97
segmentX.........................................................................................................................................97
services............................................................................................................................................98
sflow.................................................................................................................................................98
snmp................................................................................................................................................ 99
Threat Protection System Command Line Interface Reference

contexts and related commands .................................................. 101

running-aaa Context Commands.............................................. 101
ips{running-aaa}delete............................................................ 101
ips{running-aaa}display.......................................................... 102
ips{running-aaa}disable-inactive-users .................................. 102
ips{running-aaa}ldap-group..................................................... 102
ips{running-aaa}ldap-schema.................................................. 103
ips{running-aaa}login............................................................. 103
ips{running-aaa}login-banner.................................................. 104
ips{running-aaa}password...................................................... 104
ips{running-aaa}radius-group................................................ 104
ips{running-aaa}re-auth......................................................... 105
ips{running-aaa}remote-login-group...................................... 105
ips{running-aaa}role............................................................. 105
ips{running-aaa}tacacs-group............................................... 106
ips{running-aaa}user............................................................. 106
ips{running-aaa}user-group................................................... 106

aaa debug ldap test-bind....................................................... 106

aaa debug ldap authenticate-user......................................... 107

aaa debug ldap lookup-user.................................................. 108

running-aaa-ldap-group-X Context Commands...................... 109
ips{running-aaa-ldap-group-mygroup1}base-dn....................... 109
ips{running-aaa-ldap-group-mygroup1}bind-dn......................... 109
ips{running-aaa-ldap-group-mygroup1}delete.......................... 109
ips{running-aaa-ldap-group-mygroup1}port............................. 110
ips{running-aaa-ldap-group-mygroup1}retries........................ 110
ips{running-aaa-ldap-group-mygroup1}server........................ 110
ips{running-aaa-ldap-group-mygroup1}timeout....................... 110
ips{running-aaa-ldap-group-mygroup1}tls............................. 111

running-aaa-radius-group-X Context Commands..................... 111
ips{running-aaa-radius-group-2}default-usergroup................ 111
ips{running-aaa-radius-group-2}delete.................................. 111
ips{running-aaa-radius-group-2}auth-type............................. 112
ips{running-aaa-radius-group-2}retries............................... 112
ips{running-aaa-radius-group-2}server................................. 112
ips{running-blockedStreams}flushallstreams.............................................................................. 122
ips{running-blockedStreams}flushstreams..................................................................................122
ips{running-blockedStreams}list..................................................................................................122

running-certificates Context Commands....................................................................................... 122
  ips{running-certificates}certificate............................................................................................... 122
  ips{running-certificates}ca-certificate.......................................................................................... 123
  ips{running-certificates}delete..................................................................................................... 124
  ips{running-certificates}display....................................................................................................124
  ips{running-certificates}private-key............................................................................................. 124

running-debug Context Commands..................................................................................................125
  ips{running}debug....................................................................................................................... 125

running-dns Context Commands.................................................................................................. 126
  ips{running-dns}delete................................................................................................................ 126
  ips{running-dns}domain-name.................................................................................................... 126
  ips{running-dns}domain-search.................................................................................................. 127
  ips{running-dns}name-server...................................................................................................... 127
  ips{running-dns}proxy................................................................................................................. 127

running-gen Context Commands.................................................................................................. 128
  ips{running-gen}delete................................................................................................................ 128
  ips{running-gen}ephemeral-port-range....................................................................................... 128
  ips{running-gen}host................................................................................................................... 128
  ips{running-gen}https.................................................................................................................. 128
  ips{running-gen}lsm.................................................................................................................... 129
  ips{running-gen}sms-allowed-ip.................................................................................................. 129
  ips{running-gen}ssh.................................................................................................................... 129
  ips{running-gen}timezone........................................................................................................... 130
  ips{running-gen}tls...................................................................................................................... 130

running-high-availability Context Commands................................................................................130
  ips{running-high-availability}disable............................................................................................ 130
  ips{running-high-availability}enable.............................................................................................131
  ips{running-high-availability}encryption.......................................................................................131
  ips{running-high-availability}partner............................................................................................ 131

running-inspection-bypass Context Commands............................................................................131
  ips{running-inspection-bypass-rule-myrule1}action.................................................................... 134
  ips{running-inspection-bypass-rule-myrule1}eth.........................................................................134
  ips{running-inspection-bypass-rule-myrule1}ip-proto.................................................................. 135
  ips{running-inspection-bypass-rule-myrule1}vlan-id................................................................... 136

running-interface Context Commands.......................................................................................... 137
  ips{running}interface nM............................................................................................................. 137
ips{running}interface mgmt......................................................................................................... 137

running-ips Context Commands................................................................................................ 137
  ips{running-ips}afc-mode............................................................................................................ 138
  ips{running-ips}afc-severity......................................................................................................... 138
  ips{running-ips}asymmetric-network........................................................................................... 138
  ips{running-ips}connection-table................................................................................................. 138
  ips{running-ips}delete..................................................................................................................139
  ips{running-ips}deployment-choices........................................................................................... 139
  ips{running-ips}display................................................................................................................ 139
  ips{running-ips}display-categoryrules......................................................................................... 140
  ips{running-ips}gzip-decompression........................................................................................... 140
  ips{running-ips}http-encoded-resp.............................................................................................. 140
  ips{running-ips}http-mode........................................................................................................... 141
  ips{running-ips}profile..................................................................................................................141
  ips{running-ips}quarantine-duration............................................................................................ 141
  ips{running-ips}rename............................................................................................................... 141

running-ips-X Context Commands.............................................................................................. 142
  ips{running-ips-1}categoryrule.................................................................................................... 142
  ips{running-ips-1}delete.............................................................................................................. 142
  ips{running-ips-1}description.......................................................................................................143
  ips{running-ips-1}filter................................................................................................................. 143

running-log Context Commands................................................................................................... 143
  ips{running-log}delete................................................................................................................. 143
  ips{running-log}log...................................................................................................................... 144
  ips{running-log}log-option........................................................................................................... 144
  ips{running-log}logging-mode..................................................................................................... 145
  ips{running-log}sub-system.........................................................................................................145

running-notifycontacts (email) Context Commands...................................................................... 146
  ips{running-notifycontacts}contact.............................................................................................. 146
  ips{running-notifycontacts}delete................................................................................................. 146
  ips{running-notifycontacts}email-from-address........................................................................... 146
  ips{running-notifycontacts}email-from-domain.......................................................................... 147
  ips{running-notifycontacts}email-server..................................................................................... 147
  ips{running-notifycontacts}email-threshold............................................................................... 147
  ips{running-notifycontacts}email-to-default-address.................................................................... 147
  ips{running-notifycontacts}rename..............................................................................................148

running-ntp Context Commands................................................................................................... 148
  ips{running-ntp}delete................................................................................................................. 148
  ips{running-ntp}key..................................................................................................................... 148
  ips{running-ntp}ntp...................................................................................................................... 149
ips{running-ntp}polling-interval....................................................................................................149
ips{running-ntp}server............................................................................................................. 149

running-rep Context Commands..............................................................................................150
ips{running-rep}delete............................................................................................................. 150
ips{running-rep}group..............................................................................................................150
ips{running-rep}nxdomain-response......................................................................................... 150
ips{running-rep}profile.............................................................................................................151
ips{running-rep}rename...........................................................................................................152

running-rep-X (group X) Context Commands...........................................................................152
ips{running-rep-1}delete...........................................................................................................152
ips{running-rep-1}description..................................................................................................152
ips{running-rep-1}domain.........................................................................................................153
ips{running-rep-1}ip..................................................................................................................153

running-rep-X (profile X) Context Commands..........................................................................153
ips{running-rep-abc}action-when-pending................................................................................153
ips{running-rep-abc}check-destination-address.......................................................................153
ips{running-rep-abc}check-source-address..............................................................................153
ips{running-rep-abc}delete.......................................................................................................154
ips{running-rep-abc}dns-except...............................................................................................154
ips{running-rep-abc}filter.........................................................................................................154
ips{running-rep-abc}ip-except..................................................................................................155

security-policy-reset..................................................................................................................155

running-segmentX Context Commands...................................................................................155
ips{running-segment0}description............................................................................................155
ips{running-segment0}high-availability....................................................................................155
ips{running-segment0}link-down...............................................................................................156
ips{running-segment0}restart...................................................................................................156

running-services Context Commands.....................................................................................156
ips{running-services}display....................................................................................................158
ips{running-services}service..................................................................................................158

running-services-X Context Commands..................................................................................158
ips{running-services-myservice1}delete..................................................................................158
ips{running-services-myservice1}port.....................................................................................159

running-snmp Context Commands..........................................................................................159
ips{running-snmp}authtrap.......................................................................................................159
ips{running-snmp}community..................................................................................................159
ips{running-snmp}delete...........................................................................................................160
ips{running-snmp}engineID......................................................................................................160
ips{running-snmp}snmp............................................................................................................160
ips{running-snmp}trapdest................................................................. 161
ips{running-snmp}username......................................................... 161

running-sslinsp Context Commands........................................ 162
  ips{running-sslinsp}enable....................................................... 163
  ips{running-sslinsp}log sslInspection...................................... 163
  ips{running-sslinsp}profile.................................................... 163
  ips{running-sslinsp}server..................................................... 165

running-traffic-management Context Commands.................. 168
  ips{running-trafmgmt}delete.................................................. 168
  ips{running-trafmgmt}profile................................................ 168
  ips{running-trafmgmt}rename................................................ 169

running-virtual-segments Context Commands.......................... 169
  ips{running-vsegs}delete virtual-segment.............................. 170
  ips{running-vsegs}display..................................................... 170
  ips{running-vsegs}rename virtual-segment............................. 170
  ips{running-vsegs}virtual-segment......................................... 170

running-virtual-segment Context Commands............................ 171
  ips{running-vsegs}bind........................................................ 172
  ips{running-vsegs}delete bind.............................................. 172
  ips{running-vsegs}description.............................................. 172
  ips{running-vsegs}display.................................................... 173
  ips{running-vsegs}dst-address............................................ 173
  ips{running-vsegs}delete dst-address.................................... 173
  ips{running-vsegs-VSEG_NAME}ips-profile.............................. 173
  ips{running-vsegs-VSEG_NAME}delete ips-profile...................... 174
  ips{running-vsegs-VSEG_NAME}reputation-profile..................... 174
  ips{running-vsegs-VSEG_NAME}delete reputation-profile.......... 174
  ips{running-vsegs-VSEG_NAME}ssl-profile.............................. 174
  ips{running-vsegs-VSEG_NAME}delete ssl-profile..................... 175
  ips{running-vsegs}move...................................................... 175
  ips{running-vsegs}src-address............................................ 175
  ips{running-vsegs}delete src-address................................... 176
  ips{running-vsegs-vsegname}vlan-id...................................... 176
  ips{running-vsegs}delete vlan-id........................................ 177

running-vlan-translations Context Commands......................... 177
  ips{running-vlan-translations}............................................. 177
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

The following typographic conventions for structuring information are used.

<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,</td>
</tr>
<tr>
<td></td>
<td>buttons, and check boxes. Example: Click <strong>OK</strong> to accept.</td>
</tr>
<tr>
<td><strong>Italics font</strong></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

Information for you to contact product support is available on the TMC at 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>5.0</td>
<td>New features</td>
</tr>
</tbody>
</table>

- Stacking support – Stacking enables you to increase the overall inspection capacity of your TPS security device by grouping multiple TX Series devices and pooling their resources. This feature introduces the following new commands:
  - show stacking

- High availability – You can configure high availability for TPS TX Series devices by using the following commands:
  - high-availability
  - show high-availability

- Master-key support – By default, the system keystore is configured with a device generated key that you can change to a master key passphrase which you specify. The following commands are updated:
  - master-key
<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>◦ show availability</td>
</tr>
<tr>
<td></td>
<td>● sFlow:</td>
</tr>
<tr>
<td></td>
<td>running-sflow Context Commands:</td>
</tr>
<tr>
<td></td>
<td>ips{running-sflow}enable</td>
</tr>
<tr>
<td></td>
<td>ips{running-sflow}disable</td>
</tr>
<tr>
<td></td>
<td>ips{running-sflow}delete</td>
</tr>
<tr>
<td></td>
<td>ips{running-sflow}collector</td>
</tr>
<tr>
<td></td>
<td>ips{running-segment0}sflow</td>
</tr>
<tr>
<td></td>
<td>sflow</td>
</tr>
<tr>
<td></td>
<td>show sflow</td>
</tr>
<tr>
<td></td>
<td>● TACACS+:</td>
</tr>
<tr>
<td></td>
<td>running-aaa-tacacs-group-X Context Commands:</td>
</tr>
<tr>
<td></td>
<td>ips{running-aaa-tacacs-group-group1}delete</td>
</tr>
<tr>
<td></td>
<td>ips{running-aaa-tacacs-group-group1}retries</td>
</tr>
<tr>
<td></td>
<td>ips{running-aaa-tacacs-group-group1}server</td>
</tr>
<tr>
<td></td>
<td>ips{running-aaa-tacacs-group-group1}auth-type</td>
</tr>
<tr>
<td></td>
<td>ips{running-aaa}tacacs-group</td>
</tr>
<tr>
<td></td>
<td>ips{running-aaa-tacacs-group-group1}default-usergroup</td>
</tr>
<tr>
<td></td>
<td>● Inspection Bypass:</td>
</tr>
<tr>
<td></td>
<td>show inspection-bypass</td>
</tr>
<tr>
<td></td>
<td>ips{running-inspection-bypass-rule-myrule1}action</td>
</tr>
</tbody>
</table>

