TippingPoint™ Security Management System (SMS)
User Guide
Enterprise network security management system for centralized global vision and security policy control.
Legal and notice information

© Copyright 2017 Trend Micro Incorporated. All rights reserved. TippingPoint, the TippingPoint logo, and Digital Vaccine are trademarks or registered trademarks of Trend Micro Incorporated. TippingPoint Reg. U.S. Pat. & Tm. Off. All other company and/or product names may be trademarks of their respective owners.

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

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

Security Management System User Guide
# Contents

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

Target audience ...................................................................................................................................... 1

Related documentation ........................................................................................................................... 1

Conventions ............................................................................................................................................ 1

Product support ...................................................................................................................................... 2

**SMS Overview** ..................................................................................................................................... 3

Installation ............................................................................................................................................... 4

**SMS web management console** ........................................................................................................ 5

Desktop versus mobile experience – feature availability ........................................................................ 6

Log in to the SMS web management console ....................................................................................... 7

Install the SMS client ............................................................................................................................. 7

OS X prerequisites ............................................................................................................................... 8

Threat Insights ........................................................................................................................................ 9

Breached Hosts ..................................................................................................................................... 9

Attacked Vulnerable Hosts .................................................................................................................. 11

Suspicious Objects ............................................................................................................................. 13

ZDI Filter Hits ..................................................................................................................................... 15

Monitor all devices ................................................................................................................................ 16

Status conditions .................................................................................................................................. 17

Identify devices that require your attention ......................................................................................... 18

Switch a device into Layer-2 Fallback mode ...................................................................................... 19

View or download reports ................................................................................................................... 20

Download exports and archives from the SMS .................................................................................. 20
View system logs..................................................................................................................................20
Access tools and resources................................................................................................................. 21
Threat Insights and web management console FAQ...........................................................................21
SMS client .............................................................................................................................................. 24
Log in to the SMS client...................................................................................................................... 24
SMS client user interface ..................................................................................................................... 25
SMS features........................................................................................................................................27
Manage your system............................................................................................................................ 29
View notifications.................................................................................................................................. 29
Software updates.................................................................................................................................. 30
Tools ........................................................................................................................................................32
IP Lookup..............................................................................................................................................32
TMC...................................................................................................................................................... 33
ThreatLinQ............................................................................................................................................ 33
Diagnostics .......................................................................................................................................... 34
Create a logs zip file............................................................................................................................ 34
Edit logging levels............................................................................................................................... 35
Install a hotfix ..................................................................................................................................... 35
Roll back to a previous software hotfix............................................................................................... 36
Generate bookmark string.................................................................................................................... 36
Look up users on LDAP........................................................................................................................ 36
Configure, enable, and query IDResolver .............................................................................................36
Query IDResolver................................................................................................................................... 37
System preferences.............................................................................................................................. 38
Security................................................................................................................................................... 38
TMC Information Share........................................................................................................................................... 41
Device SNMP.......................................................................................................................................................... 42
Device Communication.......................................................................................................................................... 43
Dashboard............................................................................................................................................................. 44
SSH client configuration...................................................................................................................................... 45
Banner Message.................................................................................................................................................... 45
External Export.................................................................................................................................................... 46
Reports.................................................................................................................................................................... 47
Dashboard............................................................................................................................................................... 48
Dashboard palette.................................................................................................................................................. 48
Default dashboard configuration............................................................................................................................ 48
Dashboard gadgets................................................................................................................................................ 49
Health and Status gadgets.................................................................................................................................. 49
Task Status gadgets.............................................................................................................................................. 50
Inspection Event gadgets..................................................................................................................................... 51
Event Rate gadget.................................................................................................................................................. 51
Security gadgets.................................................................................................................................................... 51
Reputation gadgets............................................................................................................................................... 52
Application gadgets.............................................................................................................................................. 52
User gadgets.......................................................................................................................................................... 54
Firewall gadgets..................................................................................................................................................... 54
Customize the SMS dashboard.............................................................................................................................. 55
Select a dashboard theme..................................................................................................................................... 56
Change the dashboard layout................................................................................................................................. 56
Restore dashboard defaults................................................................................................................................ 56
Add or remove a gadget......................................................................................................................................... 56
URL Threat Analysis ............................................................................................................................ 89
Prerequisites ....................................................................................................................................... 90
Configure URL Threat Analysis ......................................................................................................... 91
URL Threat Analyzer results ............................................................................................................. 92
Reports ................................................................................................................................................... 96
Navigate the Reports workspace ......................................................................................................... 96
AD User reports .................................................................................................................................... 97
Inspection criteria panels ................................................................................................................... 97
Firewall templates .................................................................................................................................. 99
Firewall criteria panels ....................................................................................................................... 99
Reputation templates .......................................................................................................................... 101
Reputation criteria panels ................................................................................................................ 101
Rate Limit templates ........................................................................................................................... 103
Rate Limit criteria panels ................................................................................................................. 103
Device Traffic templates ..................................................................................................................... 104
Device Traffic criteria panels ........................................................................................................... 104
Advanced DDoS templates ................................................................................................................ 105
Advanced DDoS criteria panels ....................................................................................................... 106
Executive reports templates .............................................................................................................. 107
Executive report criteria panels ....................................................................................................... 107
Traffic Analysis templates ................................................................................................................... 109
Traffic Analysis criteria panels ....................................................................................................... 109
Run a report ....................................................................................................................................... 110
Run a report ..................................................................................................................................... 110
Clear filters ....................................................................................................................................... 112
Customize the criteria panels ............................................................................................................ 112
Change the criteria panels that display on a report.................................................................112

Customize a query..........................................................................................................................113

Create a custom query for a report.............................................................................................113

Report results................................................................................................................................113

Open a saved report.......................................................................................................................113

Edit result settings and permissions...........................................................................................114

Delete a saved report....................................................................................................................114

Export report results.......................................................................................................................114

Export a report result......................................................................................................................115

Report schedules...........................................................................................................................115

Create a new schedule..................................................................................................................115

Edit an existing schedule..............................................................................................................116

Delete a schedule..........................................................................................................................117

Templates.......................................................................................................................................117

Report permissions.........................................................................................................................117

Saved reports...............................................................................................................................117

Create a saved report....................................................................................................................118

Run a saved report.........................................................................................................................119

Edit a saved report.........................................................................................................................120

Save as a new report.......................................................................................................................120

All schedules................................................................................................................................120

Edit a report schedule....................................................................................................................121

Delete a report schedule.................................................................................................................121

Profiles..........................................................................................................................................122

Shared settings...............................................................................................................................123

Action sets....................................................................................................................................123

Create or edit an action set............................................................................................................124

Notification contacts.....................................................................................................................129
Set aggregation settings for global contacts ................................................................. 129
Create or edit an email notification contact ................................................................. 130
Create or edit an SNMP notification contact ............................................................... 130
Services ......................................................................................................................... 131
Add or edit a non-standard port for a service ......................................................... 131
SSL servers .................................................................................................................. 132
Add or edit an SSL server ......................................................................................... 132
Refresh certificate status ......................................................................................... 133
SSL Inspection policy ................................................................................................. 134
Inspection profiles ...................................................................................................... 135
New profiles ................................................................................................................ 136
Create a new profile ................................................................................................. 138
Use the ‘Save As’ option to copy a profile .............................................................. 138
View profile details and versions ........................................................................... 139
Edit profile details .................................................................................................... 140
Create a snapshot of a profile version .................................................................. 141
Activate a profile version ....................................................................................... 141
Distribute profiles ...................................................................................................... 142
Manual profile distribution ...................................................................................... 143
Cancel a distribution in progress ........................................................................... 143
Distribute multiple profiles ..................................................................................... 144
Distribute an inspection profile to inspection segments ..................................... 145
Compare profiles ...................................................................................................... 145
Import profiles ........................................................................................................... 146
Import a profile ......................................................................................................... 147
Export profiles ........................................................................................................... 148
Delete profiles ........................................................................................................... 149
Inspection profile filters ............................................................................................ 149
Profile overview ........................................................................................................ 150
Filter details......................................................................................................................................151
Adaptive filtering...............................................................................................................................152
Filter categories...............................................................................................................................152
Search.............................................................................................................................................. 157
   Find and view a filter.................................................................................................................... 158
   Search profile filters.................................................................................................................... 158
   View filter search results...............................................................................................................163
Editing filters.....................................................................................................................................166
   Edit category settings....................................................................................................................166
   Edit a filter.....................................................................................................................................166
   Edit multiple filters.........................................................................................................................167
   Create or edit a filter exception....................................................................................................168
   Remove a filter exception...............................................................................................................169
Security filters...................................................................................................................................169
   Security filter exceptions and restrictions.....................................................................................170
       Create or edit a security filter restriction..................................................................................170
       Create or edit a security filter exception..................................................................................171
Application filters..............................................................................................................................172
   Create or edit application filter restrictions...................................................................................172
Advanced DDoS...............................................................................................................................173
   Create or edit an Advanced DDoS filter....................................................................................... 173
Reputation filters..............................................................................................................................175
   Edit Reputation settings................................................................................................................176
   Create or edit a Reputation filter..................................................................................................176
   Edit a Reputation filter................................................................................................................177
   Change the precedence of a Reputation or Geographic filter (move up/down).........................177
   Delete a Reputation or Geographic filter....................................................................................178
   Create or edit Reputation filter exceptions..................................................................................178
   Create or edit domain name exceptions......................................................................................179
Reputation filters table..................................................................................................................179
Management tasks......................................................................................................................181
Auxiliary Digital Vaccine tasks.................................................................................................................. 200
Import Auxiliary DV packages.................................................................................................................. 200
Manage Auxiliary DV packages............................................................................................................. 200
Uninstall an Auxiliary DV....................................................................................................................... 201
Distribute Auxiliary DV packages........................................................................................................... 201
Clear an obsolete distribution listing for Auxiliary DVs......................................................................... 201
Digital Vaccine Toolkit Packages............................................................................................................. 201
Associate DV Toolkit packages with devices and profiles in the SMS.................................................. 202
Create DV Toolkit packages................................................................................................................... 203
Limit access to DV Toolkit packages.................................................................................................... 203
DV Toolkit Packages screen.................................................................................................................. 203
Import a DV Toolkit package................................................................................................................. 204
Activate a DV Toolkit package............................................................................................................... 205
Search for DV Toolkit filters.................................................................................................................. 205
View DV Toolkit filter numbers in the Search Results........................................................................... 207
Distribute a DV Toolkit package to the device....................................................................................... 207
View DV Toolkit details......................................................................................................................... 208
Remove DV Toolkit packages from the device and the SMS............................................................... 208
Deactivate a DV Toolkit package on the SMS....................................................................................... 208
Uninstall a DV Toolkit package from the device................................................................................... 209
Delete a DV Toolkit package from the SMS........................................................................................... 210
Reputation database............................................................................................................................... 210
Reputation database interface............................................................................................................... 210
Summary tab.......................................................................................................................................... 211
Database summary................................................................................................................................. 211
Activity tab............................................................................................................................................ 211
Sync progress........................................................................................................................................ 211
Tasks..................................................................................................................................................... 212
View Reputation database details for distribution to device targets.................................................... 212
Perform a full synchronization of the Reputation database................................................................. 213
Stop a synchronization of the Reputation database................................. 213
Clear obsolete distribution entries...................................................... 213

Tag Categories tab...................................................................................... 213
Import all tag categories........................................................................ 216
Export all tag categories.......................................................................... 216
Add or edit a Reputation tag category.................................................. 216
Delete a Reputation tag category.......................................................... 217

ThreatDV entries....................................................................................... 217
Import a ThreatDV package................................................................. 218
Reset a ThreatDV.................................................................................... 218

User entries............................................................................................... 219
Import entries into the Reputation database........................................ 219
Import user-provided entries to the Reputation database from a file...... 219
Adding user-provided entries to the Reputation database...................... 220
Add a user-provided entry (addresses and URLs only) to the Reputation Database.................................................. 220
Add an address, URL, tag category, or tag value to the Reputation database.......................................................... 221
Exporting user-provided Reputation entries......................................... 221
Export a user-provided entry from the Reputation Database................ 221

Geographic entries.................................................................................. 221

Reputation database search..................................................................... 222
Search criteria.......................................................................................... 222
Search results.......................................................................................... 223
Search for entries in the Reputation database...................................... 223
Edit bulk (all searched database entries).............................................. 224
Delete bulk (all searched database entries).......................................... 224
Edit a user provided entry in the Reputation database.......................... 225
Edit multiple user-provided entries in the Reputation database........... 225

ThreatDV URL Lookup........................................................................... 225

Scheduled distributions........................................................................... 226
Create a new profile distribution......................................................... 226
View a profile schedule.......................................................................... 226
Edit a profile schedule........................................................................... 226

Vulnerability Scans (eVR)....................................................................... 227
Import vulnerability scans (eVR) ................................................................. 228
Vulnerability scan (eVR) specifications ........................................................ 228
Comment on a vulnerability scan ................................................................. 229
Show CVEs for a selected vulnerability scan ............................................. 229
Search vulnerability scans for CVEs ......................................................... 230
View CVE search results ........................................................................... 231
View CVE details ...................................................................................... 233
Profile tuning ............................................................................................ 234
Delete vulnerability scans .......................................................................... 235

Firewall profiles ......................................................................................... 235
Security zones (Firewall only) .................................................................... 236
Create or edit a security zone ..................................................................... 236
Schedules (Firewall only) .......................................................................... 237
Create or edit a schedule ........................................................................... 237
Service groups (Firewall only) ................................................................. 238
Create or edit a service group ................................................................. 238
Application groups (Firewall only) .......................................................... 238
Create or edit an application group ......................................................... 238
Manage firewall profiles .......................................................................... 239
Import a firewall profile ........................................................................... 240
Create a new profile ................................................................................ 240
Create a snapshot of a firewall profile version ........................................ 241
Activate a firewall profile version .......................................................... 241
Delete a firewall profile .......................................................................... 241
Firewall rules ............................................................................................ 242
Add items to firewall rules ....................................................................... 242
Create firewall rules ................................................................................. 242
Captive portal rules ................................................................................ 245
Create a captive portal rule ..................................................................... 245
Special captive portal rules to allow blocked users to log out ................. 246
Web response action.................................................................................................................... 260
IPS quarantine response action....................................................................................................261
Delete a response action.............................................................................................................. 262

Policies................................................................................................................................................262
Policy setup options.........................................................................................................................263
Policy initiation............................................................................................................................... 263
Policy remediation communication (timeout)................................................................................ 263
Inclusions and exclusions............................................................................................................. 263
IP correlation and thresholding..................................................................................................... 264
Actions........................................................................................................................................... 264
IPS destinations.............................................................................................................................264
Default response policy................................................................................................................... 264
Edit the default response policy....................................................................................................265
Manual response..............................................................................................................................266
Initiate a manual response............................................................................................................266
New response policies.....................................................................................................................267
Create or edit a new response policy...........................................................................................267
Delete a new response policy.......................................................................................................269

Responder network devices........................................................................................................... 269
Auto discovery of switches..............................................................................................................269
Configure auto discovery of network devices............................................................................269
Adding a switch................................................................................................................................270
Add or edit a switch...................................................................................................................... 271

RADIUS...............................................................................................................................................272
Configure RADIUS.........................................................................................................................272