**Updated commands**

- High availability – You can configure high availability for TPS TX Series devices by using the following commands:
  - ◦ high-availability
  - ◦ show high-availability
- ● sFlow updates to the following commands:
  - ◦ segmentx_cli_ips
  - ◦ show_cli_ips.xml
  - ◦ segmentX
- ● TACACS+ updates to the following commands:
  - ◦ ips{running-aaa}display
  - ◦ ips{running-aaa}delete
  - ◦ show aaa
<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
</table>
|         | ◦ tech-support-report  
|         | ◦ ips{running-aaa}remote-login-group |
|         | • Increased VLAN (from 512 to 4094) for virtual segment information added to:  
|         | ◦ virtual-segments  
|         | ◦ running-virtual-segment Context Commands  
|         | ◦ running-virtual-segments Context Commands  
|         | ◦ ips{running-vsegs-vseginame}vlan-id  
|         | • Inspection Bypass enhancements information added to:  
|         | ◦ running-inspection-bypass Context Commands  
|         | • Port agnostic HTTP mode information added to:  
|         | ◦ running-inspection-bypass Context Commands  
|         | • URL filtering information added to:  
|         | ◦ debug  
|         | • Password enhancements:  
|         | ◦ password disallow-reuse (enable|disable)  
|         | ◦ password min-lifetime (enable|disable)  
|         | • You can configure login-banner settings by using the following commands:  
|         | ◦ ips{running-aaa}login-banner (enable|disable)  
|         | ◦ ips{running-aaa}login-banner text  
|         | ◦ ips{running-aaa}login-banner title  
|         | • You can enable or disable the LSM by using the following commands:  
|         | ◦ ips{running-gen}lsm (enable|disable)  
|         | • You can configure an allowed SMS IP address by using the following commands:  
|         | ◦ ips{running-gen}sms-allowed-ip A.B.C.D  
|         | ◦ ips{running-gen}sms-allowed-ip A.B.C.D/M  
|         | ◦ ips{running-gen}sms-allowed-ip X::X::X::X  
<p>|         | ◦ ips{running-gen}sms-allowed-ip X::X::X::X/M |</p>
<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>◦ <code>ips{running-gen}sms-allowed-ip all</code></td>
</tr>
<tr>
<td></td>
<td>• You can disable users who are inactive for 35 days with the following command:</td>
</tr>
<tr>
<td></td>
<td>◦ <code>ips{running-aaa}disable-inactive-users</code></td>
</tr>
<tr>
<td></td>
<td>• You can force logout users to on any authentication changes by using the following command</td>
</tr>
<tr>
<td></td>
<td>◦ `ips{running-aaa}re-auth (enable</td>
</tr>
<tr>
<td></td>
<td>• Miscellaneous updates:</td>
</tr>
<tr>
<td></td>
<td>◦ Updated the external disk reserved space to 3.5 GB in the <code>log-storage</code> command</td>
</tr>
<tr>
<td></td>
<td>◦ Changed the description of the <code>debug np stats show npSslInspStats</code> example (in the <code>debug</code> command)</td>
</tr>
</tbody>
</table>
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:

```
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>ENTER</td>
<td>Runs the command.</td>
</tr>
<tr>
<td>TAB</td>
<td>Completes a partial command.</td>
</tr>
<tr>
<td>?</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>!</td>
<td>Exclamation mark before a command allows you to execute the command from any feature context or sub-level. Example: ips{running-gen)!ping 203.0.113.0</td>
</tr>
<tr>
<td>UP ARROW</td>
<td>Shows the previous command.</td>
</tr>
<tr>
<td>DOWN ARROW</td>
<td>Shows the next command.</td>
</tr>
<tr>
<td>Ctrl + P</td>
<td>Shows the previous command.</td>
</tr>
<tr>
<td>Ctrl + N</td>
<td>Shows the next command.</td>
</tr>
<tr>
<td>Ctrl + L</td>
<td>Clears the screen, does not clear history.</td>
</tr>
<tr>
<td>Shortcut</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<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>
<tr>
<td>Prompt</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------------------------------------</td>
</tr>
<tr>
<td>ips{log-configure}</td>
<td>Displays the log configuration mode.</td>
</tr>
<tr>
<td>ips{log-configure}help</td>
<td>Displays list of valid commands and syntax usage.</td>
</tr>
<tr>
<td>ips{running}exit</td>
<td>Leaves the current configuration mode.</td>
</tr>
<tr>
<td>ips{running}!</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>help or ?</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>help commandname</td>
<td>Displays syntax for a command.</td>
</tr>
<tr>
<td>commandname?</td>
<td>Displays the options for a command. For example, <code>ping ?</code>.</td>
</tr>
<tr>
<td>string?</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:
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 17.

**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.

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

- Object statement:
  ```bash
  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 17.
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**

```plaintext
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.

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

**Valid entries at this position are:**

<table>
<thead>
<tr>
<th>Entry</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa</td>
<td>Configure users, roles, and remote authentication</td>
</tr>
<tr>
<td>actionsets</td>
<td>Enter action sets context</td>
</tr>
<tr>
<td>autodv</td>
<td>Enter autodv context</td>
</tr>
<tr>
<td>blockedStreams</td>
<td>Enter blockedStreams context</td>
</tr>
<tr>
<td>certificates</td>
<td>Enter certificates context</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>debug</td>
<td>Enter debug context</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>dns</td>
<td>Enter DNS context</td>
</tr>
<tr>
<td>exit</td>
<td>Exit edit context, see also save-config</td>
</tr>
<tr>
<td>gen</td>
<td>Timezone, ssh/https access, ip-to-hostname association</td>
</tr>
<tr>
<td>help</td>
<td>Display help information</td>
</tr>
<tr>
<td>high-availability</td>
<td>Enter high-availability context</td>
</tr>
<tr>
<td>interface</td>
<td>Enter interface context</td>
</tr>
<tr>
<td>ips</td>
<td>Enter IPS profile context</td>
</tr>
<tr>
<td>log</td>
<td>Enter log context</td>
</tr>
<tr>
<td>notifycontacts</td>
<td>Enter notify contacts context</td>
</tr>
<tr>
<td>ntp</td>
<td>Enter NTP context</td>
</tr>
<tr>
<td>reputation</td>
<td>Enter Reputation context</td>
</tr>
<tr>
<td>security-policy-reset</td>
<td>Reset IPS security policy to default values</td>
</tr>
<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>

### help

Displays help information.

**Syntax**

`help [full|COMMAND]`

**Example**

```bash
display 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**

Use `boot list-image` to get a list of TOS versions on the device:

```
}boot list-image
Index                               Version
--------------------------------------
0                                    5.0.0.4802i
1                                    5.0.0.4801i
Oldest Index is   0
Factory Reset Index is 1
```

**Example**

Use `boot rollback` to select the TOS version you want:

```
}boot rollback
Index                               Version
--------------------------------------
1                                    5.0.0.4801i
Oldest Index is   0
Factory Reset Index is 1
Select the index of the version you want to roll back to: [1]:
WARNING: System will automatically reboot when upgrade is complete 
Do you want to continue (y/n)? [n]: y
--- Performing software rollback ---
```
chpasswd

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

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

**Syntax**

chpasswd  *user_name*

**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**

```plaintext
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**

ips{}clear log-file audit

**Example**

ips{}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**

ips{}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 TippingPoint product support.

**Syntax**

ddebug

**Valid entries at this position are:**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa</td>
<td>aaa debug options</td>
</tr>
<tr>
<td>autoDV</td>
<td>Access automatic Digital Vaccine (AutoDV) functions</td>
</tr>
<tr>
<td>busy-wait</td>
<td>Wait for UDM</td>
</tr>
<tr>
<td>core-dump</td>
<td>Enable or disable core dumps</td>
</tr>
<tr>
<td>echo</td>
<td>Echo text to console</td>
</tr>
<tr>
<td>factory-reset</td>
<td>Factory Reset</td>
</tr>
<tr>
<td>force-obe</td>
<td>Forces re-run of OBE on the next reset</td>
</tr>
</tbody>
</table>
Examples

See the following examples for more information about debug commands.

**debug factory-reset**

d 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.
### Subcommand

<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>debug np best-effort enable [-queue-latency &lt;microseconds&gt;] [-recover-percent &lt;percent&gt;]</td>
</tr>
<tr>
<td>disable</td>
<td>Disables Best Effort mode.</td>
<td>debug np best-effort disable</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>debug np best-effort enable -queue-latency &lt;microseconds&gt;</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>debug np best-effort enable -recover-percent &lt;percent&gt;</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>Option</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>---------------------------------------------------------------------------------------------------</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.

ddebug 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>Option</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>-----------------------------------------------------------------------------</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.

`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 SSL inspection activity on the device:

```sh
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

**Note:** When an active session is closed, the session count is decremented. If the session count was already set to 0 by the `clear` command, then the session count will incorrectly appear as a very large number.

### debug np congestionx Example

The following example displays potential causes 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
**debug np regex Example**

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

```plaintext
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>0xf4a09ead</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>0x602fe470</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>0xb34d4b62</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>0x65b97c0b</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>0x96dcebfe</td>
<td>P</td>
<td>130</td>
<td>80</td>
<td>18</td>
<td>0</td>
<td>1439</td>
</tr>
</tbody>
</table>

**debug 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 TPS device and clears the sessions information from the LSM:

```plaintext
ips{}debug np ssl-clear
```

**debug np stats Example**

The following example displays system information:

```plaintext
ips{}debug np stats help
```

<table>
<thead>
<tr>
<th>npStats</th>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>udmAggStats</td>
<td>(CP only)</td>
<td>UDM Aggregation Statistics</td>
</tr>
<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>(DP only)</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>(DP only)</td>
<td>NetPal Scan/Sweep Memory Stats</td>
</tr>
<tr>
<td>npScanSweepStats</td>
<td>(DP only)</td>
<td>NetPal Scan/Sweep Statistics</td>
</tr>
<tr>
<td>dpsIpcClassStats</td>
<td></td>
<td>dpsIpc per-class stats</td>
</tr>
<tr>
<td>npZlibStats</td>
<td></td>
<td>NetPal Zlib Stats</td>
</tr>
<tr>
<td>sleuthPatterns</td>
<td>(CP only)</td>
<td>Sleuth pattern table stats</td>
</tr>
<tr>
<td>ruleStatsStats</td>
<td></td>
<td>stats about rule stats</td>
</tr>
<tr>
<td>dpsIpcConv</td>
<td></td>
<td>dpsIpc Conversion stats</td>
</tr>
<tr>
<td>npTrafficCaptureStats</td>
<td></td>
<td>NetPal traffic capture stats</td>
</tr>
<tr>
<td>dpsIpcRpcStats</td>
<td>(CP only)</td>
<td>dpsIpcRpc Stats</td>
</tr>
<tr>
<td>dpwdStats</td>
<td>(CP only)</td>
<td>DP Watchdog Stats</td>
</tr>
<tr>
<td>eccStatsXlrC</td>
<td>(CP only)</td>
<td>XLRC's ECC Stats</td>
</tr>
<tr>
<td>Command Name</td>
<td>(CP only)</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>-----------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>eccStatsXlrB</td>
<td>(CP only)</td>
<td>XLRB's ECC Stats</td>
</tr>
<tr>
<td>eccStatsXlrA</td>
<td>(CP only)</td>
<td>XLRA's ECC Stats</td>
</tr>
<tr>
<td>eccStats</td>
<td>(DP only)</td>
<td>ECC Stats</td>
</tr>
<tr>
<td>dpsTiming</td>
<td>(DP only)</td>
<td>Timing Subsystem</td>
</tr>
<tr>
<td>dpsIpcCPStats</td>
<td>(CP only)</td>
<td>dpsIpc CP Stats</td>
</tr>
<tr>
<td>lwipStats</td>
<td>(DP only)</td>
<td>lwip Stats</td>
</tr>
<tr>
<td>dpsIpcStats</td>
<td>(DP only)</td>
<td>dpsIpc Stats</td>
</tr>
<tr>
<td>snakeStats</td>
<td></td>
<td>Snake Stats</td>
</tr>
<tr>
<td>npTurboSimLfhStats</td>
<td>(DP only)</td>
<td>Turbo Simulator LF Hash Stats</td>
</tr>
<tr>
<td>npQuarantineActionLfhStats</td>
<td>(DP only)</td>
<td>Quarantine Action LF Hash Stats</td>
</tr>
<tr>
<td>npQuarantineAqciLfhStats</td>
<td>(DP only)</td>
<td>Quarantine AQCI LF Hash Stats</td>
</tr>
<tr>
<td>npQuarantineStats</td>
<td>(DP only)</td>
<td>NetPal Quarantine Packet Stats</td>
</tr>
<tr>
<td>npSynProxyStats</td>
<td>(DP only)</td>
<td>NetPal SYN Proxy Statistics</td>
</tr>
<tr>
<td>npIpReputationIpenderitStats</td>
<td>(null)</td>
<td>IP Reputation command IPC Stats</td>
</tr>
<tr>
<td>npIpReputationRequestStats</td>
<td>(CP only)</td>
<td>(null)</td>
</tr>
<tr>
<td>npIpReputationCallbackStats</td>
<td>(DP only)</td>
<td>IP Reputation Callback Stats</td>
</tr>
<tr>
<td>npDnsReputationStats</td>
<td>(DP only)</td>
<td>DNS Reputation Statistics</td>
</tr>
<tr>
<td>npUrlReputationStats</td>
<td>(DP only)</td>
<td>URL Reputation Statistics</td>
</tr>
<tr>
<td>npHreStats</td>
<td>(DP only)</td>
<td>Rule Statistics</td>
</tr>
<tr>
<td>npSoftLinXStats</td>
<td>(DP only)</td>
<td>NetPal SOFTLINX Statistics</td>
</tr>
<tr>
<td>trhaStats</td>
<td>(DP only)</td>
<td>TRHA Statistics</td>
</tr>
<tr>
<td>npTcpStateStats</td>
<td>(DP only)</td>
<td>TCP State module stats.</td>
</tr>
<tr>
<td>rlStats</td>
<td>(DP only)</td>
<td>Policy Rate Limiter Statistics</td>
</tr>
<tr>
<td>npHCосpStats</td>
<td>(DP only)</td>
<td>NetPal HardCode Statistics</td>
</tr>
<tr>
<td>npIPDgrams</td>
<td>(DP only)</td>
<td>(null)</td>
</tr>
<tr>
<td>npZoneStats</td>
<td>(DP only)</td>
<td>ZoneStats</td>
</tr>
<tr>
<td>npTelnetStats</td>
<td>(DP only)</td>
<td>TELNET Decode Statistics</td>
</tr>
<tr>
<td>npSnmpStats</td>
<td>(DP only)</td>
<td>SNMP Decode Statistics</td>
</tr>
<tr>
<td>npSmtpStats</td>
<td>(DP only)</td>
<td>SMTP Decode Statistics</td>
</tr>
<tr>
<td>npSmbStats</td>
<td>(DP only)</td>
<td>SMB Decode Statistics</td>
</tr>
<tr>
<td>npRpcStats</td>
<td>(DP only)</td>
<td>RPC Decode Statistics</td>
</tr>
<tr>
<td>npMsrpcStats</td>
<td>(DP only)</td>
<td>MS-RPC Decode Statistics</td>
</tr>
<tr>
<td>npOspfStats</td>
<td>(DP only)</td>
<td>OSPF Decode Statistics</td>
</tr>
<tr>
<td>npImapStats</td>
<td>(DP only)</td>
<td>IMAP Decode Statistics</td>
</tr>
<tr>
<td>npHttpStats</td>
<td>(DP only)</td>
<td>HTTP Decode Statistics</td>
</tr>
<tr>
<td>ahpStats</td>
<td>(DP only)</td>
<td>ahp Stats</td>
</tr>
<tr>
<td>npFtpStats</td>
<td>(DP only)</td>
<td>FTP Decode Statistics</td>
</tr>
<tr>
<td>npDnsStats</td>
<td>(DP only)</td>
<td>DNS Decode Statistics</td>
</tr>
<tr>
<td>udmCbStats</td>
<td></td>
<td>UDM Callback Statistics</td>
</tr>
<tr>
<td>npTTStats</td>
<td>(null)</td>
<td>NetPal Trust Table Statistics</td>
</tr>
<tr>
<td>npCTStats</td>
<td></td>
<td>NetPal Connection Table Statistics</td>
</tr>
<tr>
<td>pcbStats</td>
<td>(DP only)</td>
<td>PCB Stats</td>
</tr>
<tr>
<td>txStats</td>
<td>(DP only)</td>
<td>TX Stats</td>
</tr>
<tr>
<td>rxStats</td>
<td>(DP only)</td>
<td>Rx Stats</td>
</tr>
<tr>
<td>threadFwdStats</td>
<td>(DP only)</td>
<td>NetPal Parse Packet Statistics</td>
</tr>
<tr>
<td>npHardCodeStats</td>
<td>(DP only)</td>
<td>HardCode Packet Statistics</td>
</tr>
<tr>
<td>npFilterStatsInst</td>
<td>(DP only)</td>
<td>(null)</td>
</tr>
<tr>
<td>npReparseStatsInst</td>
<td>(DP only)</td>
<td>NetPal Non-ingress Parse Packet Stats</td>
</tr>
<tr>
<td>npParseStatsInst</td>
<td>(DP only)</td>
<td>NetPal Parse Packet Statistics</td>
</tr>
<tr>
<td>npTcpReas</td>
<td>(DP only)</td>
<td>TCP Reassembly Statistics</td>
</tr>
<tr>
<td>npReasIpv6</td>
<td>(DP only)</td>
<td>IPv6 Reassembly Statistics</td>
</tr>
<tr>
<td>npReas</td>
<td>(DP only)</td>
<td>IPv4 Reassembly Statistics</td>
</tr>
<tr>
<td>dpk</td>
<td>(DP only)</td>
<td>Data Plane Stats</td>
</tr>
</tbody>
</table>
Sample stats

```plaintext
triv

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:

```plaintext
ips{}debug np port show

PORT status:
Local Device 0 (switch in NORMAL mode) ------------------------------

<table>
<thead>
<tr>
<th>Port</th>
<th>Bcm</th>
<th>Num</th>
<th>Admin</th>
<th>Status</th>
<th>Speed</th>
<th>AutoNeg</th>
<th>Pause</th>
<th>Mode</th>
<th>MTU</th>
<th>Medium</th>
<th>SP</th>
<th>MMU</th>
</tr>
</thead>
<tbody>
<tr>
<td>enet1</td>
<td>ge1</td>
<td>3</td>
<td>Disabled</td>
<td>DOWN</td>
<td>1Gbps</td>
<td>auto</td>
<td>-</td>
<td>GMII</td>
<td>1526</td>
<td>Fiber</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>enet2</td>
<td>ge0</td>
<td>2</td>
<td>Disabled</td>
<td>DOWN</td>
<td>1Gbps</td>
<td>auto</td>
<td>-</td>
<td>GMII</td>
<td>1526</td>
<td>Fiber</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>enet3</td>
<td>ge3</td>
<td>5</td>
<td>Disabled</td>
<td>DOWN</td>
<td>1Gbps</td>
<td>auto</td>
<td>-</td>
<td>GMII</td>
<td>1526</td>
<td>Fiber</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>enet4</td>
<td>ge2</td>
<td>4</td>
<td>Disabled</td>
<td>DOWN</td>
<td>1Gbps</td>
<td>auto</td>
<td>-</td>
<td>GMII</td>
<td>1526</td>
<td>Fiber</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>enet5</td>
<td>ge5</td>
<td>7</td>
<td>Disabled</td>
<td>DOWN</td>
<td>1Gbps</td>
<td>auto</td>
<td>-</td>
<td>GMII</td>
<td>1526</td>
<td>Fiber</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>enet6</td>
<td>ge4</td>
<td>6</td>
<td>Disabled</td>
<td>DOWN</td>
<td>1Gbps</td>
<td>auto</td>
<td>-</td>
<td>GMII</td>
<td>1526</td>
<td>Fiber</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>enet7</td>
<td>ge7</td>
<td>9</td>
<td>Disabled</td>
<td>DOWN</td>
<td>1Gbps</td>
<td>auto</td>
<td>-</td>
<td>GMII</td>
<td>1526</td>
<td>Fiber</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>enet8</td>
<td>ge6</td>
<td>8</td>
<td>Disabled</td>
<td>DOWN</td>
<td>1Gbps</td>
<td>auto</td>
<td>-</td>
<td>GMII</td>
<td>1526</td>
<td>Fiber</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>enet9</td>
<td>ge9</td>
<td>11</td>
<td>Enabled</td>
<td>UP</td>
<td>1Gbps</td>
<td>auto</td>
<td>none</td>
<td>GMII</td>
<td>1526</td>
<td>Copper</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>enet10</td>
<td>ge8</td>
<td>10</td>
<td>Enabled</td>
<td>UP</td>
<td>1Gbps</td>
<td>auto</td>
<td>none</td>
<td>SGMI</td>
<td>1526</td>
<td>Copper</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>enet11</td>
<td>ge11</td>
<td>13</td>
<td>Enabled</td>
<td>UP</td>
<td>1Gbps</td>
<td>auto</td>
<td>none</td>
<td>SGMI</td>
<td>1526</td>
<td>Copper</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>enet12</td>
<td>ge10</td>
<td>12</td>
<td>Enabled</td>
<td>UP</td>
<td>1Gbps</td>
<td>auto</td>
<td>none</td>
<td>SGMI</td>
<td>1526</td>
<td>Copper</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>enet13</td>
<td>ge13</td>
<td>15</td>
<td>Disabled</td>
<td>-</td>
<td>auto</td>
<td>-</td>
<td>SGMI</td>
<td>1526</td>
<td>Copper</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>enet14</td>
<td>ge12</td>
<td>14</td>
<td>Disabled</td>
<td>-</td>
<td>auto</td>
<td>-</td>
<td>SGMI</td>
<td>1526</td>
<td>Copper</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>enet15</td>
<td>ge15</td>
<td>17</td>
<td>Enabled</td>
<td>UP</td>
<td>1Gbps</td>
<td>auto</td>
<td>none</td>
<td>SGMI</td>
<td>1526</td>
<td>Copper</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>enet16</td>
<td>ge14</td>
<td>16</td>
<td>Enabled</td>
<td>UP</td>
<td>1Gbps</td>
<td>auto</td>
<td>none</td>
<td>SGMI</td>
<td>1526</td>
<td>Copper</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>uplnk0</td>
<td>xe0</td>
<td>26</td>
<td>Uplink</td>
<td>UP</td>
<td>10Gbps</td>
<td>none</td>
<td>none</td>
<td>XGMI</td>
<td>16356</td>
<td>Fiber</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>uplnk1</td>
<td>xe1</td>
<td>27</td>
<td>Uplink</td>
<td>UP</td>
<td>10Gbps</td>
<td>none</td>
<td>none</td>
<td>XGMI</td>
<td>16356</td>
<td>Fiber</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>uplnk2</td>
<td>xe2</td>
<td>28</td>
<td>Uplink</td>
<td>UP</td>
<td>10Gbps</td>
<td>none</td>
<td>-</td>
<td>XGMI</td>
<td>16356</td>
<td>Fiber</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>uplnk3</td>
<td>xe3</td>
<td>29</td>
<td>Uplink</td>
<td>UP</td>
<td>10Gbps</td>
<td>none</td>
<td>-</td>
<td>XGMI</td>
<td>16356</td>
<td>Fiber</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

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
```
Advertised ability: 
- medium = <none>
- pause = pause_tx, pause_rx, pause_asymm
- lb = none, MAC, PHY
- flags = autoneg

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

**debug show settings Example**

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

```plaintext
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**

```plaintext
display
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.

```plaintext
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.

```plaintext
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:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa</td>
<td>Configure users, roles, and remote authentication</td>
</tr>
<tr>
<td>actionsets</td>
<td>Enter action sets context</td>
</tr>
<tr>
<td>autodv</td>
<td>Enter autodv context</td>
</tr>
<tr>
<td>blockedStreams</td>
<td>Enter blockedStreams context</td>
</tr>
<tr>
<td>certificates</td>
<td>Enter certificates context</td>
</tr>
<tr>
<td>debug</td>
<td>Enter debug context</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>dns</td>
<td>Enter DNS context</td>
</tr>
<tr>
<td>exit</td>
<td>Exit edit context, see also save-config</td>
</tr>
<tr>
<td>gen</td>
<td>Timezone, ssh/https access, ip-to-hostname association</td>
</tr>
<tr>
<td>help</td>
<td>Display help information</td>
</tr>
<tr>
<td>high-availability</td>
<td>Enter high-availability context</td>
</tr>
<tr>
<td>interface</td>
<td>Enter interface context</td>
</tr>
<tr>
<td>ips</td>
<td>Enter IPS profile context</td>
</tr>
<tr>
<td>log</td>
<td>Enter log context</td>
</tr>
<tr>
<td>notifycontacts</td>
<td>Enter notify contacts context</td>
</tr>
<tr>
<td>ntp</td>
<td>Enter NTP context</td>
</tr>
<tr>
<td>reputation</td>
<td>Enter Reputation context</td>
</tr>
<tr>
<td>security-policy-reset</td>
<td>Reset IPS security policy to default values</td>
</tr>
<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>
</tbody>
</table>
virtual-segments Enter virtual-segments context

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

fips-mode-enable

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

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

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

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

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

**Syntax**

fips-mode-enable

**Example**

ips{}fips-mode-enable
WARNING: To ensure FIPS compliance, the user must reset this device to factory default settings before running this command. For more information, see product documentation for details about how to enable FIPS mode.
WARNING: Has this device been reset to factory default settings? <y/[n]> [n]: y
WARNING: Once FIPS mode is enabled, it cannot be disabled except by resetting the device to factory defaults.
Warning: Type 'COMMIT' to enable FIPS mode: COMMIT
Settings will not take effect until reboot

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

Exaple
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]

Exaple
ips{running}help log
Enter log context
Syntax: log
log Enter log context

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

• INHA determines how the device manages traffic on each segment in the event of a system failure:
  ◦ Layer-2 Fallback (L2FB) – Either permits or blocks all traffic on each segment, depending on the
    INHA L2FB action setting for the segment. Any permitted traffic is not inspected.
    Important: If you enable INHA L2FB, L2FB not persist when you reboot the device.
  ◦ Normal – Permits and inspects traffic across all segments.
• ZPHA determines how the device routes traffic in the event of a loss of system power:
- **Bypass** – Bypasses traffic at the port level to maintain high availability of any network segments that have ZPHA support. When ZPHA bypass is enabled, the INHA Layer-2 fallback action setting for each segment is ignored.