IP Correlation......................................................................................................................................272
Configuring IP Correlation...............................................................................................................273
Network mapping using the GUI...................................................................................................273
Add/edit network mapping............................................................................................................ 273
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edit port details</td>
<td>291</td>
</tr>
<tr>
<td>Resolve out-of-service mode</td>
<td>292</td>
</tr>
<tr>
<td>VLAN translation tab – TPS and IPS (N-Platform and NX-Platform)</td>
<td>292</td>
</tr>
<tr>
<td>Create/edit VLAN translation</td>
<td>292</td>
</tr>
<tr>
<td>NGFW network configuration and tasks</td>
<td>293</td>
</tr>
<tr>
<td>Interfaces tab (NGFW)</td>
<td>293</td>
</tr>
<tr>
<td>Segments tab (NGFW)</td>
<td>294</td>
</tr>
<tr>
<td>Ports tab (NGFW)</td>
<td>294</td>
</tr>
<tr>
<td>Anti-Spoofing Filters tab (NGFW)</td>
<td>294</td>
</tr>
<tr>
<td>Add an anti-spoofing filter</td>
<td>294</td>
</tr>
<tr>
<td>DNS/DHCP</td>
<td>295</td>
</tr>
<tr>
<td>ARP/NDP</td>
<td>295</td>
</tr>
<tr>
<td>Events summary</td>
<td>295</td>
</tr>
<tr>
<td>Blocked and rate limited streams</td>
<td>296</td>
</tr>
<tr>
<td>Firewall sessions</td>
<td>297</td>
</tr>
<tr>
<td>Trusted streams</td>
<td>297</td>
</tr>
<tr>
<td>Quarantined hosts</td>
<td>298</td>
</tr>
<tr>
<td>Adaptive filter</td>
<td>299</td>
</tr>
<tr>
<td>Events configuration – TPS and IPS (S-Series, N-Platform, NX-Platform)</td>
<td>300</td>
</tr>
<tr>
<td>Event monitoring</td>
<td>301</td>
</tr>
<tr>
<td>View realtime graph data</td>
<td>301</td>
</tr>
<tr>
<td>View log</td>
<td>301</td>
</tr>
<tr>
<td>Reset events/logs</td>
<td>301</td>
</tr>
<tr>
<td>System health</td>
<td>302</td>
</tr>
<tr>
<td>Health stats</td>
<td>303</td>
</tr>
<tr>
<td>Health thresholds</td>
<td>303</td>
</tr>
<tr>
<td>System health graphs</td>
<td>304</td>
</tr>
<tr>
<td>Performance</td>
<td>305</td>
</tr>
<tr>
<td>Performance data</td>
<td>305</td>
</tr>
<tr>
<td>Performance graphs</td>
<td>306</td>
</tr>
<tr>
<td>Tier Statistics tab</td>
<td>306</td>
</tr>
<tr>
<td>Port health</td>
<td>306</td>
</tr>
<tr>
<td>Port statistics</td>
<td>306</td>
</tr>
<tr>
<td>Traffic</td>
<td>307</td>
</tr>
<tr>
<td>Traffic graphs</td>
<td>307</td>
</tr>
<tr>
<td>System log</td>
<td>307</td>
</tr>
<tr>
<td>Device health event entries</td>
<td>308</td>
</tr>
<tr>
<td>Audit log</td>
<td>310</td>
</tr>
<tr>
<td>NGFW events</td>
<td>311</td>
</tr>
<tr>
<td>System health summary</td>
<td>311</td>
</tr>
</tbody>
</table>
Performance.................................................................................................................................. 312
Packet statistics.......................................................................................................................... 312
CPU.............................................................................................................................................313
Device users..................................................................................................................................313
Traffic capture............................................................................................................................ 315
Concurrent traffic capture.......................................................................................................... 315
Traffic capture configuration...................................................................................................... 318
Traffic capture expressions....................................................................................................... 320
Create a new traffic capture file.............................................................................................. 320
Export a traffic capture file.......................................................................................................321
Transfer traffic capture files to the SMS..................................................................................321
Device Details.............................................................................................................................321
Status indicators........................................................................................................................ 322
Status indicator legends............................................................................................................ 322
Device Configuration wizard................................................................................................... 324
System update and snapshots................................................................................................... 326
System snapshots..................................................................................................................... 326
Common device tasks............................................................................................................... 326
Adding, editing, or deleting a device........................................................................................ 327
Add a device............................................................................................................................. 328
Editing one or more devices.................................................................................................... 329
Delete a device......................................................................................................................... 330
Creating or deleting a device group........................................................................................ 330
Create a device group............................................................................................................ 330
Delete a device group............................................................................................................. 330
Unmanaging or remanaging a device..................................................................................... 330
Unmanage a Device................................................................................................................ 331
Manage a device..................................................................................................................... 331
Importing or exporting device configuration......................................................................... 331
Export device settings............................................................................................................. 332
Import device settings............................................................................................................. 332
Viewing and searching events............................................................................................... 332
View events for all devices.................................................................333
View events for a specific device........................................................334
Flush events lists...............................................................................334
Managing versions, updates, and snapshots........................................334
Rollback to a previous version..............................................................334
Delete a previous TOS version............................................................336
Create a new system snapshot on the device........................................336
Import a system snapshot from a file..................................................336
Export a system snapshot to a file......................................................336
Archive a system snapshot to the SMS...............................................337
Restore from a system snapshot..........................................................337
Delete a system snapshot....................................................................338
Importing and downloading the TOS...................................................338
Download the TOS software...............................................................339
Import TOS software from a file.........................................................339
Managing TOS distribution.................................................................340
Distribute the TOS.............................................................................340
Managing virtual segments..................................................................340
Create a virtual segment....................................................................340
Delete a virtual segment....................................................................341
Analyze traffic flow for virtual segments..............................................342
Managing segment groups.................................................................342
View segment group details...............................................................343
Import a device profile......................................................................343
Create a segment group.....................................................................343
Edit segment group membership.........................................................344
Edit the name and descriptions for a segment group member............345
Edit permissions for a segment group member....................................345
Distribution queue configuration – TPS and IPS (S-Series, N-Platform, and NX-Platform).........345
View distribution queues for a device..................................................346
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change or delete a distribution queue entry</td>
<td>346</td>
</tr>
<tr>
<td>Inspection Bypass configuration – TPS and IPS (N-Platform and NX-Platform)</td>
<td>347</td>
</tr>
<tr>
<td>Create or edit an inspection bypass rule</td>
<td>349</td>
</tr>
<tr>
<td>Editing device configurations</td>
<td>350</td>
</tr>
<tr>
<td>User activities</td>
<td>350</td>
</tr>
<tr>
<td>User access</td>
<td>350</td>
</tr>
<tr>
<td>Management information</td>
<td>350</td>
</tr>
<tr>
<td>Resetting IPS filters</td>
<td>353</td>
</tr>
<tr>
<td>Management network</td>
<td>353</td>
</tr>
<tr>
<td>Configure the management network – TPS and IPS (N-Platform and NX-Platform)</td>
<td>354</td>
</tr>
<tr>
<td>Editing the management port settings for the S-Series devices</td>
<td>355</td>
</tr>
<tr>
<td>Management routes</td>
<td>356</td>
</tr>
<tr>
<td>NAT</td>
<td>356</td>
</tr>
<tr>
<td>Configure NAT</td>
<td>356</td>
</tr>
<tr>
<td>Host IP filters</td>
<td>356</td>
</tr>
<tr>
<td>Services</td>
<td>356</td>
</tr>
<tr>
<td>Services</td>
<td>359</td>
</tr>
<tr>
<td>AFC settings</td>
<td>360</td>
</tr>
<tr>
<td>HA (High Availability)</td>
<td>361</td>
</tr>
<tr>
<td>Configure network HA</td>
<td>363</td>
</tr>
<tr>
<td>Enable and disable the bypass mode on an installed bypass module – TPS (TX Series) and IPS (NX-Platform)</td>
<td>364</td>
</tr>
<tr>
<td>Performance Protection</td>
<td>364</td>
</tr>
<tr>
<td>NMS</td>
<td>365</td>
</tr>
<tr>
<td>Configure NMS settings for IPS (SNMP v2)</td>
<td>365</td>
</tr>
<tr>
<td>Configure NMS for N-Platform or NX-Platform IPS (SNMP v3)</td>
<td>365</td>
</tr>
<tr>
<td>SNMP settings</td>
<td>366</td>
</tr>
<tr>
<td>Log Configuration</td>
<td>366</td>
</tr>
<tr>
<td>Data Security – vTPS and TPS</td>
<td>366</td>
</tr>
<tr>
<td>Remote syslog</td>
<td>367</td>
</tr>
</tbody>
</table>
Create/edit remote syslog servers .............................................................. 369
Servers ........................................................................................................... 370
Email server .................................................................................................. 370
Time settings ................................................................................................. 370
Configure the time options for TPS devices .................................................. 371
Configure the time options – IPS (N-Platform and NX-Platform) ................... 372
TSE settings ................................................................................................. 375
Authentication preferences ........................................................................... 377
Configure administrative login privileges ...................................................... 378
Remote authentication configuration ............................................................... 378
Specify one or more RADIUS groups and servers for TPS ......................... 378
Specify one or more LDAP groups and servers for TPS ............................... 380
Specify one or more TACACS+ groups and servers for TPS ....................... 382
Remote Authentication .................................................................................. 383
Specify one or more RADIUS servers for IPS ............................................ 384
Import an X509 certificate ............................................................................. 385
Specify one or more TACACS+ servers for IPS .......................................... 385
sFlow® .......................................................................................................... 386
Create sFlow® collector .................................................................................. 387
Device settings ............................................................................................. 388
Application visibility ...................................................................................... 389
FIPS settings ............................................................................................... 389
Enable FIPS on IPS device using SMS ........................................................ 390
Enable FIPS on TPS device using SMS ......................................................... 392
SSL Inspection .............................................................................................. 392
Packet trace – TPS and IPS (S-Series, N-Platform, and NX-Platform) ........ 393
Save all packet trace information for a device ................................................. 393
Download all packet trace files for a device to the SMS ............................... 393
Replacing a device ....................................................................................... 393
Device replacement limitations ..................................................................... 394
Port configuration considerations ............................................................................................... 394
IPS device replacement considerations .......................................................................................... 396
Segments.................................................................................................................................... 396
DDoS...........................................................................................................................................396
Different models..........................................................................................................................396
Replace a device...........................................................................................................................397
Advanced DDoS tasks ....................................................................................................................... 397
Advanced DDoS supported models................................................................................................. 397
Advanced DDoS filter configuration ............................................................................................... 398
Edit Advanced DDoS filters.............................................................................................................. 398
Create/edit a DDoS filter exception ................................................................................................ 398
DDoS preferences............................................................................................................................399
Set DDoS preferences...................................................................................................................... 399
SMS managed devices..................................................................................................................... 399
Threat Protection System devices.................................................................................................. 400
440T devices..................................................................................................................................401
2200T devices................................................................................................................................401
TX Series devices............................................................................................................................401
Virtual Threat Protection System ....................................................................................................403
Unsupported features....................................................................................................................... 403
vTPS deployment and licensing...................................................................................................... 403
vTPS certificate installation prerequisites......................................................................................404
Create and download vTPS device license certificates ...............................................................404
To install the vTPS license certificate using the SMS .................................................................405
Intrusion Prevention System devices...............................................................................................406
S-Series devices..............................................................................................................................406
N-Platform devices.........................................................................................................................407
NX-Platform devices.......................................................................................................................407
Tier statistics for the vTPS, TPS, and IPS (NX-Platform) devices ..................................................409
Next Generation Firewall appliances.............................................................................................412
Core Controller...............................................................................................................................413
Core Controller segment (10G)....................................................................................................413
Core Controller iLinks ....................................................................................................................413
Flow management.........................................................................................................................413
TippingPoint vController ...................................................................................................................414
Access the TippingPoint vController from the SMS .................................................................414
TippingPoint Operating System........................................................................................................414
Virtual segments .................................................................................................................................416
Special notes ....................................................................................................................................416
Migration ........................................................................................................................................ 416
Limitations: 3.1 devices other than N-Platform or NX-Platform IPS devices...........................417
Virtual Segment table ......................................................................................................................417
Traffic flow analyzer .......................................................................................................................419
Segment groups .................................................................................................................................419
Device replace table ........................................................................................................................420
Replacing a previous IPS model with an NX model .................................................................422
Replacing an existing NX model with another NX model..........................................................422
General clarifications ....................................................................................................................422
NGFW....................................................................................................................................................424
NGFW routing ...................................................................................................................................
NGFW routing ...............................................................................................................................424
NGFW VPN configuration ..............................................................................................................424
NGFW authentication ......................................................................................................................424
NGFW distribution queue ..............................................................................................................425
Create a device HA cluster ............................................................................................................425
Create a device HA cluster ............................................................................................................426
Synchronize a cluster configuration ............................................................................................429
Force state change ........................................................................................................................430
Remove a cluster from the SMS .................................................................................................430
SSL appliance .................................................................................................................................430
Setting up an SSL appliance ...........................................................................................................431
Install the SSL appliance ............................................................................................................. 431
Configure the SSL appliance ........................................................................................................ 431
Configure SNMP on the SSL appliance ........................................................................................ 431
Configure SNMPv3 on the SSL appliance .................................................................................... 431
Add the SSL appliance to the SMS .............................................................................................. 432
SSL appliance configuration ............................................................................................................ 432
Device configuration ..................................................................................................................... 433
Network configuration .................................................................................................................... 433
  Ports tab ......................................................................................................................................433
Event monitoring (SSL appliance) ................................................................................................ 434
System health ................................................................................................................................ 434
Performance .................................................................................................................................. 435
Port health ..................................................................................................................................... 435
  Port statistics ............................................................................................................................... 435
Traffic ............................................................................................................................................. 436
  Server tab ................................................................................................................................. 436
  Net tab ....................................................................................................................................... 436
SSL tab ......................................................................................................................................... 437
Switch tab ..................................................................................................................................... 437
System log ..................................................................................................................................... 438
Stacking ...........................................................................................................................................439
Stacking for TPS ............................................................................................................................. 439
Overview ....................................................................................................................................... 439
Set up the stack ............................................................................................................................... 439
Stacking components ..................................................................................................................... 440
Basic stack configuration ................................................................................................................. 440
  Install the stacking components ................................................................................................ 440
Create the stack in the SMS .......................................................................................................... 442
  Add the stacking devices to the SMS .......................................................................................... 442
Create the stack ............................................................................................................................. 443
  Distribute the inspection profile ................................................................................................. 444
Resilient stack configuration .......................................................................................................... 445
Multiple network segment device configuration................................................................. 446
Update the stack configuration.............................................................................................. 448
Enable or disable stack resiliency......................................................................................... 448
Change the segment reference device................................................................................ 449
Replace a device in the stack............................................................................................... 449
Remove a device from the stack.......................................................................................... 450
Add a device to the stack...................................................................................................... 450
Delete the stack.................................................................................................................... 452
Grant permissions to the stack........................................................................................... 452
Add stack management to the user role............................................................................. 452
Grant the user group access to the stack........................................................................... 453
Distribute a TOS update....................................................................................................... 453
Troubleshooting.................................................................................................................... 453
Verify AOC cable installation.............................................................................................. 454
View stacking status............................................................................................................ 455
  Device details.................................................................................................................... 455
  Front panel stacking LEDs............................................................................................... 458
  Device shelf-level graphic............................................................................................... 459
Verify stack health and synchronization............................................................................. 459
  View overall health of the stack....................................................................................... 460
  Verify stacking bus state................................................................................................. 462
  Verify stack member state............................................................................................... 465
  Verify device state.......................................................................................................... 466
  Verify stack synchronization........................................................................................... 468
Resolve issues adding a device to the stack.......................................................................... 475
View stacking tier statistics............................................................................................... 476
Enable or disable Intrinsic High Availability Layer-2 Fallback............................................ 478
  Enable or disable Intrinsic HA L2FB on the stack......................................................... 478
  Enable or disable Intrinsic HA L2FB on a stacking device........................................... 479
CLI commands for stacking............................................................................................... 480
  show stacking................................................................................................................... 480
Limitations............................................................................................................................ 482
Repurpose a device.............................................................................................................. 483
Verify stack synchronization................................................................. 511
Resolve issues adding a device to the stack................................. 518
View stacking tier statistics................................................................. 519
Enable or disable Intrinsic High Availability Layer-2 Fallback .... 520
   Enable or disable Intrinsic HA L2FB on the stack.................... 521
   Enable or disable Intrinsic HA L2FB on a stacking device ..... 522
CLI commands for stacking................................................................. 523
   show stacking.................................................................................. 523
Limitations......................................................................................... 524
Repurpose a device............................................................................ 525
Differences between configuring a stack and a standalone device 526
Security policy configuration.............................................................. 526
Events and reports........................................................................... 529
System updates and snapshots......................................................... 530
SMS database restore to a different SMS..................................... 531
Administration.................................................................................. 532
General administration...................................................................... 532
   Working with the Admin (General) screen............................... 532
      SMS server.................................................................................. 532
      SMS software............................................................................. 532
         Download and install SMS software................................. 533
         Import and install SMS software from a CD or the TMC 533
      SMS patches............................................................................. 534
         Install an SMS patch............................................................... 535
         Roll back an SMS patch......................................................... 535
      SMS web security SSL certificate........................................ 535
         Reset the SMS web security SSL certificate.................... 536
         Import a custom Web security SSL certificate................. 536
      SMS certificate key................................................................. 537
         Update the SMS certificate key......................................... 538
   Viewing system health................................................................. 538
   Viewing port health..................................................................... 539
Viewing the SMS system log..............................................................540
View the SMS system log.................................................................540
Export SMS system log entries.........................................................540
Viewing the SMS audit log..............................................................541

Authentication and authorization..................................................542
Managing active sessions...............................................................542
Set or change a new resource group for a user account....................543
Terminate an active session............................................................543

Configuring authentication.........................................................543
Authentication source.......................................................................544
Edit the SMS server authentication source........................................544
Authentication configuration.......................................................545
Configure RADIUS authentication..................................................545
Edit the RADIUS server configuration...........................................545
Configure Active Directory authentication......................................547
Allowing remote users with Active Directory authentication............547
Edit the Active Directory server configuration..............................548
Edit Active Directory global group mapping.................................549
Import an Active Directory SSL certificate....................................550
Configure TACACS+ authentication...............................................550
Edit the TACACS+ server configuration.......................................551
Configure CAC authentication.....................................................552
CAC authentication overview......................................................554
Prerequisites...................................................................................556
Import CA Certificates....................................................................556
Add, edit, import, or delete personal identifiers..............................557
Enable CAC authentication..........................................................557
Log in to the SMS using CAC authentication...............................558

Managing user roles.....................................................................558
Create a user role..........................................................................559
Edit a user role..............................................................................560

Managing user groups..................................................................560
Create a user group......................................................................561
Edit a user group.........................................................................562
Delete a user group......................................................................562
Create a new signing request.................................................................578
Export a signing request.......................................................................579
Import the certificate............................................................................579

Database..............................................................................................579
Working with the Admin (Database) screen..........................................579
Database maintenance........................................................................579
  Edit data retention settings...............................................................582
  Reset data statistics.........................................................................583
  Initiate an immediate cleanup of data statistics..............................583
External database settings..................................................................583
  Configure the SMS for external access..........................................584
  Configure the SMS for replication..................................................584
  Configure the SMS to enable restricted access.............................585
Backup and restore............................................................................586
  Backup............................................................................................586
    Backup the SMS database............................................................586
    Edit a scheduled backup.............................................................588
    Delete a scheduled backup........................................................588
  Restore............................................................................................588
    Restore the SMS database........................................................590
Server properties................................................................................590
Configuring management properties..................................................590
  System information.........................................................................590
    Update system information........................................................591
  FIPS mode.......................................................................................591
    Enable or disable FIPS Crypto Core mode.................................592
  Services..........................................................................................593
    Enable or disable the SMS services..........................................593
Configuring network properties.........................................................594
  Network interface..........................................................................594
    Update network interface information......................................595
  Date/Time.......................................................................................595
    Enable Network Time Protocol................................................595
    Enable SMS Network Time Protocol authentication settings......595
    Manually set the time and date....................................................596
SMTP server .................................................................................................................................. 596
   Edit SMTP server settings ........................................................................................................ 596
TMC proxy ..................................................................................................................................... 597
   Configure a proxy TMC connection ........................................................................................ 597
Domain Name Service (DNS) ........................................................................................................ 598
   Configure DNS ......................................................................................................................... 598
Configuring NAT properties ......................................................................................................... 598
   SMS NAT ................................................................................................................................... 598
      Enable SMS global NAT ........................................................................................................ 598
      Disable SMS global NAT ....................................................................................................... 599
   SMS per network NAT .............................................................................................................. 599
      Enable SMS per network NAT .............................................................................................. 599
      Add or edit an SMS per network NAT address .................................................................... 599
      Delete SMS per network NAT addresses ............................................................................. 599
   Address determination ............................................................................................................. 600
Configuring integration properties ............................................................................................. 600
   IDResolver ................................................................................................................................ 600
Configuring syslog properties ....................................................................................................... 600
   Syslog format options .............................................................................................................. 600
   SMS system syslog ................................................................................................................... 601
   SMS audit syslog ..................................................................................................................... 601
   Device system syslog ............................................................................................................... 602
   Device audit syslog .................................................................................................................. 603
   Snort syslog for MARS [Deprecated] ....................................................................................... 603
   Snort syslog for V2 [Deprecated] .......................................................................................... 604
   SMS 2.0/2.1 syslog .................................................................................................................... 605
   SMS 2.5 syslog .......................................................................................................................... 607
   ArcSight CEF Format v3.5 [Deprecated] ................................................................................. 609
   ArcSight CEF Format v4.1 [Deprecated] ................................................................................ 611
   ArcSight CEF Format v4.2 ........................................................................................................ 614
   Create or edit a custom syslog format ....................................................................................... 618
      Available fields in a syslog format ....................................................................................... 618
   Copy an existing syslog format to create a custom format ...................................................... 628
   Delete a user-defined syslog format ......................................................................................... 628
   Remote syslog for events ......................................................................................................... 628
      Configure remote syslog notification settings .................................................................. 630
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edit syslog server settings</td>
<td>631</td>
</tr>
<tr>
<td>Delete a syslog server</td>
<td>631</td>
</tr>
<tr>
<td>Configuring SNMP properties</td>
<td>631</td>
</tr>
<tr>
<td>Request settings</td>
<td>632</td>
</tr>
<tr>
<td>Enable SNMP requests</td>
<td>632</td>
</tr>
<tr>
<td>Disable SNMP requests</td>
<td>632</td>
</tr>
<tr>
<td>NMS trap destinations</td>
<td>633</td>
</tr>
<tr>
<td>Configure the SMS to send NMS traps to a destination</td>
<td>633</td>
</tr>
<tr>
<td>Edit an NMS trap destination</td>
<td>633</td>
</tr>
<tr>
<td>Delete an NMS trap destination</td>
<td>633</td>
</tr>
<tr>
<td>Configuring TLS settings</td>
<td>634</td>
</tr>
<tr>
<td>Edit TLS versions</td>
<td>635</td>
</tr>
<tr>
<td>High Availability</td>
<td>635</td>
</tr>
<tr>
<td>SMS HA cluster compatibility requirements</td>
<td>636</td>
</tr>
<tr>
<td>Replication bandwidth requirements</td>
<td>636</td>
</tr>
<tr>
<td>Configure the SMS HA cluster</td>
<td>636</td>
</tr>
<tr>
<td>How do I apply SMS software updates to a cluster?</td>
<td>638</td>
</tr>
<tr>
<td>View HA cluster status</td>
<td>639</td>
</tr>
<tr>
<td>Adjust HA timeout values</td>
<td>639</td>
</tr>
<tr>
<td>Synchronize the SMS HA cluster</td>
<td>640</td>
</tr>
<tr>
<td>Deactivate the active SMS server</td>
<td>640</td>
</tr>
<tr>
<td>Swap the roles of the SMS HA cluster nodes</td>
<td>641</td>
</tr>
<tr>
<td>Invoke a failover</td>
<td>641</td>
</tr>
<tr>
<td>Disable the SMS HA cluster</td>
<td>641</td>
</tr>
<tr>
<td>Named resources</td>
<td>642</td>
</tr>
<tr>
<td>Create or edit a named resource</td>
<td>644</td>
</tr>
<tr>
<td>Create or edit named resource groups</td>
<td>644</td>
</tr>
<tr>
<td>Import or export named resources</td>
<td>645</td>
</tr>
<tr>
<td>Exports and archives</td>
<td>645</td>
</tr>
<tr>
<td>Export a file from the SMS exports and archives directory</td>
<td>646</td>
</tr>
<tr>
<td>Delete a file from the SMS exports and archives directory</td>
<td>646</td>
</tr>
</tbody>
</table>
IP address identifier........................................................................................................................................646
Add or edit an IP address ID.................................................................................................................. 647
Delete an IP address ID..........................................................................................................................648
Change the priority order for IP address groups.....................................................................................648

User ID IP Correlation...............................................................................................................................648
Add the Identity Agent............................................................................................................................649
Create an Identity Agent Group................................................................................................................649
Select an Identity Agent to be in a group..................................................................................................650
Enable Identity Agent group...................................................................................................................650
User ID IP Correlation events..................................................................................................................651
Configure a user resolver filter................................................................................................................652

Geo Locator database...............................................................................................................................652
Download a Geo Locator database file from the TMC............................................................................653
Import a Geo Locator database file.........................................................................................................653

Licensing..................................................................................................................................................653
Edit notification settings..........................................................................................................................655
Import a license entitlement package.......................................................................................................655
Licensing details.......................................................................................................................................656

SSL inspection..........................................................................................................................................658

Additional considerations.......................................................................................................................658

Requirements...........................................................................................................................................660

Manage SSL inspection from the SMS....................................................................................................661
Before you configure SSL inspection.......................................................................................................661
Update the license package.......................................................................................................................662
Import the license package.......................................................................................................................662
Verify the license package........................................................................................................................663
Enable SSL inspection..............................................................................................................................663
Configure SSL inspection........................................................................................................................664
Secure the SMS certificate repository ................................................................. 664
Import the SSL server certificate and private key ............................................. 665
Add or edit an SSL server .................................................................................. 666
Add or edit an SSL inspection policy ................................................................. 667
Distribute the inspection profile ....................................................................... 668
After you configure SSL inspection ................................................................. 669
Verify SSL inspection activity .......................................................................... 669
Replace a certificate ............................................................................................ 670
Add SSL inspection to the user role ................................................................. 671
Grant the user group access to the SSL server .................................................. 672
Best Practices ..................................................................................................... 672
Troubleshoot SSL inspection ............................................................................ 673
Basic troubleshooting ........................................................................................ 673
Advanced troubleshooting ................................................................................. 674
General troubleshooting ..................................................................................... 676
Login error messages ......................................................................................... 676
Password recovery .............................................................................................. 676
    Reset your password ..................................................................................... 677
Network changes .............................................................................................. 677
IPS port out-of-service ...................................................................................... 678
SMS error messages ......................................................................................... 678
Modifying filters ............................................................................................... 679
Distributing profiles .......................................................................................... 679
TMC connectivity ............................................................................................... 680
Geo Locator maps do not display correctly ...................................................... 681
Export a Tech Support Report .......................................................................... 681
Port information.................................................................................................................................. 683
   Required ports.................................................................................................................................... 683
   Active Response ports....................................................................................................................... 685
   HA ports..............................................................................................................................................686
   Optional ports..................................................................................................................................... 687
Reputation information.......................................................................................................................691
   Reputation import rules...................................................................................................................... 691
      Format rules.....................................................................................................................................691
      Tag category rules........................................................................................................................... 692
      Address rules................................................................................................................................... 692
SMS encryption protocols, algorithms, and cipher support.......................................................... 694
About this guide

This guide helps you get started configuring your TippingPoint system and managing your TippingPoint network devices.

This section covers the following topics:

- **Target audience** on page 1
- **Related documentation** on page 1
- **Conventions** on page 1
- **Customer support** on page 2

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

Related documentation

A complete set of documentation for your product is available on the TippingPoint Threat Management Center (TMC) at [https://tmc.tippingpoint.com](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>Bold font</td>
<td>• Key names</td>
</tr>
</tbody>
</table>
### Convention

<table>
<thead>
<tr>
<th>Convention</th>
<th>Element</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monospace font</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>Monospace, italic font</td>
<td>• Code variables</td>
</tr>
<tr>
<td></td>
<td>• Command-line variables</td>
</tr>
<tr>
<td>Monospace, bold font</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](https://tmc.tippingpoint.com).
SMS Overview

The Trend Micro™ TippingPoint Security Management System (SMS) is the control center for managing large-scale deployments of all TippingPoint products.

The main components of the system are the SMS server, the SMS web management console, and the SMS client. The SMS server, either the SMS appliance or the virtual product (vSMS), serves as a management system for multiple devices.

The following sections help you get started with the SMS.

**SMS hardware**

The SMS hardware appliance is available as a rack-mountable management server or as a virtual product (vSMS). Both include the SMS client and the SMS web management console.

See *Installation* on page 4 for an overview of installation information.

**SMS interfaces**

The SMS client provides functions similar to the Local Security Manager (LSM) on each device and enables you to configure, monitor, and report on all of the TippingPoint devices in your network from a single interface.

The SMS server includes the following interfaces:

- **SMS web management console** – Web-based interface that enables you to install or upgrade SMS client software, monitor the TippingPoint devices installed on your network, and access Threat Insights. If they are available, you can review the SMS system log, exported and archived files, or saved reports. You can also access certain web management console features from your mobile devices and tablets. For more information, see *SMS web management console* on page 5.

- **SMS client** – Java-based application for Windows, Linux, or Mac workstations. The SMS client consists of a graphical user interface that allows you to manage the TippingPoint system. For more information, see *SMS client* on page 24.

- **Command Line Interface (CLI)** – Text-based interface that enables users with SuperUser rights to log in to and configure the SMS server. For more information, see the *Security Management System Command Line Interface Reference*.