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

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

ZPHA support varies by device:

- On a TippingPoint TX Series device, optional bypass I/O modules provide high availability for copper and fiber segments. You can enable bypass mode on a particular slot or all slots with a bypass I/O module.

- On a TippingPoint 2200T security device, ZPHA support is built-in for copper segments. An external ZPHA module is required to enable ZPHA on SFP and SFP+ segments. Bypass mode can be enabled on all segments of the device only.

- On a TippingPoint 440T security device, ZPHA support is built-in for copper segments only. Bypass mode can be enabled on all segments of the device only.

- On a TippingPoint Virtual Threat Protection System (vTPS) security device, ZPHA bypass mode cannot be enabled.

**Syntax**

Enables INHA L2FB.

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

Enables ZPHA bypass.

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

**Example**

Enable INHA L2FB.

```
ips{running}high-availability force fallback
Status: OK
```

Disable INHA L2FB.

```
ips{running}high-availability force normal
Status: OK
```

Enable ZPHA bypass on a TPS 440T or 2200T security device. When you configure a 440T or 2200T, you do not need to specify the `all` parameter to configure ZPHA on the device.

```
ips{running}high-availability zero-power bypass-ips
Status: OK
```
Enable ZPHA bypass on slot 3 of a TPS 8400TX security device. When you configure a TX Series device, use the slot parameter to specify a particular I/O slot or the all parameter to specify all slots.

```bash
ips{running}high-availability zero-power slot 3 bypass-ips
Status: OK
```

Disable ZPHA bypass. When you configure a TX Series device, use the slot parameter to specify a particular I/O slot or the all parameter to specify all slots.

```bash
ips{running}high-availability zero-power slot 3 normal
Status: OK
```

Disable ZPHA bypass on a TPS 2200T security device.

```bash
ips{running}high-availability zero-power normal
Status: OK
```

## keystore

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

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

Change the keystore mode, for example, if the SMS is unreachable and you want the device to persist its own private keys. Use the `sms-unmanage` command to unmanage the device, and then use the `keystore on-device` command to change the keystore mode to the local keystore. After you change the keystore mode, use the `save-config` command to copy the running configuration (which includes the private keys in the Running configuration) to the Start configuration. If the private keys are not in the running configuration, for example, because you rebooted the device after you unmanaged it, use the `private-key` command to import the private keys manually.

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

### Syntax

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

### Related commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ips{running-certificates}private-key</code> on page 124</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><strong>ips{running-certificates}certificate</strong> on page 122</td>
<td>Import the certificate from your web server into the local keystore on the device.</td>
</tr>
<tr>
<td><strong>ips{running-sslinsp}server</strong> on page 165</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
**Example**

```plaintext
ips{} logout
```

**master-key**

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

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

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

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

Enter an option to set the master key:

- `passphrase` – This option allows you to specify a passphrase for the master key.
  
  The passphrase must meet the following complexity requirements:
  
  - Must be between 9 and 32 characters in length
  - Combination of uppercase and lowercase alpha and numbers
  - Must contain at least one special character (!@#$%)
- `device-generated-key` – This option generates a passphrase for the master key.

**Syntax**

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

**Example**

```plaintext
ips{} logout
```
Set the system master key with your own passphrase.

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

```plaintext
(master-key set passphrase
Please validate with your user password:
user password: ********
WARNING: Master key will be set to a passphrase and used to encrypt the keystore and user disk.
WARNING: This device is currently using a device generated 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
Enter Master Key : **********
Re-enter Master Key: **********
Success: Master key has been set.
```

**Example**

Set the system master key to a device-generated master key.

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

```plaintext
(master-key set device-generated-key
Please validate with your user password:
user password: ********
WARNING: Master key will be set to a device generated key and used to encrypt the keystore and user disk.
Keystore data in snapshots created with the device generated 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 generated key.
```

**Example**

Reset the keystore to erase the contents of the system keystore. This command does not change the master key.

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

```plaintext
(master-key reset-keystore
Please validate with your user password:
user password: ********
WARNING: This device is currently using a device generated key.
Changing this key will make keystore data in snapshots created with the previous key non-recoverable.
```
WARNING: Resetting keystore will delete all private keys currently held in the keystore. 
Do you want to continue (y/n)? [n]: y
Success:
WARNING: All private keys in the keystore have been deleted. Running configuration may be in an inconsistent state. Please re-import any previously saved private keys to ensure configuration consistency.

**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**

```bash
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**

```bash
ips{}ping6 100::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 65

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]:

Threat Protection System Command Line Interface Reference
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 Startup 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><code>commit</code> on page 15</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
ingservice-access disable
```

**set**

Configures an item.

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

Example

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

**setup**

Runs the setup wizard.

**Syntax**

```plaintext
setup
```

**show**

View current system configuration, status, and statistics.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>show aaa</strong> on page 47</td>
<td>Show AAA information.</td>
</tr>
<tr>
<td><strong>show auxdv</strong> on page 49</td>
<td>Show the AuxDV package.</td>
</tr>
<tr>
<td><strong>show date</strong> on page 49</td>
<td>Show the current router date and time.</td>
</tr>
<tr>
<td><strong>show dns</strong> on page 49</td>
<td>Show Domain Name Service.</td>
</tr>
<tr>
<td><strong>show filter</strong> on page 50</td>
<td>Show filter information.</td>
</tr>
<tr>
<td><strong>show health</strong> on page 51</td>
<td>Show health information.</td>
</tr>
<tr>
<td><strong>show high-availability</strong> on page 52</td>
<td>Show high-availability status.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td><code>show interface</code> on page 54</td>
<td>Show network interface.</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 55</td>
<td>Show the license number and status.</td>
</tr>
<tr>
<td><code>show log-file</code> on page 55</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 61</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>Command</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>--------------------------------------------------------------------</td>
</tr>
<tr>
<td><code>show np softlinx</code> on page 63</td>
<td>Show network processor softlinx statistics.</td>
</tr>
<tr>
<td><code>show np tier-stats</code> on page 63</td>
<td>Show network processor throughput and utilization for each tier.</td>
</tr>
<tr>
<td><code>show quarantine-list</code> on page 65</td>
<td>Show quarantine list information.</td>
</tr>
<tr>
<td><code>show reports</code> on page 65</td>
<td>Show status of data collection for reports.</td>
</tr>
<tr>
<td><code>show service</code> on page 65</td>
<td>Show network service information.</td>
</tr>
<tr>
<td><code>show sflow</code> on page 66</td>
<td>Show sFlow sampling configuration information.</td>
</tr>
<tr>
<td><code>show sms</code> on page 67</td>
<td>Show status of SMS control.</td>
</tr>
<tr>
<td><code>show snmp</code> on page 67</td>
<td>Show SNMP information.</td>
</tr>
<tr>
<td><code>show stacking</code> on page 68</td>
<td>Show stacking information.</td>
</tr>
<tr>
<td><code>show system connections</code> on page 69</td>
<td>Show active socket information.</td>
</tr>
<tr>
<td><code>show system processes</code> on page 70</td>
<td>Show system processes.</td>
</tr>
<tr>
<td><code>show system queue-stats</code> on page 71</td>
<td>Show internal queue stats.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>--------------------------------------------------------------</td>
</tr>
<tr>
<td><code>show system statistics</code> on page 71</td>
<td>Show system-wide protocol-related statistics.</td>
</tr>
<tr>
<td><code>show system usage</code> on page 72</td>
<td>Show system usage.</td>
</tr>
<tr>
<td><code>show system virtual-memory</code> on page 72</td>
<td>Show system virtual memory.</td>
</tr>
<tr>
<td><code>show system xms memory</code> on page 73</td>
<td>Show xms memory usage.</td>
</tr>
<tr>
<td><code>show terminal</code> on page 73</td>
<td>Show terminal settings.</td>
</tr>
<tr>
<td><code>show traffic-file</code> on page 73</td>
<td>Show network traffic from file.</td>
</tr>
<tr>
<td><code>show tse</code> on page 74</td>
<td>Show threat suppression engine information.</td>
</tr>
<tr>
<td><code>show user-disk</code> on page 75</td>
<td>Show user-disk statistics.</td>
</tr>
<tr>
<td><code>show users</code> on page 75</td>
<td>Show users information.</td>
</tr>
<tr>
<td><code>show version</code> on page 76</td>
<td>Show device version information.</td>
</tr>
<tr>
<td><code>show virtual segments</code> on page 76</td>
<td>Show virtual segment configuration.</td>
</tr>
</tbody>
</table>

**show aaa**

**Syntax**
show aaa capabilities USER

<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>
<tr>
<td>15</td>
<td>ACTIONSETS</td>
<td>full</td>
</tr>
<tr>
<td>16</td>
<td>SYSTEM</td>
<td>full</td>
</tr>
<tr>
<td>17</td>
<td>SMSMANAGED</td>
<td>full</td>
</tr>
<tr>
<td>18</td>
<td>MANAGEMENT</td>
<td>full</td>
</tr>
<tr>
<td>19</td>
<td>DNS</td>
<td>full</td>
</tr>
<tr>
<td>20</td>
<td>IPFILTERS</td>
<td>full</td>
</tr>
<tr>
<td>21</td>
<td>UPGRADE</td>
<td>full</td>
</tr>
<tr>
<td>22</td>
<td>NOTIFICATION</td>
<td>full</td>
</tr>
<tr>
<td>23</td>
<td>LOGGING</td>
<td>full</td>
</tr>
<tr>
<td>24</td>
<td>HIGHAVAILABILITY</td>
<td>full</td>
</tr>
<tr>
<td>25</td>
<td>HACONFIGURATION</td>
<td>full</td>
</tr>
<tr>
<td>26</td>
<td>HASTATE</td>
<td>full</td>
</tr>
<tr>
<td>27</td>
<td>SNMP</td>
<td>full</td>
</tr>
<tr>
<td>28</td>
<td>TIME</td>
<td>full</td>
</tr>
<tr>
<td>29</td>
<td></td>
<td>full</td>
</tr>
<tr>
<td>30</td>
<td>UPDATE</td>
<td>full</td>
</tr>
<tr>
<td>31</td>
<td>PACKAGES</td>
<td>full</td>
</tr>
<tr>
<td>32</td>
<td>AUTODV</td>
<td>full</td>
</tr>
<tr>
<td>33</td>
<td>SNAPSHOT</td>
<td>full</td>
</tr>
<tr>
<td>34</td>
<td>USERAUTH</td>
<td>full</td>
</tr>
<tr>
<td>35</td>
<td>LOCALUSER</td>
<td>full</td>
</tr>
<tr>
<td>36</td>
<td>USERGROUP</td>
<td>full</td>
</tr>
<tr>
<td>37</td>
<td>ROLES</td>
<td>full</td>
</tr>
<tr>
<td>38</td>
<td>RADIUS</td>
<td>full</td>
</tr>
<tr>
<td>39</td>
<td>LDAP</td>
<td>full</td>
</tr>
<tr>
<td>41</td>
<td>GENERAL</td>
<td>full</td>
</tr>
<tr>
<td>42</td>
<td>X509CERT</td>
<td>full</td>
</tr>
<tr>
<td>53</td>
<td>REPORTING</td>
<td>full</td>
</tr>
<tr>
<td>54</td>
<td>LOG</td>
<td>full</td>
</tr>
<tr>
<td>56</td>
<td>IPSLOG</td>
<td>full</td>
</tr>
<tr>
<td>57</td>
<td>REPUTATIONLOG</td>
<td>full</td>
</tr>
<tr>
<td>59</td>
<td>SYSTEMLOG</td>
<td>full</td>
</tr>
<tr>
<td>60</td>
<td>AUDITLOG</td>
<td>full</td>
</tr>
<tr>
<td>61</td>
<td>SECURITYREPORTS</td>
<td>full</td>
</tr>
<tr>
<td>62</td>
<td>NETWORKREPORTS</td>
<td>full</td>
</tr>
<tr>
<td>63</td>
<td>DEBUGTOOLS</td>
<td>full</td>
</tr>
<tr>
<td>64</td>
<td>REBOOT</td>
<td>full</td>
</tr>
<tr>
<td>65</td>
<td>SHUTDOWN</td>
<td>full</td>
</tr>
<tr>
<td>66</td>
<td>SERVICEACCESS</td>
<td>full</td>
</tr>
<tr>
<td>67</td>
<td>NETWORK</td>
<td>full</td>
</tr>
<tr>
<td>68</td>
<td>INTERFACES</td>
<td>full</td>
</tr>
</tbody>
</table>
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
## show filter

Displays the filters.

### Syntax

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

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

### Example

```plaintext
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>VSB3</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 (fallback|normal)