**SMS components and services**

At the core of the SMS is the ability to create multiple profiles, which can be distributed to specific devices. A *profile* is a collection of filters or rules that enable you to set up security configuration options for TippingPoint solutions.
Using profiles, you can distribute filters to multiple devices, specific devices, physical segments controlled by a specific device, or even virtual segments. The maximum number of devices depends on usage, network, and other environmental conditions.

When a profile is distributed, it includes shared settings (such as action sets, notification contacts, and services) as well as associated filters and filter setting modifications.

When you organize devices in groups or security zones, you simplify how security profiles get updated and distributed. The SMS can also be configured to regularly update all managed devices with the latest TippingPoint Operating System (TOS) software and Digital Vaccine (DV) packages.

The SMS interacts with the following services:

- **ThreatLinQ** – TippingPoint service that works with the TMC to collect and analyze security information. For more information, see ThreatLinQ on page 33.
- **Digital Vaccine (DV)** – Update service that includes the latest filter packages for protecting your network. For more information, see Digital Vaccines on page 188.
- **Threat Management Center (TMC)** – Centralized service center that monitors global threats and distributes up-to-date attack filter packages, software updates, and product documentation. For more information, see TMC on page 33.

**Installation**

Before you use the SMS server, install and configure the components of the SMS system. See the installation documentation for your SMS platform.

To install an SMS appliance, refer to the installation information on the TippingPoint Threat Management Center (TMC) at https://tmc.tippingpoint.com. This information describes the steps to mount the appliance in a rack, connect it to your network, and configure the server.

To install the vSMS, refer to the vSMS Getting Started Guide, which provides installation and setup information.

After you set up the SMS hardware and connect to your network, you must configure the server and install the client (see Install the SMS client on page 7). You must also complete certain initial management tasks (see Manage your system on page 29).

**Important:** Make sure your system meets TMC port requirements. See Port information on page 683.

For the most up-to-date information, download the latest SMS documentation from the TMC.
SMS web management console

The SMS web management console provides at-a-glance insight into your network security status with data that reflects the health, status, and security events related to your system. For more information on the main components of the system including the SMS server and the SMS client, see SMS Overview on page 3.

Threat Insights

Threat Insights of the SMS web management console is the starting point for monitoring application visibility and utilization, troubleshooting events and issues on your network, monitoring security alerts or issues, and capacity planning. You can also access Threat Insights from your mobile devices and tablets.

Threat Insights include:

- Breached Hosts on page 9
- Attacked Vulnerable Hosts on page 11
- Suspicious Objects on page 13
- ZDI Filter Hits on page 15

Quick access for device monitoring and management

The SMS web management console provides a convenient way to access:

- Devices – View all devices, device groups, segments, and stacks managed on the SMS. For more information, see Monitor all devices on page 16.
- Devices Requiring Attention – Quickly identify devices that might have health or performance issues. For more information, see Identify devices that require your attention on page 18.
- Layer-2 Fallback mode – In the event of a server outage, or if you detect a system failure, you can switch to the Layer-2 Fallback mode on a device. For more information, see Switch a device into Layer-2 Fallback mode on page 19.

You can also access these features from your mobile devices and tablets.

Quick access to reports, exported and archived files, and system logs

The SMS web management console provides a convenient way to access saved reports, exported files, and SMS system logs.

For more information, see the following topics:

- View or download reports on page 20
- Download exports and archives from the SMS on page 20
Desktop versus mobile experience – feature availability

A key to successfully using the web management console is understanding what is available on the SMS desktop or mobile experiences. If a feature is not currently available on a mobile device, we mention that in the feature description. The following table specifies the availability of web management console features according to your SMS deployment.

Table 1. Desktop versus mobile experience

<table>
<thead>
<tr>
<th>Feature:</th>
<th>Available on ...</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>Access Threat Insights</em> on page 9</td>
<td>• Desktop access</td>
</tr>
<tr>
<td></td>
<td>• Mobile access</td>
</tr>
<tr>
<td><em>Monitor managed devices</em> on page 16</td>
<td>• Desktop access</td>
</tr>
<tr>
<td></td>
<td>• Mobile access</td>
</tr>
<tr>
<td><em>View devices that require your attention</em> on page 18</td>
<td>• Desktop access</td>
</tr>
<tr>
<td></td>
<td>• Mobile access</td>
</tr>
<tr>
<td><em>Switch a device into Layer-2 Fallback mode</em> on page 19</td>
<td>• Desktop access</td>
</tr>
<tr>
<td></td>
<td>• Mobile access</td>
</tr>
<tr>
<td><em>View saved reports</em> on page 20</td>
<td>• Desktop access</td>
</tr>
<tr>
<td></td>
<td>• Mobile access</td>
</tr>
<tr>
<td><em>Install the SMS client</em> on page 7</td>
<td>• Desktop access only</td>
</tr>
<tr>
<td><em>View exported and archived files</em> on page 20</td>
<td>• Desktop access only</td>
</tr>
<tr>
<td><em>View system logs</em> on page 20</td>
<td>• Desktop access only</td>
</tr>
</tbody>
</table>
Log in to the SMS web management console

After the SMS server is configured and your user account has been defined (see Installation on page 4), you can connect to the SMS web management console.

1. Open a supported web browser.
   Supported web browser versions for desktop access include:
   - Firefox 51 and later
   - Chrome 55 and later
   - Safari 10 and later
   - Microsoft Internet Explorer (version 11 only)
   - Microsoft Edge 14 and later
   Supported web browser versions for mobile access include:
   - Safari 10 and later
   - Chrome for Android version 57 and later
2. Enter the IP address that you configured as the management address for the SMS server (for example, https://<sms-server>).
3. Enter your username and password, and click Log In.

Install the SMS client

The Client Installation page displays the system requirements and instructions for installing, upgrading, or uninstalling the SMS client on a Windows, Linux, or Mac computer. When a patch is available, it is noted under the installer buttons.

To communicate with the SMS server, the SMS client must use TCP port 9033 and TCP port 10042. For more information on the additional ports that you must make available, see Port information on page 683.

**Note:** You cannot install the SMS client from your mobile device or tablet. To install the SMS client, you must use a desktop workstation.

1. Log in to the SMS web management console on page 7.
2. Select Client Installation in the navigation pane.
3. Select the appropriate SMS client installer for your platform and download it.
   **Note:** Before you can install the SMS client on an OS X computer, you must follow the instructions outlined in the OS X prerequisites on page 8.
4. Run the installation wizard.
The installation wizard checks for previous installations and guides you through the options for installing or updating the client software. When installation is complete, the installer prompts you to end or open the client upon completion. For more information, see Log in to the SMS client on page 24.

OS X prerequisites

Important information when using Mac OS X to host an SMS client

When you upgrade the SMS client on OS X with Oracle Java Runtime version 1.8u71 or later, the SMS client will not be able to connect to an SMS that is still running with a 1k certificate key. To avoid this issue, upgrade the SMS from a 1k certificate key to a 2k key.

Note: If you have already completed this step in a previous SMS release, you do not need to do this again.

If you cannot connect to the SMS client using Mac OS X, you have two options:

- Temporarily make the following changes to the JRE on your local Mac OS X.
- Use a Windows SMS client to update the SMS to a 2K certificate key. After you do this, you will no longer need to temporarily change to the JRE on your local Mac OS X.

How to change the JRE on your local Mac OS X

1. Edit the java.security file located in the /Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Home/lib/security directory.

2. Locate jdk.certpath.disabledAlgorithms=MD2, MD5, RSA keySize < 1024, and then delete MD5 from the line.

   The line should now be jdk.certpath.disabledAlgorithms=MD2, RSA keySize < 1024.

3. Locate jdk.tls.disabledAlgorithms=SSLv3, RC4, MD5withRSA, DH keySize < 768, and then delete MD5withRSA from the line.

   The line should now be jdk.tls.disabledAlgorithms=SSLv3, RC4, DH keySize < 768.

4. Open the dmg (disk image) and run the installer application.

Note: If you receive the error message "TippingPoint SMS client Installer is damaged and can't be opened," go to Mac System Preferences > security & privacy settings > and change "Allow applications downloaded from" to "Anywhere."

Note: If you receive additional error messages, contact support.

How to upgrade the SMS certificate key

To upgrade the SMS certificate key, log in to the SMS and under Admin > General > SMS Certificate Key, upgrade to a 2k key. For more information, see SMS certificate key on page 537.

Review the SMS certificate key compatibility matrix for your device.
Threat Insights

Use Threat Insights to monitor all your applications and security alerts. In addition, you can use Threat Insights for troubleshooting and resource planning. Because Threat Insights are accessible from your mobile devices and tablets, you can achieve all this visibility and control remotely.

Threat Insights provide visibility into the following:

- Breached Hosts on page 9
- Attacked Vulnerable Hosts on page 11
- Suspicious Objects on page 13
- ZDI Filter Hits on page 15

To access Threat Insights, log in to the SMS web management console on page 7.

Filter Threat Insights by time period

Events are sent to the Threat Insights as they are generated with the most recent events listed at the top.

Last 24 hours, last 7 days, last 30 days, custom range

By default, the events from the last 30 days are displayed when you access Threat Insights from a desktop workstation.

Events from the last 24 hours are displayed when you access Threat Insights from a mobile device.

You can further filter your results to events from the last seven days or the last 24 hours. To narrow larger sets of events to a specific time period, you can configure your own custom date and time range.

To filter the number of Threat Insights events by time period or to adjust the time period, always return to Threat Insights and first select an option from the Time period list.

View devices that require your attention

You can quickly view a list of devices that might have system health, performance, or port issues. For more information, see Identify devices that require your attention on page 18.

Breached Hosts

Breached Hosts identify hosts in your network that might be compromised based on intelligence gathered from your Deep Discovery (DD) devices, TPS devices, and IPS devices. The following security intelligence is leveraged to identify:

- Domain generation algorithms (DGA) defense malware filters
- Reputation events that score hosts and provide context from policy and attack filters
Threat Digital Vaccine (ThreatDV) delivers a weekly malware filter package to help protect against the latest advanced threats. It prevents and disrupts malware activity, secures sensitive data, and optimizes network performance. ThreatDV also includes reputation feeds that are updated multiple times a day. Entries are assigned a threat score between 1 to 100 based on a comprehensive analysis of the activity, source, category, and threat. The malware filters are designed to detect:

- Infiltration
- Exfiltration
- Phone-home
- Command-and-control (C&C)
- DGA
- Mobile traffic

Some malware families use DGA. This malware strategy randomly generates a large number of domain names to avoid hard-coding IP addresses or domain names within the malware. The breached host then attempts to contact some of the generated domain names. DGA Defense filters use pattern recognition and linguistic analysis to detect algorithmically generated DNS requests from infected hosts. As part of a malware filter package, these filters protect your system against known malware families and suspicious domain names generated by unknown malware families.

To identify breached hosts in your network environment, your device must be registered for the ThreatDV service.

Newly discovered threats forwarded from your DD devices can also be used to identify breached hosts in your network. The DD devices detect suspicious network traffic between hosts and discovered CnC servers.

To include the C&C Callback Address data from your DD device, you must include the following predefined tag categories on the SMS:

- Trend Micro Detection Category
- Trend Micro Publisher
- Trend Micro Severity
- Trend Micro Source

For more information, see Tag Categories tab on page 213.

To view Breached Hosts on the web management console, select Threat Insights on the navigation pane, and then select Breached Hosts. The following information is displayed.
Table 2. Breached Hosts

<table>
<thead>
<tr>
<th>Heading</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>IP address (either source or destination) of the identified breached host.</td>
</tr>
<tr>
<td>Host Name</td>
<td>Host name of the IP address, if available.</td>
</tr>
<tr>
<td>Last Breached Filter</td>
<td>The name of the filter that either matches traffic from the breached host or traffic to the breached host.</td>
</tr>
<tr>
<td>Last Hit Time</td>
<td>The time on the device that the traffic was last encountered.</td>
</tr>
<tr>
<td>Blocked Hits</td>
<td>Number of times traffic was blocked by a filter and an event was generated.</td>
</tr>
<tr>
<td>Permitted Hits</td>
<td>Number of times traffic matched a filter and was permitted to flow through.</td>
</tr>
</tbody>
</table>

If you see permitted hits, consider updating your security policy. You can change the action set to block or block + notify (see Action sets on page 123). You can also associate your policy with a Responder Policy (see Responder on page 251).

Attacked Vulnerable Hosts

Attacked Vulnerable Hosts identify vulnerabilities in your network. Third-party scans generate the vulnerability data, which the SMS imports and presents as a list. This enhanced visibility into your network allows you to highlight blocked or permitted attacks targeted to vulnerable assets.

You can then make immediate updates to your security policy for the protection of your network. With the vulnerability insights provided by the Attacked Vulnerable Hosts, you can run updates on your assets.

Importing vulnerability scan data to the SMS

Before you can identify attacked vulnerable hosts in your network, you must first run a vulnerability scan using a third-party vendor and import this data to the SMS. For more information, including supported third-party vendors and scan specifications, see Import vulnerability scans on page 228.

To view Attacked Vulnerable Hosts on the web management console, select Threat Insights on the navigation pane, and then select Attacked Vulnerable Hosts. The following information is displayed.
## Table 3. Attacked Vulnerable Hosts

<table>
<thead>
<tr>
<th>Heading</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expand/Collapse</td>
<td>Controls visibility to the relevant filters associated with the vulnerable host identified in a vulnerability scan.</td>
</tr>
<tr>
<td></td>
<td>Expand to view additional information including:</td>
</tr>
<tr>
<td></td>
<td>• Relevant filter name</td>
</tr>
<tr>
<td></td>
<td>• Vulnerabilities identified including the CVEs</td>
</tr>
<tr>
<td></td>
<td>• Last hit time</td>
</tr>
<tr>
<td></td>
<td>• Number of blocked hits</td>
</tr>
<tr>
<td></td>
<td>• Number of permitted hits</td>
</tr>
<tr>
<td>IP Address</td>
<td>Network IP address of the vulnerable host.</td>
</tr>
<tr>
<td>Host Name</td>
<td>Host name of the IP address, if available.</td>
</tr>
<tr>
<td>Last Scan</td>
<td>Name of the vulnerability scan file available on the SMS, and the number of days ago it was imported to the SMS. Consider importing a new vulnerability scan file to replace files that are older than two weeks.</td>
</tr>
<tr>
<td>Relevant Filters</td>
<td>The number of filters identified. When you expand the table column, the name of the filter displays in addition to the vulnerabilities. The SMS establishes a correlation between the CVEs provided from a vulnerability scan and the CVEs included in the DV filters. Using this information, the relevant filters are displayed.</td>
</tr>
<tr>
<td>Vulnerabilities</td>
<td>When you expand the table column, the name of the filter is displayed along with any associated vulnerabilities. Expanding an event will display the unique CVE tracking number identified in the DV filter.</td>
</tr>
<tr>
<td>Last Hit Time</td>
<td>Date and time when the relevant filter was processed by the inspection, and traffic was either blocked or permitted.</td>
</tr>
<tr>
<td>Blocked Hits</td>
<td>Number of times traffic was blocked by a filter and an event was generated.</td>
</tr>
<tr>
<td>Heading</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Permitted Hits</td>
<td>Number of times traffic matched a filter and was permitted to flow through. If you see permitted hits, consider updating your security policy (see Profile tuning on page 234).</td>
</tr>
</tbody>
</table>

**Suspicious Objects**

Suspicious Objects use intelligence gathered from your Deep Discovery (DD) devices and your TippingPoint devices to block malware and other infections. In addition to preventing infections and disrupting malware communications, this integrated environment protects critical resources and isolates infected resources. Suspicious Objects also use data provided by Digital Vaccines (DVs) and the Reputation Database.

When your DD device detects a threat, it alerts your TippingPoint IPS and TPS devices by forwarding threat intelligence to the SMS.

You can use reputation filters to set policies that monitor or block access to discovered suspicious objects. When you create the reputation filters, include criteria from the following tag categories:

- Trend Micro Detection Category
- Trend Micro Publisher
- Trend Micro Severity
- Trend Micro Source

**Note:** You must have predefined tag categories configured in order for any data to be displayed for Suspicious Objects. For more information, see *Tag Categories tab* on page 213.

To view Suspicious Objects on the web management console, select Threat Insights on the navigation pane, and then select Suspicious Objects. The following information is displayed.

**Table 4. Suspicious Objects**

<table>
<thead>
<tr>
<th>Heading</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Object</td>
<td>IP address or host name, if available, of the suspicious object.</td>
</tr>
<tr>
<td>Severity</td>
<td>Severity identified for the suspicious object, based on the Trend Micro Severity tag category. For more information, see <em>Tag Categories tab</em> on page 213.</td>
</tr>
</tbody>
</table>
### Action in Profiles

Every profile that is *configured for Reputation* has at least one reputation filter. For a profile to block or permit Suspicious Objects, its reputation filter must specify the following criteria:

- Entry criteria which matches the predefined tag categories for Suspicious Objects. For more information, see *Tag Categories tab* on page 213.
- The filter is enabled.
- The action is set to **block** or **permit**.

Your security policy, as it relates to Suspicious Objects, is expressed using the following categories:

- **Protected** – All profiles configured for reputation *block* Suspicious Objects.
- **Partially protected** – Some profiles configured for reputation *block* Suspicious Objects, and other profiles *permit* Suspicious Objects.
- **Monitored** – All profiles configured for reputation *permit* suspicious objects.
- **Unprotected** – Displays for any of the following reasons:
  - At least one profile is configured for reputation, but no Suspicious Object entries match.
  - A reputation filter matches but it is disabled.
  - No profile is configured for reputation on the SMS.

If you see **Unprotected**, consider updating your security policy. See *Action sets* on page 123.

### Last Hit Time

Date and time that the filter was processed by the inspection.

### Blocked Hits

Number of times traffic was blocked by a filter and an event was generated.

### Permitted Hits

Number of times traffic matched a filter and was permitted to flow through.

If you see permitted hits, consider updating your security policy. You can change the action set to **block** or **block + notify** (see *Action sets* on page 123).
ZDI Filter Hits

Zero Day Initiative (ZDI) Filter Hits identify the number of blocked or permitted hits for pre-disclosed and disclosed filters.

DV filter protection covers the time between when a vulnerability is discovered and when a patch is made available. In addition, DV filters provide added protection for legacy, out-of-support software. DV packages are delivered weekly, or immediately when critical vulnerabilities emerge, and can be deployed automatically with no user interaction required. For more information, see Digital Vaccines on page 188.

ZDI Filter Hits include:

- **Pre-Disclosed Filters** - Include limited details to protect the secrecy of a ZDI vulnerability discovery until a product vendor can develop a patch. Although Pre-Disclosed filters apply to critical security events and do not describe the vulnerability to you, the filters provided through the DV service still protect your network environment from the unpatched vulnerability.

  **Note:** Pre-Disclosed filter event hits display regardless of the time range you select. For example, if you narrow the ZDI Filter Hits to the last 7 days, an event from the last 30 days will still display.

- **Disclosed Filters** - After details are made public in coordination with the product vendor, the DV service provides an updated description.

To view ZDI Filter Hits on the web management console, select Threat Insights on the navigation pane, and then select ZDI Filter Hits. The following information is displayed.

**Table 5. ZDI Filter Hits**

<table>
<thead>
<tr>
<th>Heading</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter</td>
<td>Name of the filter that generated the alert or block.</td>
</tr>
<tr>
<td>CVE</td>
<td>Unique tracking number used to identify a Common Vulnerabilities and Exposures (CVE). CVE IDs are publicly known security vulnerabilities.</td>
</tr>
<tr>
<td>Released</td>
<td>Date the filter was released by the TMC.</td>
</tr>
<tr>
<td>Filter Disclosed</td>
<td>Date the filter was publicly disclosed, if available.</td>
</tr>
<tr>
<td>Last Hit Time</td>
<td>Date and time that the filter was processed by the inspection.</td>
</tr>
</tbody>
</table>
### Blocked Hits
Number of times traffic was blocked by a filter and an event was generated.

### Permitted Hits
Number of times traffic matched a filter and was permitted to flow through.

If you see permitted hits, consider updating your security policy. You can change the action set to **block** or **block + notify** (see *Action sets* on page 123). You can also associate your policy with a Responder Policy (see *Responder* on page 251).

## Monitor all devices

The Devices: All Devices page on the web management console displays a list of all devices, device groups, clusters, and stacks managed on the SMS. This page also displays icons that represent each TippingPoint device that has been added to the SMS, whether the device is currently managed or unmanaged. Each icon includes the name of the device or component, status indicators, and networking information. For more information, see *Devices* on page 282.

For more information on the health and hardware statuses, see *Status conditions* on page 17. To quickly identify devices that might have health or performance issues, go to the *Devices Requiring Attention* on page 18 panel on the Threat Insights portal.

### Devices: All Devices

To open the Devices: All Devices page on the web management console, *Log in to the SMS web management console* on page 7, and then select *Devices* in the navigation pane. This page displays the following information.

### Table 6. All Devices

<table>
<thead>
<tr>
<th>Heading</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name (and icon) of the device. If a device is included in a device group, select the name of the device group to drill down or expand the device information.</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP address used to make a connection to the device.</td>
</tr>
<tr>
<td>Model</td>
<td>Model and type of the device.</td>
</tr>
</tbody>
</table>
### Security Management System User Guide

<table>
<thead>
<tr>
<th><strong>Heading</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>System Health</td>
<td>Indicator that provides information about the hardware components of the managed device. System health information is also available on the SMS client in the following areas:</td>
</tr>
<tr>
<td></td>
<td>• Dashboard (see Health and Status gadgets on page 49)</td>
</tr>
<tr>
<td></td>
<td>• Devices workspace (see System health summary on page 311)</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If the System Health indicator displays an error, you can view the error on the SMS System Log. For more information, see View system logs on page 20.</td>
</tr>
<tr>
<td>Performance</td>
<td>Indicator that provides top-level performance information of the managed device, such as packet statistics or CPU. The SMS client also provides performance information on the Devices workspace (see Performance on page 312).</td>
</tr>
<tr>
<td>Port Health</td>
<td>Indicator that tracks key port statistics for the managed device. The SMS client also provides port health information on the Devices workspace (see Devices (All Devices) on page 282).</td>
</tr>
<tr>
<td>Layer-2 Fallback</td>
<td>Indicates current Layer-2 Fallback status. If the device is in Layer-2 Fallback mode, an explanation is displayed. To switch a device into Layer-2 Fallback mode, see Switch a device into Layer-2 Fallback mode on page 19.</td>
</tr>
</tbody>
</table>

### Status conditions

Each device has a status condition that provides a high-level indication of system health, performance, and port health. Status conditions are color-coded and have associated icons so that you can quickly identify and respond to device status.

If the device is functioning properly, the System Health, Performance, and Port Health status indicators are green. If a device has issues with its health status, the status indicators change color, and the device is listed on the Devices Requiring Attention on page 18 panel. If a device is unmanaged, a message is displayed under the System Health, Performance, and Port Health. For more information about the available status conditions for a device, see Status indicator legends on page 322.

To view all status conditions for all managed devices, go to the Devices on page 16 page.
Identify devices that require your attention

The Devices Requiring Attention panel on the web management console displays a list of managed devices that might have health or performance issues so that you can quickly identify and respond to device status. For more information on all available status conditions for a device, see Status conditions on page 17.

If you want to view all devices managed on the SMS, not just those that might require your attention, go to the Devices on page 16.

To view the Devices Requiring Attention panel on the web management console, Log in to the SMS web management console on page 7, and then select Threat Insights in the navigation pane.

The Devices Requiring Attention panel displays the following information.

Table 7. Devices requiring attention

<table>
<thead>
<tr>
<th>Heading</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name (and icon) of the device that has system health, performance, or port health issues.</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP address used to make a connection to the device.</td>
</tr>
<tr>
<td>Model</td>
<td>Model and type of the device.</td>
</tr>
<tr>
<td>System Health</td>
<td>Indicates a potential issue with the hardware components of a device.</td>
</tr>
<tr>
<td></td>
<td>System health information is also available on the SMS client in the following areas:</td>
</tr>
<tr>
<td></td>
<td>• Dashboard (see Health and Status gadgets on page 49)</td>
</tr>
<tr>
<td></td>
<td>• Devices workspace (see System health summary on page 311)</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If the System Health indicator displays an error, you can view the error on the SMS System Log. For more information, see View system logs on page 20.</td>
</tr>
<tr>
<td>Performance</td>
<td>Indicates top-level performance issues of a device, such as packet statistics or CPU.</td>
</tr>
<tr>
<td></td>
<td>The SMS client also provides performance information on the Devices workspace (see Performance on page 312).</td>
</tr>
<tr>
<td>Port Health</td>
<td>Indicates port health issues of a device.</td>
</tr>
</tbody>
</table>
The SMS client also provides port health information on the Devices workspace (see Devices (All Devices) on page 282.

<table>
<thead>
<tr>
<th>Heading</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Layer-2 Fallback</td>
<td>Indicates current Layer-2 Fallback status of a device. If the device is in Layer-2 Fallback mode, an explanation is displayed. To switch a device into Layer-2 Fallback mode, see Switch a device into Layer-2 Fallback mode on page 19.</td>
</tr>
</tbody>
</table>

**Switch a device into Layer-2 Fallback mode**

In the event of a server outage, or if you detect a system failure, you can automatically switch to the Layer-2 Fallback mode on a device. You can also use the web management console to put a device into Layer-2 Fallback mode, monitor which devices are in Layer-2 Fallback mode, or to remove the Layer-2 Fallback mode on a device.

**Note:** You can access these features from your mobile devices and tablets.

Layer-2 Fallback mode determines how a device manages traffic on each segment in the event of a system failure. For more information on how to configure this setting on the device from the SMS client, see HA (High Availability) on page 361.

2. Select a device (see *Monitor all devices* on page 16 or *Identify devices that require your attention* on page 18).
3. Set the Layer-2 Fallback mode to *On*.

   When a device is in Layer-2 Fallback mode, it either permits or blocks all traffic on each segment, depending on the (Layer-2 Fallback) action setting for the segment. When a device is in Layer-2 Fallback mode, any traffic allowed through the device is not inspected; it simply passes through the device.

   **Note:** You cannot switch to the Layer-2 Fallback mode if the device is unable to communicate with the SMS.

4. Select *Confirm* to switch to the Layer-2 Fallback mode.

   After you switch the device into Layer-2 Fallback, a confirmation message is displayed.

5. To remove the Layer-2 Fallback mode on a device, set the mode to *Off*.
View or download reports

The Reports page contains links to the saved reports that are available on the SMS. For more information about how to create a saved on the SMS, see *Saved reports* on page 117.

2. Select **Reports** in the navigation pane.
3. Select **Saved Reports**, and then select a report name.
4. To view the report in a new tab, select **HTML**.
   
   Depending on your browser settings, the report is displayed in the browser or a new tab.
5. (optional) To download a report, select a file type: **PDF**, **CSV**, **XML**, **DOCX**, or **XLS**.

Download exports and archives from the SMS

The Exports and Archives page displays links to the files that have been exported or archived from the SMS. You can download or delete these files from the SMS web management console. For more information about how to export a file on the SMS, see *Exports and Archives* on page 645.

**Note:** You cannot download exported or archived files from your mobile device or tablet. To download these files, you must use a desktop workstation to access the web management console.

2. Select **Exports and Archives** in the navigation pane.
3. To download a file, select the check box next to the file name, and click **Download**.
4. To delete one or more files, select the check boxes next to the file name names, and click **Delete Selected**.
5. To delete all files, click **Delete All**.

View system logs

The System Logs page displays the system log messages from the SMS. System log messages are sent to the web management console as they are generated with the most recent messages listed at the top. For each event, the system log displays the date and time, severity level and color-coded icon, and a message description. Viewing system log events can help you troubleshoot the SMS and device issues. For more information about the system logs, see *Viewing the SMS system log* on page 540.

**Note:** You cannot view the SMS system logs from your mobile device or tablet. To view the system logs, you must use a desktop workstation to access the SMS web management console.

2. Select **System Logs** in the navigation pane.
3. To filter the system logs by severity level, select an option:
   - **All Severity** to view all system log messages.
   - **Critical** to only view critical messages.
   - **Error** to only view error messages.
   - **Warn** to only view warning conditions.
   - **Info** to only view informational messages.

4. To filter the system logs by date or time, select an option:
   - **Latest** to view the latest SMS system log messages.
   - **Custom Range** to filter the SMS system log messages by selecting or entering a start date (and time) and an end date (and time) from the calendar. This is helpful if your search has resulted in large set and you want to narrow your results to a specific time range.

## Access tools and resources

The About page contains links to the Open Source information, online help, and the Threat Management Center (TMC).

1. **Log in to the SMS web management console** on page 7.
2. Select **About** in the navigation pane.
3. To review the Open Source Information, select **Open Source Information**.
4. To view the SMS online help in a new tab, select **Help**.
   
   You can also access the help from the SMS web management console (desktop access) if you click the ? icon. For the most recent documentation and updates, check the TMC.
5. To access the TMC, select **Threat Management Center (TMC)**.

## Threat Insights and web management console FAQ

### How often are the events for Threat Insights updated?

Threat Insights events are updated approximately every minute. For more information about how to adjust this time interval, see **Reports** on page 47.

The time required to process information for display on the Threat Insights varies. Many variables affect the amount of time needed to process the data. The extent of the time range and the number of events that occur within a range are contributing factors. The time displayed on the Threat Insights reflects the time of the actual event on the detection device. This might not correspond to the SMS Receipt Time or the Device Log Time reported on the Events workspace on the SMS client. The differences could be attributed to different timekeeping configuration of the systems and the variable speeds of the network.
To synchronize Threat Insights events, you can:
- Reload the page on your web browser.
- Log out of the web management console, and then log back in.

**How can I filter events by time period?**

You can quickly filter the number of events for the Breached Hosts, Attacked Vulnerable Hosts, Suspicious Objects, and ZDI Filter Hits by:
- Last 30 days (default view on desktop access)
- Last 7 days
- Last 24 hours (default view on mobile access)
- Custom date and time range

To filter the number of Threat Insights events by time period or to adjust the time period, you must always return to the Threat Insights and first select an option from the Time Period list.

**Note:** Pre-Disclosed filter event hits display regardless of the time range you select. For example, if you narrow the ZDI Filter Hits to the last 7 days, an event from the last 30 days will still display.

**What do the counts on Threat Insights refer to?**

The count results on the Threat Insights refer to the number of events generated or suspicious objects discovered, not the number of blocked or permitted hits.

**When are Threat Insights events no longer available?**

When the maximum number of Threat Insights events are displayed on the portal, the oldest event is deleted to allow new events to be displayed.

**What are the supported web browser versions to access the web management console?**

Supported web browser versions for desktop access include:
- Firefox 51 and later
- Chrome 55 and later
- Safari 10 and later
- Microsoft Internet Explorer (version 11 only)
- Microsoft Edge 14 and later

Supported web browser versions for mobile access include:
- Safari 10 and later
• Chrome for Android version 57 and later

**What are the device version requirements to use Threat Insights?**

The following platforms support Threat Insights:

• Threat Protection System (TPS) and Intrusion Prevention System (IPS) devices with versions currently supported

• Advanced Threat Protection for Networks with version 3.85.1002 or later installed

• Advanced Threat Protection for Email with version 2.6.1313 or later installed

• SMS with version 4.6.0 or later installed

**Does DD device information display on the Devices page or the Devices Requiring Attention panel?**

The SMS web management console does not retrieve the status from Deep Discovery (DD) devices. It only displays devices that are managed through the SMS. For more information about the DD device, see the device documentation on the Trend Micro documentation site.
SMS client

Use the SMS client to manage and maintain your TippingPoint system. The SMS includes the following:

*Administration* on page 532 — Manage user access, system and audit logs, and system settings. Only users with the correct role and access can manage Admin settings.

*Devices* on page 282 — Configure, monitor, and manage devices, device groups, segments, network configuration, traffic capture. You can also download TOS updates and distribute them to managed devices from this workspace. You can monitor managed devices, and change the Layer-2 Fallback mode on a device using the SMS web management console. For more information, see *SMS web management console* on page 5.

*Profiles* on page 122 — Tune the behavior of your TippingPoint system by managing, editing, and applying profiles, filters, action sets, Digital Vaccine (DV) packages, and importing vulnerability scans.

*Events* on page 58 — Manage and view system behavior and events.

*Reports* on page 96 — Generate, download, and view reports that provide details of threats encountered by the entire system and show processing trends.

*Responder* on page 251 — Manage response actions and policies for the SMS system. You can also add network equipment such as switches and routers that may participate in the Active Response System, configure RADIUS server options, and add IP Correlation network mapping.

For more information on the main components of the system including the SMS server and the SMS web management console, see *SMS Overview* on page 3.

Log in to the SMS client

1. Launch the TippingPoint SMS client. For more information, see *Install the SMS client* on page 7.
2. Do one of the following:
   - To log in to a single SMS client, specify the IP address or fully qualified hostname in the **SMS Server** field.
   - To log in to multiple SMS clients, select **More > Add** and specify the IP address or fully qualified hostname. Repeat for each SMS.
     
     **Note:** When you log in to multiple clients, the SMS saves each address you enter. The SMS client does not list all active SMS servers. For information on account settings, see *Authentication and authorization* on page 542.

3. Provide the username and password for a user account defined on the SMS server.
   
   **Note:** Status messages are displayed at the bottom of the SMS Login screen.

4. Click **Login**.
If your password has expired, or if an administrator has set a forced password change, the **Password Change Required** dialog is displayed and you must enter your old password, a new password, and a confirmation. When you log in to multiple SMS server clients, the client for each server is displayed on a separate tab.

**Note:** Your access to various features and functionality is limited by the role assigned to your user account. For details about user roles, see *Managing user roles* on page 558.

**SMS client user interface**

The SMS client user interface provides controls that enable you to manage and maintain your TippingPoint system. The interface includes a menu bar, the SMS toolbar, a navigation pane, and a content pane. If you log in to multiple SMS servers, the client displays a tab for each server.

The basic components of the SMS client interface are described below.

![Image of the SMS client user interface]

1. **Main window**
2. **Menu bar**
3. **SMS toolbar**
4. **Navigation pane**
5. **Profile view**
6. **Filter criteria**
7. **Event view**
## Table 8. SMS client user interface

<table>
<thead>
<tr>
<th>Number</th>
<th>Object</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Menu</td>
<td>The menu bar contains five top-level menus: <strong>File</strong>, <strong>Edit</strong>, <strong>View</strong>, <strong>Tools</strong>, and <strong>Help</strong>. Each menu contains options for using SMS features. The options can differ according to your selection in the navigation pane and the screen displayed in the content pane.</td>
</tr>
<tr>
<td>2</td>
<td>Tab</td>
<td>When you are connected to multiple SMS servers, each tab displays a complete client interface for the selected SMS.</td>
</tr>
<tr>
<td>3</td>
<td>Toolbar</td>
<td>Use the toolbar to navigate to each SMS workspace including <strong>Events</strong>, <strong>Reports</strong>, <strong>Profiles</strong>, <strong>Responder</strong>, <strong>Devices</strong>, and <strong>Admin</strong>. A workspace consists of the elements in content and navigation panes that enable you to view, query, configure, or act on your TippingPoint system.</td>
</tr>
<tr>
<td>4</td>
<td>Navigation</td>
<td>Navigate to areas within the same workspace. When you select an option from the toolbar, the navigation pane displays groupings of objects, options, or functions as nodes in a navigation tree. Some nodes contain multiple levels, which you can expand by clicking the plus (+) symbol next to the node. Contents of the navigation pane differ according to your selected workspace.</td>
</tr>
<tr>
<td>5</td>
<td>Content pane</td>
<td>The content depends on your selection in the navigation pane. Content may consist of criteria for queries, lists of entries, display options, or details. The content pane displays screens for viewing and managing your SMS. This area of the user interface includes various components for searching or selecting information to view or maintain. The contents of the pane differ according to your selections in the navigation pane, SMS toolbar, or menu bar.</td>
</tr>
<tr>
<td>6</td>
<td>Panel</td>
<td>Defined, named area or section of a screen displayed in the content pane.</td>
</tr>
<tr>
<td>Number</td>
<td>Object</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td>7</td>
<td>List</td>
<td>Rows of data displayed in a table view. Typically, you can select a row to act on.</td>
</tr>
</tbody>
</table>

### SMS features

The SMS provides the following features.

Table 9. SMS features

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto complete</td>
<td>The SMS client uses an auto-complete feature to list suggested values for IP Address fields. When you type a partial address, a list of IP addresses that match that value is displayed near the input field. To use one of a value from the suggested list, click the list entry.</td>
</tr>
<tr>
<td>Tabbed views</td>
<td>Many screens in the SMS client, especially in the Profiles and Devices workspaces, include tabbed views that enable you to navigate quickly between related categories. The SMS also uses tabbed views to display separate instances. For example, the SMS client allows you to log on to multiple SMS servers, and each connection is displayed on a separate tab.</td>
</tr>
</tbody>
</table>
| Table filtering  | When the number of rows exceeds the maximum number that fit into the display area, the SMS displays a vertical scroll bar and a magnifying glass icon. Click the magnifying glass icon (located above the scroll bar) to filter the table by matching text, and then click **Refresh**.  

**Note:** Filter criteria is not case sensitive. If the desired table entry has a label that contains a space, the space must be in the filter string, for example `disk/boot`. |
<p>| Expandable table columns | Certain table columns use a plus symbol (+) to indicate you can expand secondary, hidden columns. Click the (+) symbol to expand the columns; click the minus symbol (−) to collapse the heading again. |</p>
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table column controls</td>
<td>Click the drop-down arrow in a table column heading to display the following options:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Sorting</strong> — Sort the column on ascending or descending order, based on the column entry.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Aggregation</strong> — Summarize similar column entries.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Hide Column</strong> — Hide the selected column from your view.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Table Properties</strong> — Open a dialog that enables you to define the order, visibility, sort direction and order, and aggregation properties for the column. The Remember Table Settings option saves your preferences to the workstation you are using for the client session.</td>
</tr>
<tr>
<td>Realtime data</td>
<td>The SMS client provides the option to view realtime data on screens in the Events workspace and on screens that display statistics, such as the System Health Statistics and the Port Statistics in the Admin workspace.</td>
</tr>
<tr>
<td></td>
<td>To view realtime data from a historical graph, click the Realtime icon located below the associated graph. The Realtime Viewer opens, displaying the relevant realtime data. In the Realtime Viewer, you can select <strong>Pause</strong> to freeze and resume statistical polling. Use the <strong>Polling Interval</strong> drop-down menu to adjust the polling interval.</td>
</tr>
</tbody>
</table>
|                         | The Events workspace provides an option to view events in realtime:  
|                         | 1. Use query options to adjust your criteria.  
|                         | 2. Select the **Real-time** option above the results list.  
<p>|                         | 3. Click <strong>Refresh</strong> to filter events and show matching events in realtime.                                                               |
| Named resources         | The SMS uses <strong>named resources</strong> to enable the grouping and unique identification of resources that are referred to by various features in the SMS. You can create a named resource by right-clicking an IP address in a table column. For more information see <strong>Named resources</strong> on page 642. |
| IDResolver              | The SMS can be configured to retrieve user information from an A10 Networks appliance through an Internet Protocol to Identity service. This service provides information about a user based on a host association entry on the A10 appliance. |</p>
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>To configure integration between the SMS and an A10 Networks appliance, the location and login credentials of the A10 Networks appliance must be identified to the SMS server. The IDResolver service provides access to IP address information for A10 Networks.</td>
</tr>
<tr>
<td>Right-click menus</td>
<td>Right-click a selected entry to display a list of options. These options differ according to the workspace, screen, and the entry or object you select to display the menu.</td>
</tr>
</tbody>
</table>

**Manage your system**

To begin managing your TippingPoint devices on the SMS, complete the following tasks:

- *Adding, editing, or deleting a device* on page 327
- *Download and manage Digital Vaccine packages* on page 191

**View notifications**

The SMS displays notifications after you login. You can click the notifications icon (located on the bottom right corner in the SMS) to review the latest system notifications. System notifications include the date and time the notification was received, the source of the notification, such as the name of the device, and the system message.

Notifications might include the following:

- System Notification — Indicates that an event triggered a message.
- DV Notification — Indicates a new Digital Vaccine (DV) is available from the TMC, and provides options to download the DV.
- SMS Patch Notification — Indicates a new SMS patch is available from the TMC.

When reviewing the latest system notifications, you can:

- Click **Advanced** to configure how you receive notifications including the option to show notifications immediately or to view notifications in a dialog box.
- Select one or more notifications, and then click **View** to view the details of each selected notification in a dialog box.
- Click **Clear All** to remove all system notifications.
Software updates

When TippingPoint identifies new attacks or improves methods of detecting existing attacks, the TMC makes protection available in the form of TippingPoint Operating System (TOS) updates, Digital Vaccines (DV), and SMS software updates. These software updates improve the functionality and default filter signatures used to manage and protect your network security.

Install TOS updates

TOS provides updates for the operations and functions for your devices. Updates can improve the available functionality, behavior, and performance of these devices. For more information, see Importing and downloading the TOS on page 338.

Install SMS software updates

The General screen in the Admin workspace displays information for your SMS, including the current software version, installed patches, and software and patches available for download.

To help keep your network secure, make sure you have the latest patch for your SMS.

Note: You must download and activate the latest Digital Vaccine (DV) before you upgrade the SMS server for the first time. For more information see, Digital Vaccines on page 188.

Migrate to another SMS version

To migrate from one version of SMS to a new version, first create a backup of your current SMS (see Backup and restore on page 586), update the SMS software to the current release, and then install the new SMS client (see Install the SMS client on page 7).

Note: You should include event data when you backup your SMS prior to migrating to a new version.

For more information about migration issues, refer to the SMS Release Notes that are available through the TMC.

Digital Vaccines

Digital Vaccines contain newly developed filters as well as improvements to existing filters and new filter options investigated and distributed by the TMC. These packages are continually updated to fortify your system against new malicious attacks threatening hosts and network services.

If you use the SMS to manage your devices, we recommend that you also use the SMS to download and distribute software packages. If you download a Digital Vaccine to a device and not to the SMS, the SMS reports the events passed to it from the device, but it may not be able to identify the filters associated with those events.

You can distribute software packages as soon as you download them. However, it is likely that you will need to customize some of the filters contained in a new filter package. You might also need to add filters and
enable or edit anomalies. Customizations and additions you make in filters are bundled into a profile. Once you make these changes, you can distribute the profile to the appropriate devices.

You can import, download, distribute, activate, and manage Digital Vaccines (DVs), virtual TPS DVs, Auxiliary DVs, and DV Toolkit packages. For more information, see Digital Vaccines on page 188.
Tools

Tools provide quick and convenient access to a number of tools, utilities, and services that enable you to lookup information for source and destination addresses, diagnose and resolve issues, and help ensure the security of your network.

The tool utilities available through the SMS include:

**IP Lookup** on page 32 — The IP Lookup utility enables you to specify an IP address and query a variety of information about the host or domain, including geographical location, domain name server, and “who is” information.

**TMC** on page 33 — The Threat Management Center (TMC) is an TippingPoint service center that monitors sensors around the world for the latest attack information and builds and distributes attack filters. The TMC Web site also serves as a central repository for product documentation, FAQs, the TippingPoint Knowledge Base, and related information.

**ThreatLinQ** — ThreatLinQ works with the TMC to collect and analyze information about the security posture of the Internet. Globally aggregated information about filters, source IP addresses and source/destination ports is displayed and can be used to enhance the security of your network.

**Diagnostics** on page 34 — Use the SMS Diagnostic Toolkit in connection with TippingPoint support staff to help diagnose and resolve issues.

**IDResolver** on page 36 — The SMS can be configured to retrieve user information from an A10 Networks appliance through an Internet Protocol to Identity service.

IP Lookup

The IP Lookup utility enables you to specify an IP address and query a variety of information about the host or domain, including geographical location, domain name server, “who is” information, and so on.

Available lookup services include the following:

- **Geo Locator** — Performs a lookup in the Geo locator database. For more information about the Geo locator database, see Geo Locator database on page 652.

- **Named Resource** — Searches for an IP address in the list of named resources in the SMS. If found, the most specific match will be shown. For more information about named resources, see Named resources on page 642.

- **DNS** — Performs a reverse DNS lookup on the specified IP address.

- **User Id** — Performs a query for the address in the User ID database. If found, results show the user associated with the specified address.
• **Who Is** — Displays registration information, based on the American Registry for Internet Numbers (ARIN). Typical information includes that name and address of the entity that registered the domain.

• **Reputation** — Displays reputation properties for the IP address, based on entries in the reputation database. This service is available whether or not you have a subscription for ThreatDV.

• **End Point Attributes** — Displays the end point attributes associated with a specified IP address.

You can run these services manually from the SMS client, or you can configure the SMS to run many of these services automatically. See IP address identifier on page 646.

1. Select **Tools** > **IP Lookup**.

   **Note:** Select **Multiple Lookups** to use multiple lookup services for your query. Or you can manually select multiple lookup services in the IP Address/Host Lookup query window.