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

show inspection-bypass

Syntax

show inspection-bypass

Example

ips{}show inspection-bypass

#############################
# INSPECTION BYPASS RULES #
#############################

Rule Name: test-1
ID: 2
Enabled: true
EthType: ip
Ports: <any>
IP Proto: <any>
VLAN ID: <any>
Source Port: <any>
Destination Port: <any>
Source Address: 12.34.56.7/89
Destination Address: <any>
Action Bypass
Packets matching switch rule: 0
Hardware resources: 20

Rule Name: test2
ID: 3
Enabled: true
EthType: ip
Ports: <any>
IP Proto: <any>
VLAN ID Range: 100-119
Source Port: <any>
Destination Port: <any>
Source Address: <any>
Destination Address: <any>
Action Redirect 5B
Packets matching switch rule: 0
Hardware resources: 400
**show interface**

**Syntax**

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

**Example**

```
ips{}show interface 1-1A
Interface           1-1A
MAC Address         00:10:f3:2c:81:df
Admin State         Enabled
Link                Up
Speed               1000Mbps
Auto Negotiate      Enabled
Duplex              Full
Line Type           Copper
MTU                 9208

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
- 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

```bash
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:

```bash
ips{} show log-file boot tail 5
  bridgel: port 8(ethernet7) entering disabled state
  bridgel: 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] [ASC|DESC|(tail [COUNT])] [seqnum] [more]
show log-file ipsAlert [raw|tab|csv|rawcsv] [addUUID] [ASC|DESC|(tail [COUNT])] [seqnum] [more]
show log-file ipsBlock [raw|tab|csv|rawcsv] [addUUID] [ASC|DESC|(tail [COUNT])] [seqnum] [more]
show log-file quarantine [raw|tab|csv|rawcsv] [addUUID] [ASC|DESC|(tail [COUNT])] [seqnum] [more]
show log-file reputationAlert [raw|tab|csv|rawcsv] [addUUID] [ASC|DESC|(tail [COUNT])] [seqnum] [more]
show log-file reputationBlock [raw|tab|csv|rawcsv] [addUUID] [ASC|DESC|(tail [COUNT])] [seqnum] [more]
show log-file summary [raw|tab|csv|rawcsv] [addUUID] [ASC|DESC|(tail [COUNT])] [seqnum] [more]
show log-file system [raw|tab|csv|rawcsv] [addUUID] [ASC|DESC|(tail [COUNT])] [seqnum] [more]
show log-file boot [raw|tab|csv|rawcsv] [addUUID] [ASC|DESC|(tail [COUNT])] [seqnum] [more]
```
show log-file audit [raw|tab|csv|rawcsv] [addUUID] [ASC|DESC]
    [search [(options)](0,2) PATTERN] [start-time START] [end-time END]
    [seqnum[ [begin BEGIN] [end END]]] [count COUNT] [more]

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

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

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

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

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

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

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

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

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

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

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

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

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

show log-file reputationBlock [raw|tab|csv|rawcsv] [addUUID] [ASC|DESC]
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...
1
241097
241097

show log-file summary

Syntax

show log-file summary [verbose]

Example

ips{}show log-file summary

<table>
<thead>
<tr>
<th>File</th>
<th>Total Entries</th>
<th>First Entry</th>
<th>Last Entry</th>
<th>Allocated</th>
<th>Used</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>system</td>
<td>2902</td>
<td>1</td>
<td>2902</td>
<td>174.32 MB</td>
<td>0%</td>
<td>internal</td>
</tr>
<tr>
<td>audit</td>
<td>411</td>
<td>1</td>
<td>411</td>
<td>174.32 MB</td>
<td>0%</td>
<td>internal</td>
</tr>
<tr>
<td>ipsAlert</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>350.11 MB</td>
<td>0%</td>
<td>ramdisk</td>
</tr>
<tr>
<td>ipsBlock</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>350.11 MB</td>
<td>0%</td>
<td>ramdisk</td>
</tr>
<tr>
<td>reputationAlert</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>175.06 MB</td>
<td>0%</td>
<td>ramdisk</td>
</tr>
<tr>
<td>reputationBlock</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>175.06 MB</td>
<td>0%</td>
<td>ramdisk</td>
</tr>
<tr>
<td>quarantine</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>175.06 MB</td>
<td>0%</td>
<td>ramdisk</td>
</tr>
</tbody>
</table>

show mfg-info
Shows manufacturing information.

Syntax
show mfg-info

Example

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

<table>
<thead>
<tr>
<th>General Statistics:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incoming =</td>
</tr>
<tr>
<td>Outgoing =</td>
</tr>
<tr>
<td>Dropped =</td>
</tr>
<tr>
<td>Interface discards =</td>
</tr>
<tr>
<td>Second Tier =</td>
</tr>
<tr>
<td>Matched =</td>
</tr>
<tr>
<td>Blocked =</td>
</tr>
<tr>
<td>Trusted =</td>
</tr>
<tr>
<td>Permitted =</td>
</tr>
<tr>
<td>Invalid =</td>
</tr>
<tr>
<td>Rate Limited =</td>
</tr>
</tbody>
</table>

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>Packets</th>
<th>Bytes</th>
</tr>
</thead>
</table>
### show np reassembly

**Syntax**

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

**Example**

```bash
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

Example

show np softlinx

Syntax

show np softlinx

Example

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

```plaintext
token{}show np tier-stats

---

**Tier 1 (Physical Ports):**

<table>
<thead>
<tr>
<th>Metric</th>
<th>Value</th>
<th>Max</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rx Mbps</td>
<td>261.7</td>
<td>1,250.0</td>
</tr>
<tr>
<td>Tx Mbps</td>
<td>270.4</td>
<td>1,248.6</td>
</tr>
<tr>
<td>Rx Packets/Sec</td>
<td>31,054.0</td>
<td>111,814.0</td>
</tr>
<tr>
<td>Tx Packets/Sec</td>
<td>45,279.0</td>
<td>111,682.0</td>
</tr>
<tr>
<td>Utilization</td>
<td>23.7%</td>
<td>100.0%</td>
</tr>
<tr>
<td>Ratio to next tier</td>
<td>100.0%</td>
<td>0.0%</td>
</tr>
</tbody>
</table>

---

**Tier 2 (Software Fastpath):**

<table>
<thead>
<tr>
<th>Metric</th>
<th>Value</th>
<th>Max</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rx Mbps</td>
<td>261.7</td>
<td>838.2</td>
</tr>
<tr>
<td>Rx Packets/Sec</td>
<td>31,054.0</td>
<td>74,982.0</td>
</tr>
<tr>
<td>Tx trust packets/sec</td>
<td>0.0</td>
<td>0.0</td>
</tr>
<tr>
<td>Utilization</td>
<td>23.7%</td>
<td>76.2%</td>
</tr>
<tr>
<td>Ratio to next tier</td>
<td>100.0%</td>
<td>99.6%</td>
</tr>
</tbody>
</table>

---

**Tier 3 (IPS Engine Fastpath):**

<table>
<thead>
<tr>
<th>Metric</th>
<th>Value</th>
<th>Max</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rx Mbps</td>
<td>261.7</td>
<td>836.4</td>
</tr>
<tr>
<td>Rx Packets/Sec</td>
<td>31,054.0</td>
<td>74,781.0</td>
</tr>
<tr>
<td>Tx trust packets/sec</td>
<td>0.0</td>
<td>0.0</td>
</tr>
<tr>
<td>Utilization</td>
<td>23.7%</td>
<td>76.0%</td>
</tr>
<tr>
<td>Ratio to next tier</td>
<td>0.0%</td>
<td>0.0%</td>
</tr>
</tbody>
</table>

---

**Tier 4 (IPS Engine Slowpath):**

<table>
<thead>
<tr>
<th>Metric</th>
<th>Value</th>
<th>Max</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rx Mbps</td>
<td>0.0</td>
<td>0.0</td>
</tr>
<tr>
<td>Rx Packets/Sec</td>
<td>0.0</td>
<td>2.0</td>
</tr>
<tr>
<td>Trigger match</td>
<td>0.0%</td>
<td>0.0%</td>
</tr>
<tr>
<td>Reroute</td>
<td>0.0%</td>
<td>50.0%</td>
</tr>
<tr>
<td>TCP sequence</td>
<td>0.0%</td>
<td>0.0%</td>
</tr>
<tr>
<td>Protocol decode</td>
<td>0.0%</td>
<td>0.0%</td>
</tr>
<tr>
<td>Utilization</td>
<td>0.0%</td>
<td>0.0%</td>
</tr>
<tr>
<td>Ratio to deep</td>
<td>0.0%</td>
<td>0.0%</td>
</tr>
</tbody>
</table>

---

**Tier 5 (SSL Inspection):**

<table>
<thead>
<tr>
<th>Metric</th>
<th>Value</th>
<th>Max</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rx Mbps</td>
<td>252.7</td>
<td>257.7</td>
</tr>
<tr>
<td>Rx Packets/Sec</td>
<td>21,823.0</td>
<td>22,256.0</td>
</tr>
<tr>
<td>Utilization</td>
<td>22.9%</td>
<td>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 sflow

Syntax

show sflow

Example

```plaintext
ips{}show sflow
SFLOW
   Enabled: Yes
   Collector 1: 1.1.1.1 6343
   Collector 2: 2.2.2.2 6343
Segment1
   Enabled: Yes
   Rate   : 750
Segment2
   Enabled: No
   Rate   : 1000
Segment3
   Enabled: No
   Rate   : 1000
Segment4
   Enabled: No
   Rate   : 1000
```

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

Show slot information for an 8400TX security device.

```plaintext
ips{}show slot
#################################################################
#     SLOT INFO          #
#################################################################
Slot 1
   State         : Active
   Module Type   : HP NX IPS 6-segment Gig-T Module
   Module Serial : PR131GC010
Slot 2
   State         : Empty
   Module Type   : Empty
   Module Serial : N/A
Slot 3
```
State         : Empty
Module Type   : Empty
Module Serial : N/A

Slot 4
State         : Active
Module Type   : HP NX IPS 6-segment GbE SFP Module
Module Serial : PR51FH8WSR

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 stacking**

Enter this command to show stacking status information.

**Required privilege**

Admin, Operator, Super-User

**Use**

The following example shows the default output for a device that does not support stacking. To support stacking, the device must be a supported model running TippingPoint Operating System (TOS) v5.0.0 (or later).

```
ips{} show stacking
This device does not support stacking.
```

The following example shows the default output for a supported device that is not a member of the stack.

```
ips{} show stacking
Stack member summary
---------------------
Stacking enabled : No
Stacking active : No
Stack member state : Device Ready to Inspect - Normal
Stack master : No
```

The following example shows the output for the same device after adding it to a stack of three devices.

```
ips{} show stacking
Stack member summary
---------------------
Stacking enabled : Yes
Stacking active : Yes
Stack member state : Device Ready to Inspect - Normal
Stack master : No
```
Stack summary
-------------
Number of devices configured in stack : 3
Number of devices required in stack   : 2
Stack state                          : Stack Ready to Inspect - Normal
Device Hostname
----------------------------------------- --------------------------------
device01 (local host) Device Ready to Inspect - Normal
device02 (master) Device Ready to Inspect - Normal
device03 Device Ready to Inspect - Normal

Reference

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

show system connections

Syntax

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

ips{}show system connections ipv4
Active Internet connections (servers and established)

<table>
<thead>
<tr>
<th>vfid</th>
<th>Proto</th>
<th>Recv-Q</th>
<th>Send-Q</th>
<th>Local Address</th>
<th>Foreign Address</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>tcp</td>
<td>0</td>
<td>0</td>
<td>127.0.0.1:60000</td>
<td>0.0.0.0:*</td>
<td>LISTEN</td>
</tr>
<tr>
<td>0</td>
<td>tcp</td>
<td>0</td>
<td>0</td>
<td>127.0.0.1:616</td>
<td>0.0.0.0:*</td>
<td>LISTEN</td>
</tr>
</tbody>
</table>

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/nscl/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>LISTENING</td>
<td>16970</td>
<td>/tmp/.server.sockname</td>
</tr>
<tr>
<td>unix</td>
<td>2</td>
<td>[ ]</td>
<td>DGRAM</td>
<td>LISTENING</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]
b brief Brief process information
d detail Detailed process information
e extensive Extensive process information
s 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
show system queue-stats

Show internal queue statistics.

Syntax

deploy system queue-stats [fast-path]

show system statistics

Syntax

deploy system statistics [fast-path] [non-zero]

Example

deploy 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 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>

Virtual Segment ID | In Interface | Out Interface
segment6 (A > B)   | unknown      | unknown

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>

Virtual Segment ID | In Interface | Out Interface
segment6 (A > B)   | unknown      | unknown

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>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Server IP</th>
<th>Port</th>
<th>Interface</th>
<th>Proto</th>
<th>Cipher</th>
</tr>
</thead>
<tbody>
<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**

```
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.