2. Enter an IP address or host name in the required field.

3. Click **Lookup**.

4. Click **Copy All to Clipboard** to copy the contents of the active tab to your clipboard, or click **Close** to close the query window.

As you review attack events, you may need to locate administrative contacts for domains.

The SMS provides a WhoIs utility for finding these contacts through the Events screen. The utility can run while you review events. In the Events workspace, right-click a table entry, and select **IP Lookup** > **WhoIs**, and then select the appropriate menu option for the address you want to lookup: **Src Addr**, **Client Addr**, or **Dst Addr**.

### TMC

The Threat Management Center (TMC) is a TippingPoint service center that monitors sensors around the world for the latest attack information and builds and distributes attack filters. The TMC website also serves as a central repository for product documentation, FAQs, the TippingPoint Knowledge Base, and related information.

1. In any screen, select **Tools** > **TMC** from the top menu bar.

2. From the TMC, click **Login**.

3. Log in to the TMC using your Trend Micro account and password.

### ThreatLinQ

ThreatLinQ works with the TMC to collect and analyze information about the security posture of the Internet. Globally aggregated information about filters, source IP addresses and source/destination ports is displayed and can be used to enhance the security of your network.
Data that ThreatLinQ collects could be sensitive, therefore the ThreatLinQ Event sharing option is not enabled in the default SMS configuration.

If you enable ThreatLinQ Event sharing, you have the option to hide all or some of the IP addresses in the data ThreatLinQ collects. The event sharing option also includes the hit count and filter number. For more information about the ThreatLinQ Event sharing option, see *TMC Information Share* on page 41.

When ThreatLinQ is enabled, the SMS uploads the aggregated events during the last calendar day. This shared data helps ThreatLinQ to provide a complete picture of world security and where the attacks originate.

On any screen, click **Tools** in the top menu bar, and select **ThreatLinQ**.

To access ThreatLinQ, do one of the following:

- On any screen, click **Tools** in the top menu bar, and select **ThreatLinQ**.
- **Events** - Right-click an events entry, and select **ThreatLinQ**.
- **Profiles** - Right-click an entry in one of the filter lists, and select **ThreatLinQ > Filter Info**.

## Diagnostics

Use the SMS Diagnostic Toolkit in connection with TippingPoint support staff to help diagnose and resolve issues. Available diagnostic tools include the following:

*Create a logs zip file* on page 34  
*Edit logging levels* on page 35  
*Install a hotfix* on page 35  
*Roll back to a previous software hotfix* on page 36  
*Generate bookmark string* on page 36  
*Look up users on LDAP* on page 36

### Create a logs zip file

The logs zip file is a collection of log-related attributes and can be used for troubleshooting. Before contacting support, remember to gather the log zip files.

1. Select **Tools > Diagnostics > Log Utils**.
2. Select a tab. There are two tabs: one for the SMS client logs, and one for the SMS server logs.
3. Click **Create Logs Zip File**, specify a location, and then enter a file name.
4. Click **Save**.
Edit logging levels

The log4j logger level can be changed for various logger names (log files).

1. Select **Tools > Diagnostics > Log Utils**.
2. Select a tab. There are two tabs: one for the SMS client loggers and one for the SMS server loggers.
3. Click **Edit Loggers**, select a logger name, and then specify a level.

**Table 10. Levels**

<table>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALL</td>
<td>Includes all levels.</td>
</tr>
<tr>
<td>TRACE</td>
<td>Designates more details than the DEBUG level.</td>
</tr>
<tr>
<td>DEBUG</td>
<td>Designates informational events useful to debug the log file.</td>
</tr>
<tr>
<td>INFO</td>
<td>Designates informational messages.</td>
</tr>
<tr>
<td>WARN</td>
<td>Designates potentially harmful situations.</td>
</tr>
<tr>
<td>ERROR</td>
<td>Designates errors that might still allow the application to continue running.</td>
</tr>
<tr>
<td>FATAL</td>
<td>Designates severe errors.</td>
</tr>
<tr>
<td>OFF</td>
<td>Turns off logging.</td>
</tr>
</tbody>
</table>

4. Click **OK**.

Install a hotfix

When improvements or additions are made to the SMS, TippingPoint releases a software update. When installing a hotfix, verify that the hotfix you download is not larger than the listed amount of free space.

1. Select **Tools > Diagnostics > Hotfixes**.
2. Click **Install** to install a single SMS software hotfix.
3. Click **Install Bulk > Add** to batch install multiple software hotfixes.
Roll back to a previous software hotfix

A rollback operation reverts the currently running software version on your SMS to a previous working version. The SMS retains the settings and configurations of your system. However, depending on the version you rollback to, not all functionality will be available.

1. Select **Tools** > **Diagnostics** > **Hotfixes**.
2. Select a hotfix from the list of installed hotfix entries, and then click **Rollback**.

Generate bookmark string

You can generate a bookmark string for use on the SMS client or the command line interface (CLI).

1. Select **Tools** > **Diagnostics** > **Bookmarks**.
2. Click **Generate Bookmark String**.
   
   The SMS automatically generates the string and updates the **For UITtestBaseBookmark** and **bookmark arg** fields.

Look up users on LDAP

If configured, you can look up a username and groups related to a user account that is authenticated against an LDAP server.

1. Select **Tools** > **Diagnostics** > **Users on LDAP**.
2. To configure the LDAP server, go to **Admin** > **Authentication** > **Active Directory**.

Configure, enable, and query IDResolver

The SMS can be configured to retrieve user information from an A10 Networks appliance through an Internet Protocol to Identity service. This service provides information about a user based on a host association entry on the A10 appliance.

To configure integration between the SMS and an A10 Networks appliance, the location and login credentials of the A10 Networks appliance must be identified to the SMS server. The IDResolver service provides access to IP address information for A10 Networks.

1. Select **Admin** > **Server Properties** > **Server Properties**.
2. Select the **Integration** tab.
3. Click **Edit**, and provide the following information:
   
   ◦ **Address** and **Port**.
   
   ◦ **User Name** and **Password**.
Select a value for **Password Encryption**.

Specify a numerical value for **Timeout**.

4. Click **OK**.

5. Click **Enable**.

### Query IDResolver

1. Select a table entry that displays an IP address that is part of an A10-managed network.

2. Right-click the entry, and select **Query IDResolver** from the list of options.

3. In the Query IDResolver dialog, select an entry in the Query Results table.
System preferences

Depending on your access and authorization level, you can configure the following system preferences:

- *Security* on page 38
- *TMC Information Share* on page 41
- *Device SNMP* on page 42
- *Device Communication* on page 43
- *Dashboard* on page 44
- *SSH client configuration* on page 45
- *Banner Message* on page 45
- *External Export* on page 46
- *Reports* on page 47

For details about user roles, see *Managing user roles* on page 558.

Security

1. Select **Edit > Preferences > Security**.

2. Specify level of security required when creating a user name and password. The default value is Medium. Options include the following.

<table>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 - None</td>
<td>• User names cannot contain spaces.</td>
</tr>
<tr>
<td></td>
<td>• Password length and complexity are not restricted.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: Do not use spaces in the password.</td>
</tr>
<tr>
<td>1 - Low</td>
<td>Passwords must meet Level 0 (None) restrictions and the following:</td>
</tr>
<tr>
<td></td>
<td>• User names must be at least six characters.</td>
</tr>
<tr>
<td></td>
<td>• Passwords must be at least eight characters.</td>
</tr>
<tr>
<td>Level</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| -     | • New password must be different from the previous password.  
| **Note:** Do not use spaces in the password. |
| 2 - Medium (default) | Passwords must meet Level 1 (Low) restrictions and the following:  
| • Must contain at least two alphabetic characters.  
| • Must contain at least one numeric characters.  
| • Must contain at least one non-alphanumeric character (examples include ! ? $ * #).  
| **Note:** Do not use spaces in the password. |
| 3 - High | Passwords must meet Level 2 (Medium) restrictions and the following:  
| • Must contain at least 15 characters.  
| • Must contain at least one uppercase character.  
| • Must contain at least one lowercase character.  
| • Must be different from the previous password in at least half of the corresponding character positions.  
| **Note:** Do not use spaces in the password. |

3. Select password preferences from the following options.

<table>
<thead>
<tr>
<th>Select:</th>
<th>To ...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Require password to be different from user ID</td>
<td>Determine whether the SMS allows a user to have a password that is the same as the user ID.</td>
</tr>
</tbody>
</table>
| Lock user after failed login attempts | Determine whether the SMS locks a user out after a specified number of unsuccessful login attempts.  
<p>| If this option is selected, enter a threshold to set the number of unsuccessful consecutive attempts a user can make before their account is locked out. |</p>
<table>
<thead>
<tr>
<th>Select:</th>
<th>To ...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Require new password to be different from previous passwords</td>
<td>Determine whether the SMS requires the new password to be different from previous passwords.</td>
</tr>
<tr>
<td></td>
<td>If this option is selected, enter the number of previous passwords the SMS will check, from 1-10.</td>
</tr>
<tr>
<td>Show previous login details when a user logs in</td>
<td>Determine whether the SMS displays the previous login details for the user.</td>
</tr>
<tr>
<td></td>
<td>If this option is selected, enter the number successful logins the SMS will count, from 1-30 days.</td>
</tr>
<tr>
<td></td>
<td>The SMS displays information for:</td>
</tr>
<tr>
<td></td>
<td>• Last successful login including date, timestamp, and IP address.</td>
</tr>
<tr>
<td></td>
<td>• Last failed login attempt including date, timestamp, and IP address.</td>
</tr>
<tr>
<td></td>
<td>• Number of failed login attempts since the last successful login.</td>
</tr>
<tr>
<td></td>
<td>• Any group or role changes to the user account since the last login.</td>
</tr>
<tr>
<td>Disable inactive user accounts</td>
<td>Determine whether the SMS disables inactive accounts.</td>
</tr>
<tr>
<td></td>
<td>If this option is selected, enter the number of days the user account must be inactive before it is disabled on the SMS.</td>
</tr>
<tr>
<td>Require user to re-authenticate</td>
<td>Determine whether the SMS requires the user to re-authenticate after a set number of time, from 8-48 hours.</td>
</tr>
<tr>
<td>Enforce a minimum password lifetime</td>
<td>Determine whether the SMS enforces the minimum password lifetime of 24 hours.</td>
</tr>
<tr>
<td></td>
<td>If this option is selected, the user will not be able to change the password again until the minimum time has passed.</td>
</tr>
<tr>
<td>4. Select <strong>Limit number of total and user sessions</strong> to determine whether the SMS limits the number of active sessions allowed on the SMS or for a user.</td>
<td></td>
</tr>
</tbody>
</table>
5. Select SMS client preferences from the following options.

<table>
<thead>
<tr>
<th>Select:</th>
<th>To ...</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Maximum number of active sessions allowed on the SMS</strong></td>
<td>Enter the maximum number of active sessions allowed on the SMS, from 1-50.</td>
</tr>
<tr>
<td><strong>Maximum number of active sessions allowed for a user</strong></td>
<td>Enter the maximum number of active sessions allowed for a user, from 1-10.</td>
</tr>
</tbody>
</table>

6. Click **OK**.

### TMC Information Share

1. Select **Edit > Preferences > TMC Information Share**.
2. Select from the following options.

<table>
<thead>
<tr>
<th>Select:</th>
<th>To ...</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enable update tracking on TMC</strong></td>
<td>The SMS sends information to the TMC including version, model, and managed device information.</td>
</tr>
<tr>
<td>Select:</td>
<td>To ...</td>
</tr>
<tr>
<td>--------</td>
<td>--------</td>
</tr>
<tr>
<td></td>
<td>If you select this check box, the SMS pushes additional information to the TMC including configuration metadata and which SMS features are being used.</td>
</tr>
<tr>
<td>Enable TMC Polling for DV, OS, and License Package updates</td>
<td>To enable the SMS client to periodically poll the TMC for updates.</td>
</tr>
<tr>
<td>Enable ThreatLinQ Event Sharing</td>
<td>To determine whether the SMS client can upload aggregated events to the TMC in an effort to collect and analyze the security posture of the Internet. If you enable this option, choose one of the following options:</td>
</tr>
<tr>
<td>Enable sharing CVE coverage gaps to help TippingPoint improve DV coverage</td>
<td>To enable the SMS to upload CVE IDs to the TMC. These include CVE IDs found in a vulnerability scan that are not yet associated to a filter. This helps the DV team prioritize which filters to include in the DV.</td>
</tr>
</tbody>
</table>

3. Click **OK**.

**Device SNMP**

The SMS uses SNMP to communicate with legacy devices.

1. Select **Edit > Preferences > Device SNMP**.
2. Configure device SNMP preferences from the following options.
Select this SNMP version:  

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>v2</td>
<td>Enable the SMS to communicate with managed devices using SNMPv2. If you select this option, enter and verify the SNMPv2 community.</td>
</tr>
<tr>
<td>v3</td>
<td>Enable the SMS to communicate with managed devices using SNMPv3. If you select this option, do the following: &lt;br&gt; a. Enter the user name. &lt;br&gt; b. Select an authentication protocol. &lt;br&gt; c. Enter and verify the key. &lt;br&gt; d. Select a privacy protocol.</td>
</tr>
<tr>
<td>Use SNMP v3 when possible</td>
<td>Enable the SMS to automatically use SNMPv3 to communicate with managed devices when possible.</td>
</tr>
</tbody>
</table>

3. Click OK.

**Device Communication**

Configure device communication preferences to specify the device communication and data retrieval settings. This is a periodic poll to see if the device is communicating with the SMS.

1. Select **Edit > Preferences > Device Communication**.

2. Select **Enable Device Communication Check** to enable the SMS to perform communication checks with managed devices. If selected, specify values for the following options.

<table>
<thead>
<tr>
<th>Select this communication preference:</th>
<th>To ...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failure threshold</td>
<td>Set the maximum number of failures, from 1-4, 5 (default), 10, or 20. &lt;br&gt; This only applies to IPS devices that are using SNMP traps to send alert logs.</td>
</tr>
</tbody>
</table>
Select this communication preference: | To ...
---|---
Comm check interval | Set the time between communication checks, from 20 or 30 seconds, or 1, 5, or 10 minutes. This does not apply to IPS devices using the Encrypted Alert Channel.

3. Specify **Data Retrieval Polling Intervals** from the following options.

<table>
<thead>
<tr>
<th>Interval</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device history stats</td>
<td>from 1-30 minutes</td>
</tr>
<tr>
<td>Device health and performance</td>
<td>from 1-30 minutes</td>
</tr>
<tr>
<td>Device port stats</td>
<td>from 1-30 minutes</td>
</tr>
<tr>
<td>SMS Health and performance</td>
<td>from 1-30 minutes</td>
</tr>
</tbody>
</table>

4. Click **OK**.

## Dashboard

You must have SuperUser permissions to configure dashboard preferences.

1. Select **Edit > Preferences > Dashboard**.

2. Select **Enable Dashboard** to determine whether the dashboard automatically displays when a user logs in to the SMS client. If disabled, a user can still access the dashboard (**View > Dashboard > View**), but the SMS will not update the dashboard information.

3. Select dashboard preferences from the following options.

| Select: | To ...
---|---
Dashboard Update Interval | Specify the time at which the dashboard is updated, from 5–60 minutes.
Font name | Specify the font used on all dashboard gadgets.
Select: | To ...
---|---
Font style | Specify the font style used on all dashboard gadgets, such as plain, bold, italic, or bold + italic.
Font size | Specify the font size used on all dashboard gadgets, from 5 to 24.

4. Click **OK**.
5. To restore the dashboard defaults, see XX.

**SSH client configuration**

Specify which external SSH client application to use for the SSH client terminal from the SMS client.

1. Select **Edit > Preferences > SSH Client Configuration**.
2. Click **Browse**, and choose the local program to use as the SSH client.
3. Click **OK**.

**Banner Message**

Configure banner messages to display security notices on the SMS client toolbar or when a user attempts to log in to the following interfaces: SMS client, web management console, command line interface (CLI), or remote SSH client.

1. Select **Edit > Preferences > Banner Message**.
2. Select **Enable Banner Message** to determine whether the banner message displays.
3. Select banner message preferences from the following options.

| Select: | To ...
---|---
Title | Enter a title, up to 1024 characters.
Message | Enter a message, up to 4000 characters.
Display on client toolbar | Display the banner title and message on the SMS toolbar (located to the right of the Admin).
<table>
<thead>
<tr>
<th>Select:</th>
<th>To ...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display on client login</td>
<td>Display the banner title and message on the SMS client login.</td>
</tr>
<tr>
<td>Display on web login</td>
<td>Display the banner title and message on the SMS web management console login page.</td>
</tr>
<tr>
<td>Display on console/CLI login</td>
<td>Display the banner title and message on the CLI console.</td>
</tr>
<tr>
<td>Display on remote/SSH login</td>
<td>Display the banner title and message on the remote SSH login.</td>
</tr>
</tbody>
</table>

4. Click **OK**.

## External Export

Configure PCAP download preferences to provide remote storage information (directory and server name) for packet capture (PCAP) files, which can then be viewed through the SMS client.

**Note:** The SMS retrieves the most recent PCAPs first and then works backward to retrieve older PCAPs. Newer PCAPs are downloaded by the SMS even if a device accumulates PCAPs at a rate faster than the SMS can retrieve them. If the SMS cannot retrieve all PCAPs from the device, the SMS generates a message in the system log.

Before configuring this information, make sure you have the following:

- User role that enables you to edit preferences. For more information, see *Administration* on page 532.
- Sufficient storage space for the PCAP files. (See *Packet trace* on page 74.)
- PCAP management application.

**Note:** Multiple SMS servers should NOT use the same remote destination to store PCAP files because file names are not unique across different SMS servers. If remote storage is full, an error message displays in the log file. You must manually clean up PCAP files.

1. Select **Edit > Preferences > External Export**.
2. Select an external source from the following options.
Select: | To ...
---|---
IPS | 
NFS | Enter the remote directory and server name.
SMB | Enter a username and password. You have the option to specify a **Domain** to access.

3. Click **OK**.

## Reports

Configure reporting extract, transform, and load (ETL) preferences to determine how often data is extracted from the database, transformed, and loaded on the SMS client and the Threat Insights Portal.

1. Select **Edit > Preferences > Reports**.
2. Specify a time interval (in minutes) for the SMS to run an ETL process.
3. Click **Run ETL Process Now** to run the ETL process immediately.
Dashboard

Use the dashboard to continuously display the information that is most important for monitoring your network. The SMS alerts you when there is an issue on your network. When you need to take action, you can drill down quickly to view the details of an alert.

Note: If you are logged in to multiple SMS servers, the client uses a tabbed view to display each SMS dashboard. Click a tab to display the dashboard for that particular SMS.

Dashboard palette

The dashboard palette is a collapsible toolbar with icons of the dashboard gadgets that are available to you. To open or collapse the palette area, click the Show Palette button (paint brush) in the dashboard toolbar.

Use the arrows at either end of the dashboard palette to scroll through the list of available gadgets.

You have the option to move the dashboard palette to the top, bottom, right, or left of the SMS Dashboard window. To change the location of the palette, click the Location button (compass needle) in the dashboard toolbar, and select an option.

For more information about adding gadgets to your dashboard, see Customize the SMS dashboard on page 55.

Default dashboard configuration

The SMS dashboard is configured with several gadgets. You can customize the existing gadgets or add additional gadgets to display the information that you need to monitor. By default, the dashboard contains the following gadgets:

- Top 5 Attacks (Last Hour)
- Top 5 Applications (Last Hour)
- Attacks (Last 24 Hours)
- Application Events (Last 24 Hours)
- Top 5 Attack Destinations (Last Hour)
- Top 5 Application Destinations (Last Hour)
- Top 5 App Users (Last Hour)
- Top 5 Attack Users (Last Hour)
- Device Health
- Device Status
• SMS Health
• SMS Client Health
• Distribution Status
• Top 5 Attack Geographic Sources (Last Hour)

See Customize the SMS dashboard on page 55 for information on how to customize your dashboard and Dashboard gadgets on page 49 for an overview of available gadgets.

Dashboard gadgets

The SMS dashboard provides you with configurable gadgets that enable you to view, monitor, and analyze health, status, and events at system and device levels. You can choose the gadgets that are displayed on your dashboard as well as the look and feel of the dashboard itself. Gadgets are categorized into:

• Health and Status gadgets on page 49 — System health and status of managed devices
• Task Status gadgets on page 50 — Distribution status and software update status
• Inspection Event gadgets on page 51 — Information about events that trigger security or application filters on your system, as well as trends such as the top events and top events by IP address or geographic location
  ◦ Event Rate gadget on page 51 — Overall number of filter-triggered events that the SMS is processing over a specified period of time.
  ◦ Security gadgets on page 51 — Information based on SMS Security filters, and can display various aspects of related events including number of instances, IP addresses, and geographic locations.
  ◦ Reputation gadgets on page 52 — Information based on the security filters and are further refined by the Reputation filter category.
  ◦ Application gadgets on page 52 — Information based on application filters and can display various aspects of related events including number of instances, IP addresses, and geographic locations.
  ◦ User gadgets on page 54 — Information based on user and user group query criteria including login names, and source and destination IP addresses of domains and machines.
• Firewall gadgets on page 54 — Information based on firewall policy criteria and can display various aspects of related events including number of instances, IP addresses, and geographic locations.

Health and Status gadgets

Health and Status gadgets monitor characteristics of system health and report on the basic health and status of managed devices. These dashboard gadgets provide a high-level warning system for potential health and performance problems with your system and devices. Main focal points of the Health and Status gadgets include:
• System Health — SMS health status for CPU, memory, temperature, file system, and system log. Select gadget to display the General – System Health screen

• SMS Client Health — Health of the SMS client memory and CPU usage.

• Device Health — Number of devices in each condition of system health:
  ◦ Green – Normal
  ◦ Yellow – Major
  ◦ Red – Critical

Depending on gadget options, health status might include system health, performance, and port health. Click a device to display the Device Details screen in the Devices workspace.

• Device Status – Number of devices in a particular state:
  ◦ Managed
  ◦ Unmanaged
  ◦ Updating
  ◦ Fallback Mode
  ◦ Non-communicating
  ◦ Rebooting

Click on the device to display the Devices screen in the Devices workspace.

**Note:** Device Health and Status gadgets display the number of devices in a condition or state, not the number of health events or device health items.

### Task Status gadgets

The dashboard provides two gadgets that report the status for particular tasks:

• **Distribution Status** shows the status of the most recent profile and Digital Vaccine (DV) distributions. You can specify how many status entries to show for each distribution category:
  ◦ Inspection Profile
  ◦ Firewall Profile
  ◦ Digital Vaccine
  ◦ Reputation

• **Software Update Status** shows the current (active) and available TippingPoint software versions, including SMS software, SMS patches, Digital Vaccines, and TOS software.
Click anywhere in the Software Update gadget to display the Admin (General) workspace in the SMS client.

**Inspection Event gadgets**

The dashboard includes many gadgets you can use to analyze inspection events that occur on your system. These gadgets provide information about events that trigger security or application filters on your system, as well as trends such as the top events and top events by IP address or geographic location.

**Event Rate gadget**

The **Event Rate** gadget shows the overall number of filter-triggered events that the SMS is processing over a specified period of time. This gadget displays the time period and total number of events, and it shows the breakdown of events by device for a number of top devices.

Configurable options for the Event Rate gadget include the time period by which events are measured, the number of top devices for which to display statistics (1–100), and the option to include all managed devices or selected devices.

Click anywhere in this gadget to display the Devices workspace in the SMS client.

**Security gadgets**

Security gadgets display information based on SMS Security filters, and can display various aspects of related events including number of instances, IP addresses, and geographic locations.

With the exception of the Geographic gadgets, you can click a Security gadget to open the SMS client to the Events screen. If you click a specific entry in a pie chart, bar chart, or table, the Events screen displays events according to the filter and criteria selected.

The following table provides a description of each dashboard Security gadget.

**Table 11. Security gadgets**

<table>
<thead>
<tr>
<th>Security gadget</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attacks</td>
<td>Number of attacks observed over a specific period of time, based on the Security filter type. You can specify the Time Period in the gadget options. Click in this gadget to display Security events in the SMS client.</td>
</tr>
<tr>
<td>Top Attack Destinations</td>
<td>Top attack destination IP addresses displayed in table, bar graph, or pie chart format, and sorted by hit count. In addition to Event Criteria, you can configure the Time Period, the number of top events to display, and the chart type. Click an entry in this gadget to display the filter events in the SMS client.</td>
</tr>
<tr>
<td>Security gadget</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Top Attack Geographic Destinations</td>
<td>Map or table view of the top geography (city, region, country) based on top hit count for destination IP addresses in attack events. In addition to Event Criteria, you can configure the Time Period, the number of top events to display, and whether to display information in a map or a table.</td>
</tr>
<tr>
<td>Top Attack Geographic Sources</td>
<td>Map or table view of the top geography (city, region, country) based on top hit count for source IP addresses in attack events. In addition to Event Criteria, you can configure the Time Period, the number of top events to display, and whether to display information in a map or a table.</td>
</tr>
<tr>
<td>Top Attack Sources</td>
<td>Top attack source IP addresses displayed in table, bar graph, or pie chart format, and sorted by hit count. In addition to Event Criteria, you can configure the Time Period, the number of top events to display, and the chart type. Click an entry in this gadget to display the filter events in the SMS client.</td>
</tr>
<tr>
<td>Top Attacks</td>
<td>Top attacks displayed in table, bar graph, or pie chart format, and sorted by hit count. In addition to Event Criteria, you can configure the Time Period, the number of top events to display, and the chart type. Click an entry in this gadget to display security events in the SMS client.</td>
</tr>
</tbody>
</table>

**Reputation gadgets**

Reputation gadgets are based on the Security filter type, but are further refined by the Reputation filter category. The SMS dashboard includes the following Reputation gadgets:

- **Top Reputation DNS Names** – Displays the top reputation DNS name hits as a table, bar graph, or pie chart sorted by hit count. You can select the Time Period, modify event criteria, specify the number of addresses to display (1–10), and choose the type of chart to use for display in the gadget options.

- **Top Reputation IP Addresses** – Displays the top reputation IP Address hits as a table, bar graph, or pie chart sorted by hit count. You can select the Time Period, modify event criteria, specify the number of addresses to display (1–10), and choose the type of chart to use for display in the gadget options.

**Application gadgets**

Application gadgets display information based on application filters, and can display various aspects of related events including number of instances, IP addresses, and geographic locations.

The following table provides a description of dashboard application gadgets.
<table>
<thead>
<tr>
<th>Application gadget</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Events</td>
<td>Number of application events observed over a specific period of time, based on the Application filter type. You can specify the Time Period in the gadget options. Click in this gadget to display Application events in the SMS client.</td>
</tr>
<tr>
<td>Top Application Destinations</td>
<td>Top application destination IP addresses displayed in table, bar graph, or pie chart format, and sorted by hit count. In addition to Event Criteria, you can configure the Time Period, the number of top events to display, and the chart type. Click an entry in this gadget to display the filter events in the SMS client.</td>
</tr>
<tr>
<td>Top Application Geographic Destinations</td>
<td>Map or table view of the top geography (city, region, country) based on top hit count for destination IP addresses in application events. In addition to Event Criteria, you can configure the Time Period, the number of top events to display, and whether to display information in a map or a table.</td>
</tr>
<tr>
<td>Top Application Geographic Sources</td>
<td>Map or table view of the top geography (city, region, country) based on top hit count for source IP addresses in application events. In addition to Event Criteria, you can configure the Time Period, the number of top events to display, and whether to display information in a map or a table.</td>
</tr>
<tr>
<td>Top Application Sources</td>
<td>Top application source IP addresses displayed in table, bar graph, or pie chart format, and sorted by hit count. In addition to Event Criteria, you can configure the Time Period, the number of top events to display, and the chart type. Click an entry in this gadget to display the filter events in the SMS client.</td>
</tr>
<tr>
<td>Top Applications</td>
<td>Top applications displayed in table, bar graph, or pie chart format, and sorted by hit count. In addition to Event Criteria, you can configure the Time Period, the number of top events to display, and the chart type. Click an entry in this gadget to display application events in the SMS client.</td>
</tr>
</tbody>
</table>
User gadgets

The SMS dashboard includes two gadgets that you can use to monitor Active Directory information, such as user and user group query criteria, login names, and source and destination IP addresses of domains and machines. From the dashboard, you can also access the User Info Criteria on page 82.

The following table provides a description of dashboard user gadgets.

Table 13. User gadgets

<table>
<thead>
<tr>
<th>User gadget</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top App Users</td>
<td>Top user login IDs in an application displayed in table, bar graph, or pie chart format, and sorted by hit count. In addition to Event Criteria, you can configure the Time Period, the number of top events to display, and the chart type. Click an entry in this gadget to display the filter events in the SMS client.</td>
</tr>
<tr>
<td>Top Attack Users</td>
<td>Top user login IDs in Security displayed in table, bar graph, or pie chart format, and sorted by hit count. In addition to Event Criteria, you can configure the Time Period, the number of top events to display, and the chart type. Click an entry in this gadget to display security events in the SMS client.</td>
</tr>
</tbody>
</table>

Firewall gadgets

Firewall gadgets display information based on Firewall Policy Criteria, and can display various aspects of related events including number of instances, IP addresses, and geographic locations.

The following table provides a description of dashboard Firewall gadgets.

Table 14. Firewall gadgets

<table>
<thead>
<tr>
<th>Firewall gadget</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top Applications by Bandwidth</td>
<td>Top applications by bandwidth displayed in table, bar graph, or pie chart format, and sorted by bandwidth. When displayed as bar or stacking bar format, the graph plots inbound and outbound traffic. When displayed in pie chart format, this gadget displays total bandwidth. In addition to Event Criteria, you can configure the Time Period, the number of top events to display, and the chart type.</td>
</tr>
<tr>
<td>Firewall gadget</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Top Applications by Hit Count</td>
<td>Top applications displayed in table, bar graph, or pie chart format, and sorted by hit count. In addition to Event Criteria, you can configure the Time Period, the number of top events to display, and the chart type.</td>
</tr>
<tr>
<td>Top Blocked Applications</td>
<td>Top blocked applications displayed in table, bar graph, or pie chart format, and sorted by hit count. In addition to Event Criteria, you can configure the Time Period, the number of top events to display, and the chart type.</td>
</tr>
<tr>
<td>Top IPs by Bandwidth</td>
<td>Top bandwidth by IP address displayed in table, bar graph, or pie chart format, and sorted by bandwidth. When displayed as bar or stacking bar format, the graph plots inbound and outbound traffic. When displayed in pie chart format, this gadget displays total bandwidth. In addition to Event Criteria, you can configure the Time Period, the number of top events to display, and the chart type.</td>
</tr>
<tr>
<td>Top Rules by Bandwidth</td>
<td>Top utilized rules by bandwidth displayed in table, bar graph, or pie chart format, and sorted by bandwidth. When displayed as bar or stacking bar format, the graph plots inbound and outbound traffic. When displayed in pie chart format, this gadget displays total bandwidth. In addition to Event Criteria, you can configure the Time Period, the number of top events to display, and the chart type.</td>
</tr>
<tr>
<td>Top Rules by Hit Count</td>
<td>Top utilized rules by hit count displayed in table, bar graph, or pie chart format, and sorted by hit count. In addition to Event Criteria, you can configure the Time Period, the number of top events to display, and the chart type.</td>
</tr>
<tr>
<td>Top Users by Bandwidth</td>
<td>Top bandwidth by user displayed in table, bar graph, or pie chart format, and sorted by bandwidth. When displayed as bar or stacking bar format, the graph plots inbound and outbound traffic. When displayed in pie chart format, this gadget displays total bandwidth. In addition to Event Criteria, you can configure the Time Period, the number of top events to display, and the chart type.</td>
</tr>
</tbody>
</table>

**Customize the SMS dashboard**

Customize your dashboard to provide the information you need to monitor for issues and react quickly:
• **Select a dashboard theme** on page 56 – Select the color and contrast of the visual elements of the dashboard

• **Change the dashboard layout** on page 56 – Change the column widths or move gadgets around

• **Add or remove a gadget** on page 56 – Choose which gadget you want to see on the dashboard

• **Configure a gadget** on page 57 – Change the gadget to show items

**Note:** Changes to the dashboard are linked to user accounts. Other users will not be able to view your dashboard changes.

---

**Select a dashboard theme**

Dashboard theme determines the color and contrast of the visual elements in your dashboard.

To change your dashboard theme, click the **Select Theme** button (picture) on the dashboard toolbar, and select a color scheme. Changes apply immediately to your dashboard.

---

**Change the dashboard layout**

The dashboard displays gadgets in three adjustable columns. To adjust column width, select a column divider and drag it left or right.

To move a gadget up, down, or across columns, clicking the gadget and then drag and drop it to its new location on the dashboard.

You can minimize a gadget, or maximize it to the full size of the dashboard screen:

- To minimize a gadget, click the gadget title bar once. Click the title bar again to return the gadget to its usual size.

- To maximize a gadget to the full size of the dashboard screen, double-click the gadget title bar. Double-click the title bar again to return the gadget to its usual size.

---

**Restore dashboard defaults**

Click **Restore Defaults** (360° arrow) to remove all customizations to the dashboard. This removes all gadgets added that are not part of the default configuration. It also removes any customizations made to the gadgets included in the default configuration.

---

**Add or remove a gadget**

All of the dashboard gadgets can be found on the Dashboard Palette. You have the option to move the dashboard palette to the top, bottom, right, or left of the SMS Dashboard window. To change the location of the palette, click the **Location** button (compass needle) in the dashboard toolbar, and select top, bottom, right, or left.
1. Click the **Show Palette** button (paint brush) in the top right hand corner of the dashboard. To change the location of the palette, click the **Location** button (compass needle) in the dashboard toolbar, and select top, bottom, right, or left.

2. Hover over the palette and use the scroll button on your mouse to scroll through the available gadgets. See *Dashboard gadgets* on page 49 for information on the different types of gadgets available.

3. Either double-click or drag and drop the gadget from the dashboard palette to the display area.

4. To remove a gadget from your dashboard, hover the mouse over the gadget title and click the close button in the top-right corner of the gadget.

### Configure a gadget

1. Hover the mouse over the top right of the gadget title bar to display the configuration tools.

2. Click the **Configure** button (wrench) to display configuration options.

3. In the Options wizard, select a category in the navigation pane to display related options. Depending on the gadget, option categories might include:
   - **General** – Change the title and other general settings, such as time period. Description is a read-only field.
   - **Event Criteria** – Change what the events the gadget will track, such as filter criteria, filter taxonomy criteria, device or segment criteria. You can also build a custom query. For background information about editing Event Criteria, see *Create an inspection query with filter criteria* on page 79
   - **Display** – Choose how you want the information displayed. Some options are Top N Events or whether you want it to be a bar char, pie chart, or a table.

4. Use controls on each screen to configure the gadget.

5. Click **OK** to save your changes and close the Options wizard.
Events

As the SMS responds to traffic triggered by the events and filters defined in your profile action sets and inspection profiles, data is logged in the SMS database.

To open the Events workspace, click Events on the SMS toolbar. The Events workspace includes three main events tables; each is described in detail below.

Inspection events on page 59 — Filter, view, and save inspection events for all or specific devices, segment groups, and event filter elements.

Firewall events on page 61 — Filter, view, and save firewall rule hit events detected by the Firewall for all or specific devices, interfaces, zones, and rule filter elements.

Monitor events on page 64 — When you access a table, it appears with a variety of criteria panels at the top of the screen. By using the criteria panels, you can look at your data from multiple angles.

Saving queries on page 77 — You can save, run, and manage queries through the Events screen. Saved queries display in the Saved Queries sections under Inspection Events and Firewall Events in the navigation screen.

URL Threat Analysis on page 89 — Configure URL Threat Analysis to send inspection event URLs from the SMS to the DD Analyzer device for analysis.

Note: When SuperUser or Admin User access or authority is specified, the user must have the respective SuperUser or Admin capabilities. See Authentication and authorization on page 542.

Navigate the Events workspace

From the Events workspace, you can do the following:

• Create, run, and save queries regarding events against the alert logs of the TippingPoint system. The SMS provides export functionality to save the results to a comma- or tab-delimited file.

• View event details, such as the contents of packets that comprised that event and information identifying where the event originated from including the geographic location.

• Export event data to an external file and generate reports. This aids with diagnostics, and you can export event data to an external file and generate event reports.

Note: The time displayed in the Time column for events reflects the time of the actual event on the detection device. This might not correspond to the SMS Receipt Time or the Device Log Time reported in the Event Details dialog. The differences might depend on the timekeeping configuration of the systems and on the speed of the network.
**Inspection events**

The SMS includes different types of Inspection events: Quarantine, Rate Limit, and Reputation events, which also includes the geographic location information for an IP address.

For Inspection events, pre-defined event queries are available for browsing the event log. Pre-defined views include Quarantine, Reputation, and Rate Limit. For these pre-defined queries, the columns and selection criteria are already customized appropriately for the corresponding view.

To access the pre-defined queries, expand the Inspection events entry in the left navigational menu and select one of the following listings:

- Quarantine events
- Rate Limit events
- Reputation events

For information about how you can query for events with a stack of devices, see *Events and reports* on page 529.

**Criteria panels**

You can refresh inspection events based on the following criteria panels:

- Filter Criteria
- Filter Taxonomy Criteria
- Network Criteria
- User Info Criteria
- Device, Segment, Rule Criteria
- Event Criteria

For more information about the criteria panels, see *Create an inspection query with filter criteria* on page 79.

**Inspection Events table**

The following table describes the columns in the Inspection Events table.
<table>
<thead>
<tr>
<th><strong>Column</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Time</td>
<td>Date and time that the event was processed by the inspection.</td>
</tr>
<tr>
<td>Severity</td>
<td>Indicates the importance of the event.</td>
</tr>
<tr>
<td>Name</td>
<td>Name of the filter that generated the alert or block.</td>
</tr>
<tr>
<td>Category</td>
<td>Type of event filter.</td>
</tr>
<tr>
<td>Action</td>
<td>Type of action for the filter.</td>
</tr>
<tr>
<td>Hit Count</td>
<td>Number of times there was a filter match.</td>
</tr>
<tr>
<td>Profile</td>
<td>Profile associated with the alert or block.</td>
</tr>
<tr>
<td>Device</td>
<td>Name of the device responding to the traffic.</td>
</tr>
<tr>
<td>Segment/Rule</td>
<td>Segment for IPS-generated events, and rules for firewall-generated inspection events.</td>
</tr>
<tr>
<td>Src. Addr.</td>
<td>Source IP address of the traffic that caused the event. Expand this column for location details, including geography map, region, city, and named resource.</td>
</tr>
<tr>
<td>Src. Port</td>
<td>Port of the source IP address.</td>
</tr>
<tr>
<td>Src. User</td>
<td>Login name of the source user.</td>
</tr>
<tr>
<td>Client Addr.</td>
<td>The IP address of the attacking client. Expand this column for location details, including geography map, region, city, and named resource.</td>
</tr>
<tr>
<td>Column</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Dst. Addr.</td>
<td>Destination IP address of the system at which the event was targeted. Expand this column for location details, including geography map, region, city, and named resource.</td>
</tr>
<tr>
<td>Dst. Port</td>
<td>Port of the destination IP address.</td>
</tr>
<tr>
<td>Dst. User</td>
<td>Login name of the destination user.</td>
</tr>
<tr>
<td>Seg</td>
<td>Number of the segment.</td>
</tr>
<tr>
<td>VLAN</td>
<td>VLAN on which the event took place.</td>
</tr>
<tr>
<td>Trace</td>
<td>Indicates if the event has a packet trace (or saved portion of the packet used in the event).</td>
</tr>
<tr>
<td>SSL Inspect</td>
<td>Indicates whether the event was part of an SSL session.</td>
</tr>
<tr>
<td>HTTP Hostname</td>
<td>Indicates whether there is an HTTP URI associated with the event and identifies the hostname. URI information displays in the Permit, Block, Rate Limit, and Trust logs.</td>
</tr>
<tr>
<td>Comment</td>
<td>Information added by the user.</td>
</tr>
</tbody>
</table>

**Firewall events**

To view the details about an event, you need to locate the event and display it. Each entry includes information on the device and issues of the triggered event.

For inspection and firewall events, you can also view and save the packet trace for an event if the filter triggering the event has a packet trace option set. See *View the packet trace* on page 75.

The following table describes the columns in the Firewall Events table.
Table 16. Firewall Events

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time</td>
<td>Date and time that the event was processed.</td>
</tr>
<tr>
<td>Event Type</td>
<td>Type of Event.</td>
</tr>
<tr>
<td>Hit Count</td>
<td>Number of times the event was triggered.</td>
</tr>
<tr>
<td>Src. Addr.</td>
<td>Source IP address of the system that sent the event. Expand this column for location details, including geography map, region, city, and named resource.</td>
</tr>
<tr>
<td>Src. Port</td>
<td>Source port of the source IP address.</td>
</tr>
<tr>
<td>Src. NAT</td>
<td>Source NAT address of the system that sent the event. Expand this column for location details, including geography map, region, city, and named resource.</td>
</tr>
<tr>
<td>Src. NAT Port</td>
<td>Source port of the NAT address.</td>
</tr>
<tr>
<td>Interface In</td>
<td>Interface where the event entered.</td>
</tr>
<tr>
<td>Src. Zone</td>
<td>The source zone where the source originated.</td>
</tr>
<tr>
<td>Dst. Addr.</td>
<td>Destination IP address of the system targeted in the attach. Expand this column for location details, including geography map, region, city, and named resource.</td>
</tr>
<tr>
<td>Dst. Port</td>
<td>Destination port of the destination IP address.</td>
</tr>
<tr>
<td>Dst. NAT</td>
<td>Destination NAT address of the system targeted in the event. Expand this column for location details, including geography map, region, city, and named resource.</td>
</tr>
<tr>
<td>Dst. NAT Port</td>
<td>Destination port of the Destination NAT.</td>
</tr>
<tr>
<td>Column</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Interface Out</td>
<td>Outbound Interface.</td>
</tr>
<tr>
<td>Dst. Zone</td>
<td>Destination zone of the event.</td>
</tr>
<tr>
<td>User Name</td>
<td>The user name of the account involved.</td>
</tr>
<tr>
<td>Application</td>
<td>The application that is implicated in the event. If you expand this column, you can view additional data including Transaction, Category, and Vendor. This data is derived directly from the digital vaccine.</td>
</tr>
<tr>
<td>Transport Protocol</td>
<td>Actual protocol as reported by the firewall.</td>
</tr>
<tr>
<td>Action</td>
<td>Type of action for the filter.</td>
</tr>
<tr>
<td>Total Byte</td>
<td>Total number of bytes.</td>
</tr>
<tr>
<td>Profile</td>
<td>Firewall profile associated with firewall rules.</td>
</tr>
<tr>
<td>Device</td>
<td>Name of the device responding to the traffic.</td>
</tr>
<tr>
<td>Firewall Rule</td>
<td>The specific firewall rule that was triggered.</td>
</tr>
<tr>
<td>Session ID</td>
<td>The session ID in which the event occurred.</td>
</tr>
<tr>
<td>Trace</td>
<td>Indicates if the events has a packet trace (or saved portion of the packet used in the event).</td>
</tr>
<tr>
<td>Comment</td>
<td>Information added by the user.</td>
</tr>
</tbody>
</table>

**SSL Inspection Logs**

To view logging information about SSL inspection, choose **Events > SSL Inspection Logs.**
The SSL Inspection log displays SSL session information for the SSL servers with logging enabled, including information about SSL sessions that failed to negotiate SSL parameters. Note that by default, when you add an SSL server, logging is disabled. The SSL inspection log does not contain SSL system errors; check the System log.

For more information, see SSL inspection on page 658.

Monitor events

When you access a table, it appears with a variety of criteria panels at the top of the screen. By using the criteria panels, you can look at your data from multiple angles. The available criteria panels depend on the type of table that you select. The Events viewer in the SMS is broken up into two parts:

- **Criteria panels.** This section is at the top of the screen, and you can use it to filter the table. Click the arrow on the left side of the event table name, and use the criteria panels to limit the results of your table.

- **Events table.** This section shows the table that displays the results of your search criteria, and you can open an event from the table. By default, new events appear at the top of the table. The initial view of certain segment and device tables are empty and have the option to customize the table listing by adding list items using the Add option. You can also use the table to define the order, visibility, sorting, and aggregation properties of each column.

**Tip:** Click a column heading to quickly re-sort the table by the selected column. Rearrange the order of the columns by clicking on a column heading and dragging the column. Right-clicking an event gives you access to the Table Properties option which provides a central location for customizing all column listings.

Monitor inspection or firewall events

1. On the navigation pane for the Events workspace, expand **Inspection Events** or **Firewall Events**, and then select an event.

   The Events screen for the selected inspection or firewall event opens.

2. Use the criteria filters to limit results on your table.

   The standard filters will vary based on the event you chose. The criteria panel displays any applied filters in italics on the title bar of the criteria panel.

   If you have inspection or firewall events with advanced filters, you can easily reset the filters to expand the results. To the right of a criteria panel, click **Reset** to remove a filter. Click **Reset All** to quickly clear all filters and re-populate the Events table.