```
ips{}show tse connection-table blocks
```

**Second device**

```
ips{}show tse connection-table blocks
```

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

show user-disk

**Syntax**

```
show user-disk
```

**Example**

```
ips{}show user-disk
```

**External User Disk**

- **Status:** Mounted
- **Encryption:** None
- **Capacity:** 3952263168 bytes
- **Used:** 784158720 bytes
- **Free:** 2907357184 bytes

show users

**Syntax**

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

ips{}show users

<table>
<thead>
<tr>
<th>USER</th>
<th>IDLE</th>
<th>INTERFACE</th>
<th>LOGIN</th>
<th>IPADDRESS</th>
<th>TYPE</th>
</tr>
</thead>
<tbody>
<tr>
<td>myadminuser</td>
<td>00:00</td>
<td>SSH</td>
<td>2013-07-19 23:42:56</td>
<td>198.51.100.139</td>
<td>LOCAL</td>
</tr>
</tbody>
</table>

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 67

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>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Version Model</th>
<th>Restore</th>
</tr>
</thead>
<tbody>
<tr>
<td>440T</td>
<td>Yes</td>
</tr>
</tbody>
</table>

snapshot remove

Syntax

```
snapshot remove
```

Example

```
ips{}snapshot remove s_041713
```
Success

snapshot restore

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

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

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

When restoring a snapshot, keep in mind:

- The contents of the system keystore are not included in the snapshot. When you restore a snapshot to a different device, you should plan to also import any private key information from the device where the snapshot was taken.
- When you want to restore a snapshot to a different device, and URL Reputation Filtering is enabled, a full synchronization of the Reputation database is required after you restore the snapshot. The snapshot does not include the ThreatDV URL Reputation Feed and User-defined URL Entries database. For more information, see the SMS User Guide.
- The snapshot includes the license package. The license package provides license information for each of your TippingPoint devices. If the license package that was included in the snapshot is outdated, restore the snapshot and then download and install an updated license package from the TMC.
- If an external ZPHA was configured on the original device, be sure to add an external ZPHA to the target device or update the device configuration to remove ZPHA.

Syntax

snapshot restore NAME

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

**Example**

ips{}tcpdump mgmt count 2
ips{}tcpdump bridge0 record mycapturefile count 100 proto tcp without udp pcap "dst port 443" background
ips{}tcpdump6: listening on bridge0, link-type EN10MB (Ethernet), capture size 65535 bytes
100 packets captured
100 packets received by filter
0 packets dropped by kernel
ips{}tcpdump stop
All tcpdump processes stopped.

tech-support-report

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

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

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

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

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

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

**Syntax**

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

**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:X [from X: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 external user disk (CFast or SSD).
After you mount the user disk, the device can automatically mount the disk when you reboot the device.

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

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

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

**Syntax**

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

**Example**

Unmount the external user disk.

```plaintext
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.

```plaintext
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 external user disk.

```plaintext
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 user 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 75

*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%
```
email

Allows you to set logging email daemon parameters.

**Syntax**

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

**Example**

```plaintext
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.

**Syntax**

```plaintext
log-file-size FILE_NAME USAGE[%]
log-file-size (audit|ipsAlert|ipsBlock|quarantine|reputationAlert|
reputationBlock|system|visibility) USAGE[%]
```

**Example**

```plaintext
log-file-size system 50%
log-file-size audit 50%
#
# Total 100%
```
Threat Protection System Command Line Interface Reference

log-storage

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

Syntax

log-storage external USAGE[%]
log-storage ramdisk USAGE[%]
log-storage externalReserve RESERVESIZE [MB]

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 86
- Contexts and related commands on page 101

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 101

actionsets

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

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

autodv

Enters Auto Digital Vaccine context mode.

Syntax

autodv

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
ddebug

display item
delete interface
Displays file or configuration item.

delete
Deletes file or configuration item.

Syntax
delete interface

display
Displays file or configuration item.
Syntax

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

dns
Enters DNS context mode.

Syntax
dns

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

```plaintext
ips{running}gen
generates{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
  lsm            Enable of disable lsm
  sms-allowed-ip Configure allowed SMS IP address
  ssh            Enable or disable ssh service
  timezone       Display or configure time zone
  tls            Enable or disable TLS (Transport Layer Security) versions
```
**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.

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

**Syntax**

Configure network interface 1A in slot 3.

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

Configure the management interface.

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

**Example**

```
ips{running-3-1A}
Valid entries at this position are:
   delete       Delete file or configuration item
   help         Display help information
   ipaddress    Configure endpoint IP address
   physical-media Configure ethernet port settings
   restart      Restart Ethernet port
```
**shutdown**

**Shutdown logical interface state**

**physical-media settings**

Valid entries are:

- 10half – Supported port speed and mode
- 10full – Supported port speed and mode
- 100half – Supported port speed and mode
- 100full – Supported port speed and mode
- auto-neg – Enable auto-negotiation (default is on)

**Line speed**

The line speed setting for a port.

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

**Duplex setting**

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

**Auto negotiation**

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

**ips**

Enters IPS profile context mode.

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

**Syntax**

```
ips
```

**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
```
### 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
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**

```plaintext
ntp
```

**Example**

```plaintext
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**

```plaintext
reputation
```

**Example**

```plaintext
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:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>delete</td>
<td>Delete file or configuration item</td>
</tr>
<tr>
<td>display</td>
<td>Display all reputation profiles and groups</td>
</tr>
<tr>
<td>group</td>
<td>Create/enter reputation group context</td>
</tr>
<tr>
<td>help</td>
<td>Display help information</td>
</tr>
<tr>
<td>nxdomain-response</td>
<td>NXDOMAIN response handling for DNS queries</td>
</tr>
<tr>
<td>profile</td>
<td>Create/enter reputation profile context</td>
</tr>
<tr>
<td>rename</td>
<td>Rename a reputation profile or group</td>
</tr>
</tbody>
</table>

**security-policy-reset**

Resets IPS security policy to the default values.

**Syntax**

security-policy-reset

**Example**

```bash
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**

```bash
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
  - sflow disable
  - sflow enable [SAMPLE-RATE]
  - sflow sample-rate SAMPLE-RATE
# 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 Intrinsc HA Layer 2 Fallback action
link-down Link down synchronization mode
restart Restart both Ethernet ports of segment
sflow Configure sFlow packet export

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

sflow

Enter sFlow® global configuration context mode.

sflow

Example

ips{running}sflow
ips{running-sflow}help
Valid commands are:
collector [pos N] IPADDR [PORT]
delete collector all
delete collector pos N
delete collector [pos N] IPADDR [PORT]
disable
enable
help [full|COMMAND]
ips{running-sflow}?
Valid entries at this position are:
collector          Adds or select an sFlow collector
delete collector   Delete file or configure item
disable            Disable service or configuration on item
enable             Enable service or configuration on item
help               Display help information

**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 authype AUTHTYPE AUTHPASS [inform]
  trapdest HOST [port PORT] ver 3 USERNAME authype AUTHTYPE AUTHPASS privproto PRIVPROTO [PRIVPASS] [inform]
  username USERNAME
  username USERNAME authype AUTHTYPE AUTHPASS
  username USERNAME authype AUTHTYPE AUTHPASS privproto 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
  engineID                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

<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-traffic-management}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:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>delete</td>
<td>Delete file or configuration item</td>
</tr>
<tr>
<td>display</td>
<td>Display traffic-management profiles context</td>
</tr>
<tr>
<td>help</td>
<td>Display help information</td>
</tr>
<tr>
<td>profile</td>
<td>Create/enter traffic-management profile context</td>
</tr>
<tr>
<td>rename</td>
<td>Rename traffic-management profile</td>
</tr>
</tbody>
</table>

**virtual-segments**

Enters virtual-segments context.

**Syntax**

```plaintext
toolkit> 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 tacacs-group (TACACSNAME|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
ips{running-aaa}delete radius-group group1
ips{running-aaa}delete role myrole1
```
ips{running-aaa}delete tacacs-group group1
ips{running-aaa}delete user myuser1
ips{running-aaa}delete user-group group1

ips{running-aaa}display

Display configuration.

Syntax

<table>
<thead>
<tr>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>display ldap-group LDAPGROUP [xml]</td>
</tr>
<tr>
<td>display ldap-schema LDAPSCHEMA [xml]</td>
</tr>
<tr>
<td>display login-settings [xml]</td>
</tr>
<tr>
<td>display password-settings [xml]</td>
</tr>
<tr>
<td>display radius-group RADIUSGROUP [xml]</td>
</tr>
<tr>
<td>display remote-login-group [xml]</td>
</tr>
<tr>
<td>display role USER [xml]</td>
</tr>
<tr>
<td>display tacacs-group [xml]</td>
</tr>
<tr>
<td>display user USER [xml]</td>
</tr>
<tr>
<td>display usergroup USERGROUP [xml]</td>
</tr>
</tbody>
</table>

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 tacacs-group group1
ips{running-aaa}display user myuser1
ips{running-aaa}display usergroup group1

ips{running-aaa}disable-inactive-users

Disable users who are inactive for 35 days.

Syntax

<table>
<thead>
<tr>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>disable-inactive-users</td>
</tr>
</tbody>
</table>

Example

ips{running-aaa}disable-inactive-users

ips{running-aaa}ldap-group

Configure LDAP group. Maximum number of groups is two.

Syntax

<table>
<thead>
<tr>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>ldap-group LDAPNAME</td>
</tr>
</tbody>
</table>

ips{running-aaa}ldap-group LDAPNAME

Example

```plaintext
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

```plaintext
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

```plaintext
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

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

Example of help for login settings

```plaintext
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      lockout-period
audit               Notify in audit log each failed login exceeding
maximum-attempts    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}login-banner

Configure login banner settings, including title and banner text.

Syntax

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

Example

ips{running-aaa}login-banner enable
ips{running-aaa}login-banner text
ips{running-aaa}login-banner title

ips{running-aaa}password

Configure password settings.

Syntax

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

Example

ips{running-aaa}password quality maximum
ips{running-aaa}password expiry-time 30d
ips{running-aaa}password expiry-action force-change
ips{running-aaa}password disallow-reuse enable
ips{running-aaa}password min-lifetime enable

ips{running-aaa}radius-group

Configure Radius group. Maximum number of radius groups is 2.
Syntax
radius-group RADIUSNAME

Example
ips{running-aaa}radius-group group1

ips{running-aaa}re-auth
Configure re-authentication settings. When this command is enabled, the CLI will force users to log out on any authentication changes.

Syntax
re-auth (enable|disable)

Example
ips{running-aaa}re-auth enable

ips{running-aaa}remote-login-group
Configure LDAP, RADIUS group, or TACACS+ group to use for administrative login.
The name you provide for each group cannot be changed. To give a group a new name, you must delete the group and re-create it with the new name.

**Note:** Both RADIUS and TACACS+ authentication use protocols that are not FIPS-compliant. Before configuring RADIUS or TACACS+ for remote authentication, disable FIPS mode. For more information, see `fips-mode-enable` on page 33.

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

Example
ips{running-aaa}remote-login-group administrator group1

ips{running-aaa}role
Configure an access role.

Syntax
role ROLE [OLDROLE]

Example
ips{running-aaa}role myrole1
ips{running-aaa}tacacs-group

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

Syntax

tacacs-group TACACSNAME

Example

ips{running-aaa}tacacs-group group1
ips{running-aaa-tacacs-group-group1}

Valid entries at this position are:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>auth-type</td>
<td>Configure TACACS+ server group authentication protocol</td>
</tr>
<tr>
<td>default-usergroup</td>
<td>default usergroup</td>
</tr>
<tr>
<td>delete</td>
<td>Delete file or configuration item</td>
</tr>
<tr>
<td>display</td>
<td>Display TACACS+ server's information</td>
</tr>
<tr>
<td>help</td>
<td>Display help information</td>
</tr>
<tr>
<td>retries</td>
<td>Configure server(s) retries</td>
</tr>
<tr>
<td>server</td>
<td>Configure server</td>
</tr>
</tbody>
</table>

ips{running-aaa}user

Configure a name identified user.

Syntax

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

ddebug 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

ddebug aaa 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>
</tbody>
</table>
### Option

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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:

```plaintext
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

ips{debug aaa ldap lookup-user admin user1} Debugging LDAP lookup for 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.

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

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><code>ips{running-certificates}ca-certificate</code> on page 123</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-aaa-tacacs-group-X Context Commands

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

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

Syntax

auth-type ASCII|PAP|CHAP

Example

ips{running-aaa}tacacs-group group1
ips{running-aaa-tacacs-group-group1}auth-type ?
Valid entries at this position are:
  ASCII Authenticate using ASCII Authentication
  PAP Authenticate using Password Authentication Protocol (PAP)
  CHAP Authenticate using Challenge-Handshake Authentication Protocol (CHAP)
ips{running-aaa-tacacs-group-group1}auth-type CHAP

Related commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ips{running-certificates}ca-certificate</td>
<td>Import a CA certificate.</td>
</tr>
</tbody>
</table>

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

Default usergroup. The default is operator.

Syntax

default-usergroup GROUP

Example

ips{running-aaa}tacacs-group group1
ips{running-aaa-tacacs-group-group1}default-usergroup ?
Valid entry at this position is:
  GROUP Group name
ips{running-aaa-tacacs-group-group1}default-usergroup administrator

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

Delete file or configuration item.
Syntax

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

Example

```plaintext
ips{running-aaa-tacacs-group-group1}delete server 123.456.7.8
```

```plaintext
ips{running-aaa-tacacs-group-group1}retries
```

Configure server retries.