3. (Optional) Select a time range from the following:
   
   - Real-time.
• Prescribed time interval (last X minutes, hours, days, or month).

• User Defined start and end time range — Type in the field or click the calendar to select a date.

4. Click **Refresh** to apply your selected filters. The table reappears based on the filters you defined.

   **Note:** The time required to process an event query varies, as many variables affect the amount of time needed for an event query to process including the time range, the number or type of search criteria, and the number of events accumulated within the time range.

5. If you ultimately want to save the event as a custom query, click **Save As**, and then save the query as usual.

**Right-click options from the events table**

To easily manage your events monitoring and filter tuning activities, the SMS provides quick right-click access to many cross-functional tasks.

**Table 17. Right-click options for events**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Copy</strong></td>
<td>Provides the following options for copying data:</td>
</tr>
<tr>
<td></td>
<td>• Selected Rows — Copies the selected rows. Use the Shift key to select multiple rows or the Ctrl key to select specific rows.</td>
</tr>
<tr>
<td></td>
<td>• Cell Value — Copies the cell content data, such as an event name or IP address.</td>
</tr>
<tr>
<td><strong>Export to File</strong></td>
<td>Exports selected rows or all rows to a delimited text file.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Selected Rows</strong> — Exports the selected rows. Use the Shift key to select multiple rows or the <strong>Ctrl</strong> key to select specific rows.</td>
</tr>
<tr>
<td></td>
<td>• <strong>All rows</strong> — Copies all currently viewed rows.</td>
</tr>
<tr>
<td><strong>Find</strong></td>
<td>Allows you to find a term or times listed in the table.</td>
</tr>
<tr>
<td><strong>Details</strong></td>
<td>Opens the Event Details window displaying the details of the event. The comment field allows you to add comments to the event. There is also an option copy the details to the clipboard.</td>
</tr>
<tr>
<td><strong>Event Comment</strong></td>
<td>Adds annotation to event listing.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Search on</td>
<td>Allows you to search all results based on the column heading for the selected event. For example, you can search for all events with the same Source Address as the selected event.</td>
</tr>
<tr>
<td>ThreatLinQ</td>
<td>Displays globally aggregated information about filters, source IP addresses, and source/destination ports.</td>
</tr>
<tr>
<td>Packet Trace</td>
<td>Provides the following Packet Trace options:</td>
</tr>
<tr>
<td></td>
<td>• View</td>
</tr>
<tr>
<td></td>
<td>• Save</td>
</tr>
<tr>
<td></td>
<td>• Download to the SMS</td>
</tr>
<tr>
<td></td>
<td>• Configure View Settings</td>
</tr>
<tr>
<td>IP Addr ID</td>
<td>Allows you to configure the ID for the IP address or edit the IP address by opening the New/Edit IP Addr ID Entry window.</td>
</tr>
<tr>
<td>Config</td>
<td></td>
</tr>
<tr>
<td>Reputation</td>
<td>For both Inspection and Firewall events you can create any number of reputation entries based on the source or destination address. For Inspection events, you also have the option of disputing the entry or creating an exception. Inspection events also allow you to use the event criteria to search in the Reputation Database.</td>
</tr>
<tr>
<td>New Traffic</td>
<td>(Inspection Events only) Create a new traffic capture for a segment on the device.</td>
</tr>
<tr>
<td>Capture</td>
<td></td>
</tr>
<tr>
<td>Reports</td>
<td>(Inspection Events only) Provides the following report options:</td>
</tr>
<tr>
<td></td>
<td>• Specific Filter Report</td>
</tr>
<tr>
<td></td>
<td>• Specific Source Report</td>
</tr>
<tr>
<td></td>
<td>• Specific Destination Report</td>
</tr>
<tr>
<td></td>
<td>• Specific User Report</td>
</tr>
<tr>
<td></td>
<td>• Specific Peer Report (Src. Addr.)</td>
</tr>
<tr>
<td></td>
<td>• Specific Peer Report (Dst. Addr.)</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Profile</td>
<td>(Inspection Events only) Allows you to edit filters, create exceptions, or create a Traffic Management filter.</td>
</tr>
<tr>
<td>Firewall Rule</td>
<td>(Firewall only) Select this option to edit the firewall rule based on the event. You can also easily include or exclude the event from the firewall rule.</td>
</tr>
<tr>
<td>Show Inspection</td>
<td>(Firewall only) Filter the Inspection Events table based on firewall event data for the following:</td>
</tr>
<tr>
<td>Show Inspection</td>
<td>• Source Address</td>
</tr>
<tr>
<td>Events</td>
<td>• Destination Address</td>
</tr>
<tr>
<td></td>
<td>• Firewall Rule</td>
</tr>
<tr>
<td></td>
<td>• Session ID</td>
</tr>
<tr>
<td>IP Lookup</td>
<td>• Geo Locator</td>
</tr>
<tr>
<td></td>
<td>• Named Resource</td>
</tr>
<tr>
<td></td>
<td>• DNS</td>
</tr>
<tr>
<td></td>
<td>• User ID</td>
</tr>
<tr>
<td></td>
<td>• Who is</td>
</tr>
<tr>
<td></td>
<td>• Reputation</td>
</tr>
<tr>
<td></td>
<td>• End Point Attributes</td>
</tr>
<tr>
<td></td>
<td>• Multiple Lookups</td>
</tr>
<tr>
<td>Create Response</td>
<td>Create a manual response based on Source Address, Source NAT, Destination Source, and Destination NAT.</td>
</tr>
<tr>
<td>Query</td>
<td>Provides access to IP address information for A10 Networks.</td>
</tr>
<tr>
<td>IDResolver</td>
<td></td>
</tr>
<tr>
<td>Create Named</td>
<td>Create a named source based on Source Address, Source NAT, Destination Source, and Destination NAT.</td>
</tr>
<tr>
<td>Source</td>
<td></td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Table Properties</td>
<td>Allows you to define the order, visibility, sorting, and aggregation properties of each column in your table.</td>
</tr>
</tbody>
</table>

**Customizing display options**

As events occur, the system compiles event information into the system log. By entering a query, you can display events according to criteria such as by device, event type, and severity. By default, new rows appear at the top of the events pane as the system identifies and responds to packets that match event filters.

After entering a search query, a list of matching events display in the Events table. You can modify the list of entries by using the display options and sorting. The display options allow you to select between real-time mode and a set range of time. Entries display according to the dating setting. You can also click the table column heading to sort in ascending and descending order.

**Note:** Users have access to events if they have access to either the device or the segment group.

**Events display**

The Events screen enables you to monitor events in real time. By default, events are shown for the last 15 minutes. As traffic moves through your network, new events appear at the top of the Events table. You can use the scroll bar on the right side of the table to view hidden information. At the top of the Events table, click the Real-time (running) radio button to turn on real-time mode.

Customize the time period for displaying events by selecting increments from the drop down or click on the calendar icon to the right of the time control, and use the pop-up calendar to select a new date and time. After you change the time, click Refresh.

**Note:** By default, DNS data does not display in the events table. To configure the IP Identifier and enable the DNS lookup service, see [IP address identifier](#) on page 646.

**Severity level**

Event filters are assigned a severity level which indicates the importance of event. Severity levels are color-coded, have associated icons, and appear in the Events table so that you can quickly identify and respond appropriately to events.

The SMS uses the following severity levels:

- **Red/Critical** — Indicates critical events that must be looked at immediately.
- **Yellow/Major** — Indicates major events that must be looked at soon as possible.
- **Cyan/Minor** — Indicates minor events that should be looked at as time permits.
• **Gray/Low** — Indicates traffic that is probably normal, but may have security implications.

**Note:** For corresponding SANS terminology, “Major” equates to “High” and “Minor” equates to “Moderate”.

**Table properties**

The Table Properties option allows you to customize the display options. For each column in the table, you can define the order, visibility, sorting, and aggregation properties. To customize the display options for the output table, right-click on the table.

**Customize table property settings**

1. Right-click on a table entry, and then select **Table Properties** from the right-click menu.
2. In the Table Properties dialog, make desired selections for columns.
3. To move a column or columns, select the entire entry or hold down the **SHIFT** key for multiple entries, and then click either **Move Up** or **Move Down**.
4. To save the settings as the default, select **Remember Table Settings**. To use the settings in this session only, do not select **Remember Table Settings**.

**Note:** When you save a query, the table properties will be remembered by default.

5. Click **Apply**.

**Add a comment**

1. On the Events table, select one or multiple rows of events, then right-click and select **Event Comment**.
2. In the Event Comment dialog, type a comment.
3. Click **OK**.

**Edit a comment**

To edit a comment, do one of the following:

- Select one or multiple rows, right-click and select **Event Comment**.
- Double-click the row with the comment you want to edit, and click **Edit** next to the Comment area of the Event Details dialog.

**Note:** If you select multiple rows that do not have the same comment, any new comment you enter replaces the previous comment for all of the selected rows.

**Viewing event details**

Based on the type of event, the Events - Event Details dialog displays the following information about an event.
Event section: information about the event

- **Event No.** - The order in which the event appeared in the SMS.
- **Hit Count** - The number of packets aggregated before notification was sent. Click **Packet Trace** at the bottom of the screen to view more information about the packets involved in the event. The **Packet Trace** button is disabled when packet trace information is not available. See *View the packet trace* on page 75.
- **Event Time** - The time on the device that the traffic was first encountered.
- **Action** - The flow control action associated with the event filter that matched the event.
- **Severity** - (Inspection Events only) The importance of the event. See *Severity level* on page 68.
- **Event Type** - (Firewall Events only) Type of event.
- **Session ID** - (Firewall Events only) The ID of the session with the event.
- **Event Msg** - The message for the event.
- **Comment** - User-generated text added to the event.

Rule/device section: information about the rule and/or device that triggered the event

- **Rule** - (Firewall Inspection Events only) The rule that triggered the event
- **Device** - The device that responded to the traffic
- **Interface In and Out**

Note: Device information is based on whether it is an IPS generated inspection event or a firewall generated inspection event, and may not display the information listed above. Firewall Inspection events have the rule listed with the device, Firewall 'firewall' events have the rule listed in the Rule info section that is specific to firewall event details.

Segment/device section (IPS Inspection Events only): information about the segment and/or device that triggered the event

- **Segment** - (IPS Inspection Events only)
- **Segment Port In** - (IPS Inspection Events only)
- **Device**
- **VLAN**

Network: information about the source and destination of the event

This section provides the Source Address and Port, and the Destination Address and Port of the event. If the additional event information option has been selected, the client IP address also appears in addition to the geographic location for the IP address including the country and flag icon (if available), region, and city.
If both an X-Forwarded-For value and a True-Client-IP value are available, and they differ from each other, the Client IP field reflects the X-Forwarded-For value.

Firewall event details will also include:

- Source NAT Address and Port
- Destination NAT Address and Port
- Source and Destination Zones

**Filter info (Inspection Events only)**

- Filter Name - The name of the filter that triggered the event. If the filter is editable, the Edit Filter button will allow you to easily modify the filter.
- Description - Description of the filter
- Class - Class of the event/filter
- Category - Type of event filter
- Profile - Profile associated with the alert or block
- Protocol - Protocol the filter monitors
- Platform - Platform the filter applies to
- CVE ID - The CVE ID (if available) of the event trigger. The CVE is a dictionary of publicly known information security vulnerabilities and exposures.
- Function
- Globally Collected Filter Info (via ThreatLinQ) - Helps you to understand the global impact of the issue. See *TMC ThreatLinQ charts and graphs* on page 74 for more information.

**Rule info (Firewall only)**

- Profile - Profile associated with the alert or block
- Rule Name - The category of the application defined in the rule.
- Description
- Application
- Category - Type of event filter
- Class - Application classification
- Protocol
- Function
Additional event information

If the additional event information option has been selected, this panel provides the client IP address and hostname information associated with any HTTP URI. X-Forwarded-For and True Client technology captures a client IP address before it can be overwritten by a forwarding proxy IP address. Additional information for this panel includes values for the following possible categories:

- X-Forwarded-For
- True-Client-IP
- URI Method
- URI Hostname
- URI

URL/URI information

A URL Information panel appears only when an HTTP URI value is displayed in the Additional Event Information panel. If a valid URL is established, this panel displays a table that dissects the URL according to its components. If a valid URL cannot be constructed from the URI string, the SMS attempts to construct a URI, which, if successful, appears in a URI Information panel. If the attempt fails, the URI Information panel displays a message describing why the URI is malformed. URI strings have a maximum length of 8KB and can only be transmitted over Secure Socket Layer (SSL).

To display the URI information, the SMS encodes the URI data. Non-ASCII characters, with byte values less than 20h and greater than 7Eh, will be encoded as \xHH where HH represents two hex digits. Backslash characters—5Ch—will be encoded as two consecutive backslash characters.

For example, the following unencoded data:

/foo\bar.htmlDELbaz

where DEL represents a single byte, would be encoded as:

/foo\\bar.html\x7Fbaz

Filter information

A Filter Information panel appears for geographic filter events. It displays the name of the filter, the matching IP address, and the countries that are included or excluded in the filter. From here, you can quickly edit the filter or view additional geographic information.

Edit a geographic filter

1. Click Edit Filter.
The Edit Geographic Filter dialog opens.

2. Update any fields as required.

3. (Optional) To add a country, click the + icon (located to the right of the Country list). Alternatively, right-click in the County list, and then select Add Country.

   **Important:** A country can only be assigned to one Geographic filter at a time. For example, if you create a filter and allow Japan, you cannot search for and select Japan in a different Geographic filter until you remove it from the first filter. If you search for Japan, it will not display in the Choose Countries list.

4. (Optional) To remove a country, select a country, and then click the - icon (located to the right of the Country list). Alternatively, right-click the country, and then select Remove Selected Countries.

5. (Optional) To include a country, right-click a country, and then select Include Countries.

6. (Optional) To exclude a country, right-click a country, and then select Exclude Countries.

   **Note:** You cannot include some countries and exclude others in the same filter. When you exclude or deny a country, the SMS automatically includes every other country available in the database, as shown by a green check mark and Any.

7. Click OK.

View geographic filter description

- Click More to review the countries included or excluded in the Geographic filter and matching IP address dialog.

View event details

1. In the Events table, locate an event.

2. Do one of the following:
   - Double-click the event row.
   - Select the event row, right-click, and select Details.

3. The Events - Event Details dialog opens. From this dialog you can:
   - Edit an event comment.
   - Edit the associated filter or rule.
   - View packet trace information, where available.
   - Copy event details to your clipboard, to be pasted into other applications.
   - View details for the previous or next event in the list.

4. To close this dialog, click Close.
Reputation information

When an Events entry represents a Reputation event, a tool tip displays for the Filter Name column of the Events table. You can view extended information by pressing F2 when the tool tip is displayed. This expanded information is also displayed in the Event Details dialog in the Description field for reputation events.

The following information is included:

• Criteria for the filter that created the event.

• Tag values for the matching entry from the reputation database. This includes both Reputation DV and user-defined tags.

TMC ThreatLinQ charts and graphs

The inspection event details dialog provides embedded ThreatLinQ data. While the chart and map are loading, you can interact with Event Detail dialog.

If you are not authorized to retrieve ThreatLinQ information or cannot contact the ThreatLinQ server, this information is not displayed.

If the Geo Map does not display correctly, you may need to specify the proxy host information required for the JVM on the client. To specify the required information, modify the C:\Program Files\TippingPoint SMS Client\jre\lib\net.properties file and add the information to the following lines:

http.proxyHost=
http.proxyPort=
Http.nonProxyHosts=

Packet trace

The packet trace compiles information about packets that triggered the filter. It encapsulates the information according to requirements set in the application per filter. For events with the appropriate settings, you can view the compiled and stored packet trace.

A filter compiles a packet trace according to the action set settings. If the action set of the associated event filter is configured to log a packet trace, you can view the packet trace log. See Profiles on page 122.

The system saves the packet trace to a packet capture (PCAP) file. The default filename uses the SMS event identifier (Event No).

For more information, see Packet trace – TPS and IPS (S-Series, N-Platform, and NX-Platform) on page 393.

Packet trace options

Packet trace options are available from the Events area or Device area of the SMS. You can request multiple packet trace files from multiple events or all packet traces on a specific device. Packet trace options are
available for devices that support the packet trace feature. Devices, such as the Core Controller and the SSL do not support packet trace. For information on packet trace options available through the Device area of the SMS, see *Save all packet trace information for a device* on page 393.

The **PCAP Download** option can be enabled through the **System Preferences** wizard. See *External Export* on page 46.

**Right-click packet trace menu options**

- **View** — Opens the packet trace viewer.
- **Save** — Opens a file chooser dialog where you can provide a location on the client system for saving the packet trace information for the selected events. Packet trace files are merged into one PCAP file.
- **Download to SMS** — Downloads the packet trace information for the selected events into the **Exports and Archives** section of the SMS Client. When the download is complete, a popup message displays the location where the PCAP file was downloaded and provides an active HTML link to the files.
- **Configure View Settings** — Launches the **Packet Capture Viewer Settings**.

**External packet trace viewer**

You can configure the Packet Trace Viewer to use:

- Internal Packet Capture Viewer
- An application registered with PCAP file association
- External Packet Capture Viewer

**View the packet trace**

1. On the Events screen, locate an entry.
2. Right-click the entry that is associated with a filter that has packet trace enabled. Those events have a check mark in the **Trace** column.
3. Select **Packet Trace**, and then select the **View** option.

**Save packet trace files**

This option opens a file chooser dialog where you can provide a location on the client system for saving the packet trace information.

1. On the Events screen, select one or more packet trace entries you want to save.
2. Right-click the entry or entries.
3. Select **Packet Trace** and then the **Save** option.
4. Browse to the area where you want to save the packet trace information and click **Save**.
Download packet trace files to the SMS

This option downloads the PCAP files into the Exports and Archives section of the SMS Client.

1. On the Events screen, select one or more packet trace entries you want to download.
2. Right-click the entry or entries.
3. Select Packet Trace, and then select the Download to the SMS option.

Configure packet trace view settings

1. On the Events screen, right-click an entry.
2. Select Packet Trace and then the Configure View Settings option.
3. In the Packet Trace Viewer Settings dialog select one of the following options:
   - Internal Packet Capture Viewer
   - An application registered with PCAP file association
   - External Packet Capture Viewer
4. To use an external viewer, browse to the location of the viewer application.
5. Click OK.

Exporting query results

After creating and running an event query, you can export the results of the query to a comma- or tab-delimited file. This file can be imported into programs such as Crystal Reports or Microsoft Excel.

Note: When exporting query results, you must set the results to an analysis mode not including Real-Time. The results can export for Last Hour or date/time range.

Export query results

1. Select Inspection Events or Firewall Events from the left navigational tree.
2. Configure and run an event query.
3. Above the list of events, select an analysis mode other than Real-Time. You can export results for a preset time option (for example: Last Minute, Last 30 Minutes, Last Month, and so on) or for a specified date/time range.
4. At the top of the query pane, click Export Results. Use the file browser to select a file for saving the results.
5. Enter the desired file name. If you are exporting the query to a local file, click Browse to select the directory in which to save the file.
6. Select a Field Delimiter from the drop-down menu.
7. Click OK.
The system saves the query results to a comma- or tab-delimited CSV file. If the query is exported to the SMS Web server, the report will be visible in the Reports section of the SMS Web home page from which you downloaded the SMS client installer.

**Note:** You cannot export queries when the **Real-Time** option is selected.

For more information, see *Exports and archives* on page 645.

## Saving queries

Click **Saved Queries** or **Firewall Saved Queries** to view a table of all of the name of your saved queries and query expressions.

You can save, run, and manage queries through the **Events** screen. Saved queries display in the **Saved Queries** sections under **Inspection Events** and **Firewall Events** in the navigation screen. You can load and modify these saved queries to locate events in the event viewer. Through the screen, you can also remove queries and run saved queries.

When you run a query, you can cancel the query using the **Cancel** button. A query may take a significant amount of time or resources to run. When you cancel the query, it ends without displaying details.

When you select a saved query, it displays in the **Events** screen. You can click **Refresh** to run the query again. The results display in the Events table.

### Open a saved query

1. Navigate to either **Inspection Events** or **Firewall Events** in the navigation screen.
2. In the left navigation pane, expand the **Saved Queries** listing and select a query entry. The query displays in the **Event Viewer**.

### Edit a saved query

1. On the Events screen, click a query entry in the **Saved Queries** section in the navigation pane. The query displays in the **Event Viewer**.
2. Modify parameters as needed.
3. Click **Refresh**. The returned events display in the Events table.
4. To save the modified query and overwrite the existing saved query, click **Save**. This option allows you to save the modified query. To save the modified query with a new name, click **Save As**. The query displays in the Saved Queries section of the navigation pane.

### Delete a saved query

1. On the Events navigation pane, click **Saved Queries** under either **Inspection Events** or **Firewall Events**. The Saved Queries screen displays.
2. Select the query to delete.
3. On the Menu Bar, select the **Edit** then **Delete**.

**Filter criteria**

See *Create an inspection query with filter criteria* on page 79 and *Inspection Events table* on page 59.

The following table lists the fields available in the Filter Criteria Query pane.

**Table 18. Filter criteria**

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter Details</td>
<td>Enables you to enter the name and/or number of the filter.</td>
</tr>
<tr>
<td>Filter Category</td>
<td>Enables you to select one or more filter categories:</td>
</tr>
<tr>
<td></td>
<td>• Application Protection – Exploits, Identity theft, Reconnaissance, Security Policy, Spyware, Virus, Vulnerabilities</td>
</tr>
<tr>
<td></td>
<td>• Infrastructure Protection – DDoS, Network Equipment Protection, Traffic Normalization</td>
</tr>
<tr>
<td></td>
<td>• Performance Protection – Instant Messaging, Peer to Peer, Streaming Media</td>
</tr>
<tr>
<td>Profile</td>
<td>Enables you to select an existing profile.</td>
</tr>
<tr>
<td>Suspicious URL Metadata</td>
<td>Enables you to filter events with suspicious URL metadata.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The correct DV is required to enable the Suspicious URL Metadata field. Activate the DV after you upgrade the SMS. For more information on the correct DV version for your product, see the SMS Release Notes on the TMC at <a href="https://tmc.tippingpoint.com/">https://tmc.tippingpoint.com/</a>.</td>
</tr>
<tr>
<td>Filter Severity</td>
<td>Enables you to select the severity of the event.</td>
</tr>
<tr>
<td>Filter Type</td>
<td>Enables you to filter the events by Security or Application type.</td>
</tr>
<tr>
<td>Reputation Type</td>
<td>Enables you to filter the events by Reputation or Geographic filter. By default, both filters are selected.</td>
</tr>
</tbody>
</table>
For Geographic filters, the Events table displays the name of the filter, any included or excluded countries (Filter Criteria), the country flag icon (if available), and matching IP address for the filter.