Syntax

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

Example

```plaintext
ips{running-aaa-tacacs-group-group1}retries 3
```

```plaintext
ips{running-aaa-tacacs-group-group1}server
```

Configure TACACS+ server.

Syntax

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

Example

```plaintext
ips{running-aaa-tacacs-group-group1}server 123.456.7.8 1812 secret mysecret priority 1 timeout 12
ips{running-aaa-tacacs-group-group1}server 123.456.8.9 1812 secret mynewsecret priority 2 timeout 7
```

**running-actionsets Context Commands**

Immediate Commit Feature. Changes take effect immediately.

```plaintext
ips{running-actionsets}actionset
```

Enter an action set context with defined name.

Syntax

```plaintext
actionset ACTIONSETNAME
```

Example

```plaintext
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**

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

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

Add IP for limit quarantine.

**Syntax**

```plaintext
limit-quarantine SOURCEIP
```

**Example**

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

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

Configure packet trace option.

**Syntax**

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

**Example**

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

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

Set packet trace priority.

**Syntax**

```plaintext
priority PRIORITY
```

**Example**

```plaintext
ips{running-actionsets-myactionset1}priority medium
```

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

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

**Syntax**

```plaintext
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 TPS requires both the certificate and private key from your web server.

(Best Practice) Name the certificate so that you can safely and reliably assign it to the correct SSL server. When the keystore mode is **sms-managed**, use the SMS to manage device certificates and private keys.

**Syntax**

`certificate CERTNAME`
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 124</td>
<td>Import the private key from your web server into the local keystore on the TPS device.</td>
</tr>
<tr>
<td><code>ips{running-sslinsp}server</code> on page 165</td>
<td>Add an SSL server to the TPS device with the same security settings as your web server, and assign the corresponding certificate and private key.</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):
  -----BEGIN CERTIFICATE-----
  SoIDQTCAqoCCQDiEcSvKsrhKTANBgkqhkiG9w0BAQQFADBMQswCQYDVQQGEwJB
  VTEtmBEGA1UECMBMK29tZ21TdGF0ZTEhMB8GA1UEChMYSW50ZXJuZXQgV2lkZ2l0
  cyQgV21kZ210cyQgTHeRkMB4XDTA5MDQxNjE3MDUxNloDTA5MDUxNjE3MDUxNlowbDEQMA4G
  A1UEBhMHVW5rzbm93bjEQMA4GA1UECBMHVW5rzbm93bjEQMA4GA1UEBxMHW5rzbm93
  bjEQMA4GA1UEChMHW5rzbm93bjEQMA4GA1UEfxxMHW5rber93bjEQMA4GA1UEAxMH
  VW5rzbm93bjCCAbcwqgEsBgcqhkjOQAQBMIIBHwKBgQD9fLOBHxUSKVLfsPwu7OTn
  9hG3UjzvRADDHj+Ap1EmaUVdQCJR+1k9jVj6v8X1ujD2y5tVbNeB04AdNG/yZmC3
```
ips{running-certificates}delete

Delete file or configuration item.

Syntax

delete ca-certificate (all|CANAME)

Example

ips{running-certificates}delete ca-certificate myCAname

ips{running-certificates}display

Display file or configuration item.

Syntax

display ca-certificate CANAME [pem|text]

Example

ips{running-certificates}display
# CERTIFICATE AUTHORITIES
certificate myCAname
-----BEGIN CERTIFICATE-----
SoIDQTCCAqoCCQDiEcSvKsrhKTANBgkqhkiG9w0BAQQFADBFMQswCQYDVQQGEwJB
...
PISrOjgU6A2+VTbkZTJB32/Zng/hTDUQUkyyj11skdmafS1b9SSs0Z7SpLu6VDB
zR6PBzoFwaWk3nX21Ysk/gPpf07z
-----END CERTIFICATE-----

ips{running-certificates}private-key

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

To inspect secure sessions, the TPS requires both the certificate and private key from your web server.
When the keystore mode is **sms-managed**, this command is not applicable. Use the SMS to manage device certificates and private keys.

**Syntax**

```
private-key CERTNAME
```

**Example**

Import the private key from your web server into the keystore 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><code>ips{running-certificates}certificate</code> on page 122</td>
<td>Import the certificate from your web server into the local keystore on the TPS device.</td>
</tr>
<tr>
<td><code>ips{running-sslinsp}server</code> on page 165</td>
<td>Add an SSL server to the TPS device with the same security settings as your web server, and assign the corresponding certificate and private key.</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

delete domain-name
delete domain-search (primary|secondary|tertiary|all)
delete name-server (all|A.B.C.D|X:X::X:X)
delete 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

delete proxy cache cleaning interval
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

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

domain-search primary example.com
domain-search secondary example.org
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

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 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

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 129 for more information.

**Syntax**

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

**Example**

```plaintext
ips{running-gen}https enable
```

**ips{running-gen}lsm**

Disable and enable the LSM.

**Syntax**

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

**Example**

```plaintext
ips{running-gen}lsm enable
```

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

Configure allowed SMS IP addresses.

**Syntax**

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

**Example**

```plaintext
ips{running-gen}sms-allowed-ip 192.168.1.1
```

**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 128 for more information.

**Syntax**

```plaintext
ssh (enable|disable)
```
Example

```
ips{running-gen}ssh enable
```

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
```

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
```

**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
```

Enables high-availability on the local device.

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

Syntax

crypt

Example

The following example enables HA on the local device.

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

Applies encryption hash for a passphrase.

Syntax

crypt (passphrase PASPHRASE)|enable|disable

Example

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

Specifies the serial number of the HA partner.

Syntax

crypt 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 TPS devices without inspection. You can view a list of current inspection bypass rules with the display command.
Important: When creating an inspection bypass rule that includes source and destination ports or IP addresses, you must first specify the IP protocol as UDP or TCP.

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

<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>256 when bypassing IPv4 traffic, 128 for IPv6 traffic</td>
</tr>
</tbody>
</table>
| 2200T | 2560 when bypassing IPv4 traffic  
1280 when bypassing IPv6 traffic |
| 8200TX| 512 when bypassing IPv4 or IPv6 traffic                  |
| 8400TX| 512 when bypassing IPv4 or IPv6 traffic                  |

Syntax

Type `help` and press Enter for more information.
ips{running-inspection-bypass}help
Valid commands are:
  delete RULENAME
  help [full|COMMAND]
  rule NEWRULENAME
  rule RULENAME

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:
  action bypass
  action block
  action redirect PORTNAME
  action ingress-mirror PORTNAME
  action egress-mirror PORTNAME
  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:
**Syntax**

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

**Examples**

To list the available actions for the rule to apply on incoming traffic:

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

<table>
<thead>
<tr>
<th>action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>block</td>
<td>A rule match causes the packet to be blocked</td>
</tr>
<tr>
<td>bypass</td>
<td>A rule match causes the packet to bypass inspection (this is the default)</td>
</tr>
<tr>
<td>egress-mirror</td>
<td>A rule match causes the packet to be mirrored at egress to the specified port</td>
</tr>
<tr>
<td>ingress-mirror</td>
<td>A rule match causes the packet to be mirrored at ingress to the specified port</td>
</tr>
<tr>
<td>redirect</td>
<td>A rule match causes the packet to be redirected to the specified port</td>
</tr>
</tbody>
</table>

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

To block incoming traffic:

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

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

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

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

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

**Note:** A full list of Ethernet Type values can be found at the Internet Assigned Numbers Authority website. 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.

```
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.

```
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
Specify 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.

**Note:** A full list of IP protocol values can be found at the Internet Assigned Numbers Authority website at [http://www.iana.org/assignments/protocol-numbers](http://www.iana.org/assignments/protocol-numbers).

**Syntax**

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

```
ips{running-inspection-bypass-rule-myrule1}help ip-proto
Enter ip protocol for inspection bypass rule
Syntax: ip-proto PROTO_OPTION|PROTO_VALUE
    ip-proto       Enter ip protocol for inspection bypass rule
    PROTO_OPTION   Enter ip protocol (udp or tcp) for inspection bypass rule
    Possible values for PROTO_OPTION are:
        udp         udp protocol
```
**Example**

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

```plaintext
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.

```plaintext
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**

interface nM

Valid entries at this position are:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>delete</td>
<td>Delete file or configuration item</td>
</tr>
<tr>
<td>help</td>
<td>Display help information</td>
</tr>
<tr>
<td>physical-media</td>
<td>Configure ethernet port settings</td>
</tr>
<tr>
<td>restart</td>
<td>Restart Ethernet port</td>
</tr>
<tr>
<td>shutdown</td>
<td>Shutdown logical interface state</td>
</tr>
</tbody>
</table>

**Example**

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

ips{running}interface mgmt

Enters context for configuring management settings.

**Syntax**

interface mgmt

Valid entries at this position are:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>delete</td>
<td>Delete file or configuration item</td>
</tr>
<tr>
<td>description</td>
<td>Enter description for the management interface</td>
</tr>
<tr>
<td>help</td>
<td>Display help information</td>
</tr>
<tr>
<td>host</td>
<td>Configure host name, location, or contact</td>
</tr>
<tr>
<td>ip-filter</td>
<td>Limit which IP addresses can access mgmt port</td>
</tr>
<tr>
<td>ipaddress</td>
<td>Configure IP address</td>
</tr>
<tr>
<td>physical-media</td>
<td>Configure mgmt port speed/duplex</td>
</tr>
<tr>
<td>route</td>
<td>Add IPv4/IPv6 static route</td>
</tr>
</tbody>
</table>

**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
  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
```

**Example**

```
connection-table connection-table timeout type
```
Possible values for TIMEOUTTYPE are:

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>non-tcp-timeout</td>
<td>Connection table non-tcp timeout</td>
</tr>
<tr>
<td>timeout</td>
<td>Connection table timeout</td>
</tr>
<tr>
<td>trust-timeout</td>
<td>Connection table trust timeout</td>
</tr>
<tr>
<td>SECONDS</td>
<td>Connection table timeout seconds</td>
</tr>
</tbody>
</table>

**Example**

```bash
display
```

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

**Example**

```bash
delete
```

```
ips{running-ips}delete profile myprofile
```

**Example**

```bash
deployment
```

```
ips{running-ips}deployment-choices
```

**Syntax**

```
delete profile XPROFILENAME
```

**Example**

```bash
ips{running-ips}deployment-choices
```

**Syntax**

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

**Example**

```bash
deployement-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>

**Example**

```bash
ips{running-ips}display
```

**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 "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-nr 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. If a flow does not have HTTP traffic, HTTP processing stops so that optimum performance is maintained.

**Syntax**

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

ips{running-ips}profile

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

**Syntax**

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

**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.

```plaintext
ips{running-ips-1}categoryrule
Enters categoryrule context.
```

**Syntax**

```plaintext
categoryrule
```

**Example**

```plaintext
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
event Display help information
ips{running-ips-1-categoryrule}display
categoryrule
category "Network Equipment" enabled actionset "Recommended"
category "IM" enabled actionset "Recommended"
category "Spyware" enabled actionset "Recommended"
category "Virus" enabled actionset "Recommended"
category "Identity Theft" enabled actionset "Recommended"
category "Streaming Media" enabled actionset "Recommended"
category "Security Policy" enabled actionset "Recommended"
category "Reconnaissance" enabled actionset "Recommended"
category "Exploits" enabled actionset "Recommended"
category "Vulnerabilities" enabled actionset "Recommended"
category "P2P" enabled actionset "Recommended"
category "Traffic Normalization" enabled actionset "Recommended"
exit
```

```plaintext
ips{running-ips-1}delete
Delete file or configuration item.
```

**Syntax**

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

**Example**

```plaintext
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:
ips{running-log}log

Add log to a log session.

**Syntax**

```plaintext
log audit CONTACT-NAME [ALL|none]
log quarantine CONTACT-NAME [ALL|none]
log system CONTACT-NAME [SEVERITY]
```

Valid entries at this position are:

<table>
<thead>
<tr>
<th>Entry</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;Enter&gt;</td>
<td>Execute command</td>
</tr>
<tr>
<td>audit</td>
<td>Configure log for audit services</td>
</tr>
<tr>
<td>quarantine</td>
<td>Configure log for quarantine services</td>
</tr>
<tr>
<td>system</td>
<td>Configure log for all services</td>
</tr>
</tbody>
</table>

**Example**

```plaintext
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**

```plaintext
log-option xmsd( all)|( LOG_OPTION)
```

Possible values for LOG_OPTION are:

<table>
<thead>
<tr>
<th>Entry</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>segments</td>
<td>Enable logging segments</td>
</tr>
<tr>
<td>mgmt</td>
<td>Enable logging mgmt</td>
</tr>
<tr>
<td>interface</td>
<td>Enable logging interface</td>
</tr>
<tr>
<td>xms_configure</td>
<td>Enable logging xms configure</td>
</tr>
<tr>
<td>xms_process</td>
<td>Enable logging xms process</td>
</tr>
<tr>
<td>xms_stream</td>
<td>Enable logging xms stream</td>
</tr>
<tr>
<td>aaa</td>
<td>Enable logging aaa</td>
</tr>
<tr>
<td>dns</td>
<td>Enable logging dns</td>
</tr>
<tr>
<td>ethernet</td>
<td>Enable logging ethernet</td>
</tr>
<tr>
<td>highavailability</td>
<td>Enable logging highavailability</td>
</tr>
<tr>
<td>linkmonitor</td>
<td>Enable logging linkmonitor</td>
</tr>
<tr>
<td>log</td>
<td>Enable logging log</td>
</tr>
<tr>
<td>ntp</td>
<td>Enable logging ntp</td>
</tr>
<tr>
<td>ports</td>
<td>Enable logging ports</td>
</tr>
<tr>
<td>services</td>
<td>Enable logging services</td>
</tr>
<tr>
<td>udm-conf-handler</td>
<td>Enable logging UDM configuration handler</td>
</tr>
<tr>
<td>snmp</td>
<td>Enable logging snmp</td>
</tr>
<tr>
<td>system</td>
<td>Enable logging system</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>--------------------------------------</td>
</tr>
<tr>
<td>qos</td>
<td>Enable logging qos</td>
</tr>
<tr>
<td>virtual-segments</td>
<td>Enable logging virtual-segments</td>
</tr>
<tr>
<td>xmsupdate</td>
<td>Enable logging xmsupdate</td>
</tr>
<tr>
<td>vrf</td>
<td>Enable logging vrf</td>
</tr>
<tr>
<td>x509</td>
<td>Enable logging x509</td>
</tr>
<tr>
<td>xipc</td>
<td>Enable logging xipc requests</td>
</tr>
<tr>
<td>trafficlights</td>
<td>Enable logging trafficlights requests</td>
</tr>
<tr>
<td>vlan-translations</td>
<td>Enable logging vlan-translations</td>
</tr>
</tbody>
</table>

**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**

```plaintext
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]
```

- **SUBSYSTEM**: System to set logging level for
- **SEVERITY**: Level of severity for logging

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

```command
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**

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

**Example**

```command
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**

```command
delete contact XCONTACTNAME
delete EMAILSETTING
```

**Example**

```command
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**

```command
e-mail-from-address EMAIL
```

**Example**

```command
ips{running-notifycontacts}email-from-address someone@example.com
```
ips{running-notifycontacts}email-from-domain

From domain name.

**Syntax**

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

**Example**

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

ips{running-notifycontacts}email-server

Set mail server IP.

**Syntax**

```
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 XPROFILENAME
```

Valid entries:

- **group** Reputation group
- **profile** Delete reputation profile

**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: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

\texttt{domain NEWDOMAIN}

Example

\texttt{ips\{running-rep-1\}domain example.com}

ips{running-rep-1}ip

Syntax

\texttt{ip IPADDRESS}

Example

\texttt{ips\{running-rep-1\}ip 123.45.67.890}

\textbf{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

\texttt{action-when-pending (permit|drop)}

ips{running-rep-abc}check-destination-address
Enables or disables check destination address.

Syntax

\texttt{check-destination-address (enable|disable)}

Example

\texttt{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)
(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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ips{running-services-myservice1}delete icmp any</td>
<td>delete an icmp service</td>
</tr>
<tr>
<td>ips{running-services-myservice1}delete icmpv6 any</td>
<td>delete an icmpv6 service</td>
</tr>
<tr>
<td>ips{running-services-myservice1}delete port udp 53</td>
<td>delete a UDP port</td>
</tr>
<tr>
<td>ips{running-services-myservice1}delete port tcp all</td>
<td>delete a TCP port</td>
</tr>
<tr>
<td>ips{running-services-myservice1}delete protocol 6</td>
<td>delete a protocol</td>
</tr>
<tr>
<td>ips{running-services-myservice1}delete service http</td>
<td>delete a service</td>
</tr>
<tr>
<td>ips{running-services-myservice1}delete service dns</td>
<td>delete a service</td>
</tr>
</tbody>
</table>

**ips{running-services-myservice1}port**

Apply TCP or UDP port number.

**Syntax**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>port tcp PORT [to LASTPORT]</td>
<td>apply TCP port</td>
</tr>
<tr>
<td>port udp PORT [to LASTPORT]</td>
<td>apply UDP port</td>
</tr>
</tbody>
</table>

**Example**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ips{running-services-myservice1}port tcp 80 to 88</td>
<td>apply a TCP port range</td>
</tr>
</tbody>
</table>

**running-snmp Context Commands**

Immediate Commit Feature. Changes take effect immediately.

**ips{running-snmp}authtrap**

Enable or disable SNMP authentication failure trap.

**Syntax**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>authtrap (enable</td>
<td>disable)</td>
</tr>
</tbody>
</table>

**Example**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ips{running-snmp}authtrap enable</td>
<td>activate SNMP authentication failure trap</td>
</tr>
</tbody>
</table>

**ips{running-snmp}community**

Configure SNMP read-only community.

**Syntax**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>community COMMUNITY [SOURCE]</td>
<td>configure SNMP community</td>
</tr>
<tr>
<td><strong>COMMUNITY</strong></td>
<td>Text to identify SNMP system community</td>
</tr>
<tr>
<td><strong>SOURCE</strong></td>
<td>IP (A.B.C.D</td>
</tr>
<tr>
<td><strong>default</strong></td>
<td>allow any IPv4/6 source</td>
</tr>
</tbody>
</table>

**Example**

```plaintext
isps{running-snmp}community mycommunity default
```

```plaintext
isps{running-snmp}delete
```
Delete file or configuration item.

**Syntax**

```plaintext
delete community (COMMUNITY|all)
delete trapssession ((A.B.C.D|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**

```plaintext
isps{running-snmp}delete community mycommunity
isps{running-snmp}delete community all
isps{running-snmp}delete trapssession 192.168.1.1 ver 3
isps{running-snmp}delete trapssession all
```

```plaintext
isps{running-snmp}engineID
```
Configure SNMPv3 engine ID.

**Syntax**

```plaintext
engineID ENGINE-ID
```

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

**Example**

```plaintext
isps{running-snmp}engineID 0x800012ef0302a11aab33f4
```

```plaintext
isps{running-snmp}snmp
```
Enable or disable SNMP.

**Syntax**

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

**Example**

```plaintext
isps{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)
oAuthNoPriv 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

```
ips{running-snmp}trapdest snmpserver.example.com ver 2c mycommunity inform
ips{running-snmp}trapdest 192.168.1.1 port 162 ver 2c mycommunity
ips{running-snmp}trapdest 192.168.1.1 port 162 ver 3 mysnmpusername level
autNoPriv authtype SHA mysnmppassword inform
ips{running-snmp}trapdest 100:0:0:0:0:0:0:1 ver 3 mysnmpusername level
autNoPriv authtype SHA mysnmppassword inform
```

ips{running-snmp}username

Configure SNMPv3 USM read-only user.

Syntax

```
username USERNAME
```

---

**Threat Protection System Command Line Interface Reference**  161
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

ips{running-snmp}username mysnmpusername level noAuthNoPriv
ips{running-snmp}username mysnmpusername level authNoPriv authtype SHA
mySNMPPassword
ips{running-snmp}username mysnmpusername level authPriv authtype SHA
mySNMPPassword 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.

Example

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

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
ips{running-sslinsp}enable

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

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

**Syntax**

```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 TPS device saves SSL inspection log information to the "Management Console" notification contact which is available for display from the LSM and is found in the `sslInspection.log` on the device.

**Important:** To generate SSL inspection log entries, enable logging on the SSL server for troubleshooting purposes only. By default, an SSL server does not generate logging information. See `ips{running-sslinsp}server` on page 165 for more information.

**Syntax**

```plaintext
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.

```plaintext
ips{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.

```
ips{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.

```
ips{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><code>ips{running-certificates}certificate</code> on page 122</td>
<td>Import the certificate from your web server into the local keystore on the device.</td>
</tr>
<tr>
<td><code>ips{running-certificates}private-key</code> on page 124</td>
<td>Import the private key from your web server into the local keystore on the device.</td>
</tr>
<tr>
<td><code>ips{running-vseg-VSEG_NAME}ssl-profile</code> on page 174</td>
<td>Update the virtual segment to assign the SSL inspection profile.</td>
</tr>
<tr>
<td><code>ips{running-sslinsp}server</code> on page 165</td>
<td>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.
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_SHA256
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.

```
ips{running-sslinsp-server-myserver}ip address 192.168.1.0/24
```
(Required) Specify the **device certificate** that the TPS device 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.

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

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

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

**Related commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ips{running-certificates}certificate</code> on page 122</td>
<td>Import the certificate from your web server into the local keystore on the device.</td>
</tr>
<tr>
<td><code>ips{running-certificates}private-key</code> on page 124</td>
<td>Import the private key from your web server into the local keystore on the device.</td>
</tr>
<tr>
<td><code>ips{running-vseg-VSEG_NAME}ssl-profile</code> on page 174</td>
<td>Update the virtual segment to assign the SSL inspection profile.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td><code>ips{running-sslinsp}profile</code></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-trafmgmt}profile
Create or enter traffic-management profile context. When traffic filters are added to a profile, more options become available.

**Syntax**

```
profile NEWTRAPPROFNAME
profile TRAPPROFNAME
```

**Examples**

```
ips{running-trafmgmt}profile MyTrafficProfile
ips{running-trafmgmt-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-trafmgmt-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-trafmgmt-MyTrafficProfile}traffic-filter MyTrafficFilter
ips{running-trafmgmt-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-trafmgmt-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]
  move 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 ICMPCODE]

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. Use this context to define an individual virtual segment.

Syntax

ips{running}virtual-segments
ips{running-vsegs}?

Valid entries at this position are:
delete Delete file or configuration item
**help**  
Display help information

**rename**  
Rename virtual-segment

**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.

**ips{running-vsegs}delete virtual-segment**

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

**Syntax**

```
delete virtual-segment VSEGNAME
```

**Example**

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

**ips{running-vsegs}display**

Display file or configuration item.

**Syntax**

```
display {xml}
```

**ips{running-vsegs}rename virtual-segment**

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

**Syntax**

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

**Example**

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

**ips{running-vsegs}virtual-segment**

Create or enter virtual-segment context.

**Syntax**

```
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-vsegs)virtual-segment segmentname
ips(running-vsegs-segmentname)?
```

Valid entries at this position are:

<table>
<thead>
<tr>
<th>Entry</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bind</td>
<td>Bind physical ports to virtual segment</td>
</tr>
<tr>
<td>delete</td>
<td>Delete file or configuration item</td>
</tr>
<tr>
<td>description</td>
<td>Update virtual segment description</td>
</tr>
<tr>
<td>display</td>
<td>Display file or configuration item</td>
</tr>
<tr>
<td>dst-address</td>
<td>Add destination address to a virtual segment</td>
</tr>
<tr>
<td>help</td>
<td>Display help information</td>
</tr>
<tr>
<td>ips-profile</td>
<td>Virtual segment ips profile</td>
</tr>
<tr>
<td>move</td>
<td>Move virtual segment priority position</td>
</tr>
<tr>
<td>reputation-profile</td>
<td>Virtual segment reputation profile</td>
</tr>
<tr>
<td>src-address</td>
<td>Add source address to a virtual segment</td>
</tr>
<tr>
<td>ssl-profile</td>
<td>Virtual segment SSL profile</td>
</tr>
<tr>
<td>traffic-profile</td>
<td>Virtual segment traffic-management profile</td>
</tr>
<tr>
<td>vlan-id</td>
<td>Add vlan id or range to virtual segment</td>
</tr>
</tbody>
</table>

Example

```
ips{}edit
ips(running)virtual-segments
ips(running-vsegs)virtual-segment myVseg
```

**Notes**

- A maximum of 64 virtual segments can be configured.
- Each virtual segment name must be unique.
- You can configure up to 4094 VLAN IDs per virtual segment.
- Each VLAN ID in a range counts individually. For example, `vlan-id range 1 5` counts as five IDs.
- A CIDR counts as a single address. For example, `192.168.1.0/24` counts as one address.
- At least one traffic criteria must be defined for each virtual segment. Traffic criteria can be VLAN IDs, src-addresses, and dst-addresses.
• If no physical ports are defined on a virtual segment, the virtual segment will apply to all physical ports.

• If no VLAN IDs are defined on a virtual segment, all VLAN IDs are included.

• If no source addresses are defined, all source addresses are included. If no destination addresses are defined, all destination addresses are included.

• Position values must remain contiguous across all defined virtual segments, so there should never be a gap in the sequence.

• Position values start with 1 and increment by one for each new virtual segment added. The highest possible position value that can be configured is 64.

ips{running-vsegs}bind
Bind physical ports to virtual-segment.

Syntax
bind in-port PHYSPORT out-port PHYSPORT

Example
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
delete bind in-port EXISTING_PHYSPORT out-port EXISTING_PHYSPORT

Example
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
description TEXT

Example
ips{running-vsegs}description "virtual segment for ips profile"
ips{running-vsegs}display
Display file or configuration item.

**Syntax**

display {xml}

isps{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>ips{running-sslinsp}profile</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 v1
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

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

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

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

ips{running-vsegs-vsegname}vlan-id

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

Syntax

vlan-id VLANID_NUMBER

vlan-id range MINADDR MAXADDR

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

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

Example

ips{running-vsegs-vsegname}vlan-id range 301 304

where vsegname is the name of the virtual segment for which the range is defined.
ips{running-vsegs}delete vlan-id

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

**Syntax**

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

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

**Example**

```
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**

```
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**

```
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:

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

Display the currently defined VLAN translations:

```
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:

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