If the Geographic filter events display as Reputation events, or if you have other issues with the search criteria, redistribute all the profiles to all the segments for the distribution to start working again.

<table>
<thead>
<tr>
<th>Action Type</th>
<th>Enables you to select the action; Permit, Block, or Active Response.</th>
</tr>
</thead>
</table>

**Create an inspection query with filter criteria**

1. On the Events screen, click **Inspection Events** in the navigation pane.
2. On the Query pane, select **Filter Criteria** to expand this option.
3. On the Filter Details fields, enter the appropriate information.
4. On the Filter Severity area, deselect any option you do not want in your query.
5. On the Filter Category area, select one or more categories in the **Category** list you want to include in your query.

   You can expand a listing to select individual entries or select a top-level list item to include every item listed under it.

6. On the Profile area, select a profile from the drop-down list to include in your query.
7. On the Filter Severity area, deselect any option you do not want in your query.
8. On the Filter Type area, deselect any option you do not want in your query.
9. On the Reputation Type area, deselect any option you do not want in your query.
10. On the Action Type area, deselect any option you do not want in your query.
11. Enter the number of matching rows (1 – 10,000) to list in the Events table.

   Limiting the number of row may decrease the query processing time.

12. Click **Refresh**.

   The returned events display in the Events table.

13. To save this query, click **Save As**.
14. Enter a name for the query when prompted.

   The query displays in the Saved Queries section of the **Events** navigation pane.

15. To create a new query, click **Clear**.
The query pane resets and clears the criteria fields. See Inspection Events table on page 59.

**Note:** You are not required to complete all query fields. Complete only as many as you need to successfully execute your query.

### Filter taxonomy criteria

The Query Pane also includes a Taxonomy option that enables you to search filters based on the class of event, protocol, and platform. You can select multiple options within each grouping. See Create a query with filter taxonomy criteria on page 80 and Inspection Events table on page 59.

The following table lists the fields available in the Filter Taxonomy Query Pane.

**Table 19. Filter taxonomy criteria**

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classification</td>
<td>Type of event.</td>
</tr>
<tr>
<td>Protocol</td>
<td>System communication methods, such as LDAP, SNMP, or SSH.</td>
</tr>
<tr>
<td>Platform</td>
<td>OS-based applications, services or supported device, such as Windows Client, networked router, UNIX Client application, etc.</td>
</tr>
</tbody>
</table>

**Create a query with filter taxonomy criteria**

1. On the Events screen, click **Inspection Events** in the navigation pane.
2. On the Query pane, select **Taxonomy Criteria** to expand this option.
3. Select one or more criteria from the **Classification**, **Protocol**, and **Platform** columns.
   - To select a consecutive range of column entries, hold down the **SHIFT** key.
   - To select multiples entries within a column, hold down the **CTRL** key.
4. Enter the number of matching rows (1 –10,000) to list in the Display Pane. Limiting the number of row may decrease the query processing time.
5. Click **Refresh**. The returned events display in the Events table.
6. To save this query, click **Save As**.
   - Enter a name for the query when prompted. The query displays in the **Saved Queries** section of the **Events** navigation pane. To create a new query, click **Clear**. The query pane resets and clears the criteria fields. See Inspection Events table on page 59.
Note: You are not required to select criteria in all columns.

**Network criteria (Inspection Events)**

The SMS can perform search queries based on single, multiple, or ranges of source and destination ports and filter numbers. In the source (Src Port) and destination (Dest Port), you can enter a range uses a dash (-) and multiple ports by separating with commas (,).

To enhance searches, you can enter both types of parameters in the port field. For example, to display events that had a source port of 22,25, or between 1000 and 32000, you would enter “22,25,1000-32000”.

IP address fields support single entries or CIDR blocks. See *Create a query with network criteria* on page 82 and *Inspection Events table* on page 59.

**Table 20. Network criteria (Inspection Events)**

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Addresses and Ports</td>
<td>Enables you to enter criteria for searching and displaying events. These options include the following:</td>
</tr>
<tr>
<td></td>
<td>• Src Addr — Source IP address</td>
</tr>
<tr>
<td></td>
<td>• Src Port — Port of the source IP address</td>
</tr>
<tr>
<td></td>
<td>• Dst Addr — Destination IP address</td>
</tr>
<tr>
<td></td>
<td>• Dst Port — Port of the destination IP address</td>
</tr>
<tr>
<td>Packet Trace</td>
<td>Indicates if the query should locate action sets with packet trace enabled:</td>
</tr>
<tr>
<td></td>
<td>• All</td>
</tr>
<tr>
<td></td>
<td>• Events with Packet Trace</td>
</tr>
<tr>
<td></td>
<td>• Events without Packet Trace</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>Enables you to enter criteria for searching and displaying events based on VLAN ID.</td>
</tr>
<tr>
<td>Additional Event</td>
<td>Enables you to enter criteria for searching and displaying events based on client IP address or HTTP hostname.</td>
</tr>
<tr>
<td>Information</td>
<td></td>
</tr>
</tbody>
</table>
Create a query with network criteria

1. On the Events screen, click Inspection Events in the navigation pane.
2. On the Query pane, select Network Criteria to expand this option.
3. In the Addresses and Ports area, enter:
   - **Src Addr(s)** — Source IP address
   - **Src Port(s)** — Port of the source IP address
   - **Dst Addr(s)** — Destination IP address
   - **Dst Port(s)** — Port of the destination IP address
4. To use client IP addresses, select the Use Client IP for Source Addresses when Available check box in the Client IP area.
5. When searching for source or destination IP addresses, you can:
   - Enter multiple IP address separated by commas.
   - Enter one address or a CIDR block.
   - Exclude IP addresses in a CIDR block by using the “!” symbol.
6. Select the desired entry from the Packet Trace drop-down listings.
7. If you want to include a VLAN ID in your search query, enter the ID in the VLAN area.
8. Enter the number of matching rows (1 – 10,000) to list in the Display Pane. Limiting the number of row may decrease the query processing time.
9. Click Refresh. The returned events display in the Events table.
10. To save this query, click Save As. Enter a name for the query when prompted. The query displays in the Saved Queries section of the Events navigation pane. To create a new query, click Clear. The query pane resets and clears the criteria fields. See Inspection Events table on page 59.

   **Note:** You are not required to select criteria in all areas.

**User info criteria (Inspection Event viewer)**

The SMS can perform search queries based on users. You can create search criteria rules that include or exclude users based on their login names, their source and destination domain addresses, and by the source and destination machine IP addresses of users.

If no criteria is specified, the default of Any users will be applied to all queries.

IP address fields support single entries or CIDR blocks. See Inspection Events table on page 59.
Table 21. Inspection Event viewer

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Users</td>
<td>Enables you to enter criteria for searching and displaying users. These options include the following:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Src Users</strong> — Login name of source users or user groups</td>
</tr>
<tr>
<td></td>
<td>- <strong>Dst Users</strong> — Login name of destination users or user groups</td>
</tr>
<tr>
<td></td>
<td>The users and user groups available to be added depend on which <strong>Show</strong> radio button you have selected (LDAP, Local, RADIUS, TACACS+).</td>
</tr>
<tr>
<td>Domains</td>
<td>Specifies the source and destination IP address of the user domains.</td>
</tr>
<tr>
<td>Machines</td>
<td>Specifies the source and destination IP address of the user machines.</td>
</tr>
</tbody>
</table>

Create a query with user information criteria

1. On the **Events** screen, click **Inspection Events** in the navigation pane. The **Query** pane displays.
2. On the **Query** pane, select **User Info Criteria** to expand this option.
3. In the **Users** area, click the + button for the **Src User** field to create new users for the criteria rule, or click the - button to remove users from the rule.
4. If you clicked the + button to add a user, the Choose Users dialog opens.
5. Click the + button to specify the login names of source users based on which **Show** radio button you have specified (LDAP, Local, RADIUS, TACACS+).
   
   To narrow the list in the Users field, start typing the user’s login name in the **Search** field.

   **Note:** Adding and deleting users to the rule will add and delete references to those accounts managed elsewhere. The actual user accounts are managed in an Active Directory, RADIUS, TACACS+, or LDAP server and not in SMS.

6. Select **Inclusions** to add the user information to the query criteria rule, or **Exclusions** to exclude the user information from the query criteria rule.
7. Click **OK**.
8. Repeat steps 3 through 7 for the **Dst User** field.
9. In the **Domains** area, specify the IP address of the source and destination domains.
10. In the **Machines** area, specify the IP address of the source and destination machines.
11. To save this query, click **Save As**. Enter a name for the query when prompted. The query displays in the **Saved Queries** section of the **Events** navigation pane. To create a new query, click **Clear**. The query pane resets and clears the criteria fields. See **Inspection Events table** on page 59.

| Note: You are not required to select criteria in all areas. |

### Device/segment/rule criteria

The Query Pane includes segment, device, and firewall profile options to enable you to search filters based on segments, devices and/or firewall profiles.

You can select everything within a group or multiple options within each grouping. See **Create a query with device segment criteria** on page 84 and **Inspection Events table** on page 59.

#### Table 22. Device/segment/rule criteria

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Segment</td>
<td>Group of hosts protected through a licensed pair of ports on a device.</td>
</tr>
<tr>
<td>Device</td>
<td>Devices managed by the SMS.</td>
</tr>
<tr>
<td>Firewall Profile</td>
<td>Firewall profiles managed by the SMS.</td>
</tr>
</tbody>
</table>

**Create a query with device segment criteria**

1. On the Events screen, click **Inspection Events** in the navigation pane. The Query pane displays.
2. On the Query pane, select **Device, Segment Criteria** to expand this option.
3. In the Segment and Devices areas, select one or more items in the lists that you want to include in your query. You can expand a listing to select individual entries or select a top-level list item to include every item listed under it.
   - For information about how you can query for events with a stack of devices, see **Events and reports** on page 529.
4. Enter the number of matching rows (1 – 10,000) to list in the Display Pane. Limiting the number of row may decrease the query processing time.
5. Click **Refresh**. The returned events display in the Events table.
6. To save this query, click **Save As**.
Enter a name for the query when prompted. The query displays in the Saved Queries section of the Events navigation pane. To create a new query, click Clear. The query pane resets and clears the criteria fields. See Inspection Events table on page 59.

**Note:** You are not required to select criteria in all columns.

### Tuning event filters (Inspection events)

The Events screen provides a performance history of event filters and system behavior. The SMS uses the segment of the selected inspection event to determine the profile that will be edited to add or update the filter associated with the event.

The SMS system uses the Profile that was last distributed to the segment and updates that Profile with your filter modifications. Some filters have different options available on the edit dialog box.

**Note:** If the segment specified in the event was not updated from the SMS, you may receive an error indicating that the correct Profile cannot be determined. If the Profile cannot be determined, you must modify the filter directly through the Profiles screen. See Profiles on page 122.

### Filter modifications

The most common modifications that you can do from the Events table include the following items:

- **Edit event filters** — When you review event information, you may want to modify event filter settings to better react to events. For example, a filter that is generating a high number of alerts may need to be changed so that it is not invoked against certain types of events.

- **Create event filter exceptions** — Filters may not always respond correctly to source and destination IP addresses. For example, you may have a filter set to block packet traffic to all hosts; however, some benign traffic is destined for a specific host in your network. In that case, you can create a filter exception.

- **Create traffic management filters** — When you review event information, you might want to create a Traffic Management filter to block, trust, permit, or rate limit traffic based on different protocols and specific source and destination IP addresses.

### Application, transaction, and user criteria (Firewall Events)

This panel allows you to specify search criteria by specific applications or application groups, transactions, and users. Only applications that are defined in the Digital Vaccine will appear in the Choose Applications dialog. Application groups are based on criteria that matches applications in the Digital Vaccine.

### Application groups

We recommended that you create and use application groups for your criteria. The application groups are automatically updated to match Digital Vaccine applications. Also, when you select an application group,
you cannot add individual applications. Control of application groups now extends to transactions at the subapplication level. For Firewall events, you can refine your search according to the following criteria:

- Applications or Application Categories
- Transactions
- Users

**Update query results**

To update the displayed results, click **Refresh**, or right-click on list entries according to the column data.

**Sort query results**

To sort query result by column headings, click on any column heading. The up arrow on the heading indicates an ascending sort and the down arrows indicates a descending sort. To access additional sorting and aggregation options, right-click on a column heading.

**Filter query results by time**

To filter the results by certain time intervals, select from the following options on the Events table:

- **Real-time** — Displays entries as they occur on the system. This option displays data by refreshing the screen. It calculates the refresh rate based on the time it takes to run the query and display the results.
- **By set amount** — Displays entries according to the selected time amount; for example: Last Minute, Last Five Minutes, Last Hour, Last 24 Hours, and so on.
- **Time range** — Displays events during a range of time you select, including date, hour, and minute for Start Time and End Time settings.

**Add application, transaction, and user criteria**

1. Click the + button to open the Choose Applications window.
2. Select either **Application Groups** or **Applications**.

   The dialog lists only applications that are defined in the Digital Vaccine.
3. Find the applications or application groups to add by either entering text in the Search field or scrolling through the list in the window.
4. Double click an application or application group to add it. To select more than one application, press CTRL and click to select the applications, and then click **OK**.

   **Note:** You can only select a single application group; however, you can select multiple applications.
5. As necessary, refine your criteria by adding transactions and users in the same way. Transactions listed in the Choose Transactions dialog are connected to activities of applications defined in the Digital Vaccine.
6. Click **OK**.
For more information on refining the criteria of application groups, see Application groups (Firewall only) on page 238.

Edit application criteria

After you have added individual applications to the Application Criteria, you can choose to include or exclude the application.

1. On the Query pane, select Application, Transaction, and User Criteria to expand this option.
2. Select the application or CTRL+ click to select more than one application, and then right click.
3. From the right-click menu, you can:
   • Remove the selected items
   • Include the items
   • Exclude the items

Important: You cannot use include and exclude applications in the same query.

Firewall policy criteria

The Firewall Policy criteria pane is composed of four sections:

- Firewall profile/rules - Indicate the firewall rule you want to use as a filter, and select the firewall profile you want to apply.
- Filter severity - Indicate the severity of the events you want to see in the results.
- Action - Filter the results based on the actions taken.
- Event type - Indicate the event types to filter by (Session Start, Application Detect, Session End, and/or Blocked by Firewall).

Create a firewall query with filter criteria

1. On the Query pane, select Firewall Policy Criteria to expand this option.
2. In the Firewall Profile/Rule field, enter the appropriate information.
3. In the Filter Severity area, deselect any option you do not want in your query.
4. In the Action area, deselect any option you do not want in your query.
5. In the Event Type area, deselect any option you do not want in your query.
6. Click Refresh. The returned events display in the Events table.

To save this query, click Save As. Enter a name for the query when prompted. The query displays in the Saved Queries section of the Firewall Events navigation pane. To create a new query, click Reset All. The query pane resets and clears the criteria fields. See Inspection Events table on page 59.
Note: You are not required to complete all query fields. Complete only as many as you need to successfully execute your query.

Device, Segment/Interface criteria

The Device, Segment/Interface criteria allows you to filter your results by:

- Devices/Groups/Stacks
- Interfaces In
- Interfaces Out

To filter your results by these criteria, select Add next to the appropriate section then select the appropriate items. Click OK to save your selections.

Note: You are not required to complete all query fields. Complete only as many as you need to successfully execute your query.

Network criteria (Firewall Events)

The Network Criteria Query Panel allows you to search based on Addresses and Ports, Security Zones, Packet Traces, and/or by Country. The SMS can perform search queries based on single, multiple, or ranges of source and destination ports and filter numbers. In the source (Src Port) and destination (Dest Port), you can enter a range using a dash (-) and multiple ports by separating with commas (,). To enhance searches, you can enter both types of parameters in the port field. For example, to display events that had a source port of 22,25, or between 1000 and 32000, you would enter “22,25,1000-32000”. IP address fields support single entries or CIDR blocks.

Create a firewall query with network criteria

1. On the Query pane, select Network Criteria to expand this option.
2. In the Addresses and Ports area, enter:
   - Src Addr(s) — Source IP address
   - Src Port(s) — Port of the source IP address
   - Dst Addr(s) — Destination IP address
   - Dst Port(s) — Port of the destination IP address
3. Select the appropriate Source or Destination Security Zones by clicking the + symbol.
4. From the Packet Trace drop-down listings, select All (Default), Events with Packet Trace, or Events without Packet Trace.
5. Select the Source or Destination Country from the appropriate country selection dialog.
6. Click Refresh. The returned events display in the Events table.
To save this query, click Save As. Enter a name for the query when prompted. The query displays in the Saved Queries section of the Events navigation pane. To create a new query, click Clear. The query pane resets and clears the criteria fields. See Inspection Events table on page 59.

Note: You are not required to complete all query fields. Complete only as many as you need to successfully execute your query.

Schedule, Service Criteria

The Schedule, Service Criteria query pane allows you to search for events triggered by a schedule or services rule.

Create a query with schedule or service criteria

1. On the Query pane, select Schedule, Service Criteria to expand this option.
2. In the Schedules or Services area, click the + symbol to add a new schedule.
3. Select whether to Include or Exclude the schedule or service from the search results.
4. Click OK.

Network Address Translation criteria

The Network Address Translation (NAT) Query Pane allows you to search based on Source and/or Destination NAT Addresses and Ports. You can also add the Source or Destination Country.

Note: You are not required to complete all query fields. Complete only as many as you need to successfully execute your query.

Users criteria (Firewall Events)

The Users criteria allows you to search for events based on a particular user or a group of users. You can use this criteria to find events related to a user account that is either local or authenticated against an LDAP or RADIUS server.

Event criteria (Firewall Events)

The Event criteria allows you to search for events based on whether it has a comment or not. You can also use this criteria to search by event number.

URL Threat Analysis

URL Threat Analysis enables the SMS to automatically use the Deep Discovery (DD) Analyzer device. The DD device analyzes suspicious content in HTTP traffic to detect malware threats to browsing clients in your network.
Configure URL Threat Analysis to send inspection event URLs from the SMS to the DD Analyzer. The DD device analyzes the URLs and then sends the threat analysis results to the SMS. The results are displayed in the URL Threat Analyzer Results panel and indicate which event URLs might pose a threat. Based on the results, you can make device configuration adjustments, such as modifying profile action sets or creating a manual response to quarantine an infected host.

The following information describes how to configure and use URL Threat Analysis:

- **Prerequisites** on page 90
- **Configure URL Threat Analysis** on page 91
- **URL Threat Analyzer results** on page 92

For more information about the DD Analyzer, see the DD Analyzer documentation on the Trend Micro documentation site.

**Prerequisites**

Complete the following tasks before you configure URL Threat Analysis. See Configure URL Threat Analysis on page 91 for steps to connect the DD Analyzer device and enable URL Threat Analysis.

- SMS v4.6.0 or later
- Use devices that support HTTP metadata collection, which includes the following versions:
  - **IPS (N or NX Series)** — TOS v3.7.0 or later
  - **TPS (440T or 2200T)** — TOS v4.2.0 or later
  - **TPS (8200TX or 8400TX)** — TOS v5.0.0 or later
  - **DD Analyzer** — v5.5.0 or later
- Ensure that TCP port 443 is available so that the SMS can send event URLs to the DD Analyzer. See Port information on page 683 for more information about the SMS network ports.
- Configure one or more profiles to generate events with URL data using the following steps:
  - Navigate to Profiles > Inspection Profiles > <profile name>.
  - In the Details tab, click Edit Details....
  - Select HTTP Context.
  - Click OK to configure the profile to extract HTTP metadata from filter alerts.
  - Distribute the profile. See Distribute profiles on page 142 for more information.
- Review the filter settings for your profile. Trend Micro recommends including action sets with + Notify.
- Save an inspection event query in Events > Inspection Events.

When creating a saved inspection event query, keep the following information in mind:
Include any parameters that create a set of events with URLs that you want to send to the DD device to analyze.

- At a minimum, the saved inspection event query must include HTTP-based events. In **Filter Taxonomy Criteria**, under Protocol, select the **HTTP** setting.

- Trend Micro recommends that you include Events with suspicious URL metadata. In **Filter Criteria**, under Suspicious URL Metadata, select **Include**.

  **Note:** The correct DV is required to enable the Suspicious URL Metadata field. Activate the DV after you upgrade the SMS. For more information on the correct DV version for your product, see the SMS Release Notes on the TMC at [https://tmc.tippingpoint.com/](https://tmc.tippingpoint.com/).

- When you modify the URL Threat Analysis saved query, the SMS uses the updated version to send the next set of event URLs to the DD Analyzer.

  For more information about creating an inspection query, see *Create an inspection query with filter criteria* on page 79.

### Configure URL Threat Analysis

Before you configure URL Threat Analysis, gather the following DD Analyzer device information:

- **IP address** — In IPv4 format.
- **API key** — Located in the **Help > About** page on the DD device management console in your browser.
- **Certificate** — The SSL certificate used for web requests to the DD Analyzer. Import the certificate to the SMS from the DD device management console.

For more information about the DD Analyzer, see the DD Analyzer documentation on the Trend Micro documentation site.

To connect the SMS to the DD Analyzer and enable URL Threat Analysis:

1. From the Events workspace, click **URL Threat Analysis** in the navigation pane.
2. Under URL Threat Analyzer Configuration, click **Edit**.
3. In the URL Threat Analyzer Configuration options, select **Enable URL Forwarding**.
4. Select a saved inspection event query.
   - For more information about the saved inspection event query, see *Prerequisites* on page 90.
5. Enter the DD Analyzer device IP address.
6. Enter the API key.
7. Enter the certificate.
8. Click **OK**.
9. (Optional) To unregister the DD Analyzer from the SMS and stop the SMS from sending URLs to the DD device, do one of the following:

- Clear Enable URL Forwarding in the URL Threat Analyzer Configuration options to simply disable URL forwarding. The configuration settings are still saved when you clear Enable URL Forwarding.
- Click Reset on the URL Threat Analysis page to delete the current DD device configuration settings as well as disable URL forwarding.

**URL Threat Analyzer results**

Use the URL Threat Analyzer results panel to identify potential URL threats to your network and adjust your profile filter action sets if necessary. After the SMS sends a set of inspection event URLs to the DD Analyzer device for analysis, the progress and results are displayed in this panel. For steps to set up URL Threat Analysis, see URL Threat Analysis on page 89.

The SMS can submit event URLs to the device at a faster rate than the DD Analyzer can analyze the URLs and return the results. For this reason, several entries might be in the Queued state in the results panel at the same time.

If there are more DD Analyzer devices connected in a cluster to perform analysis, the analysis rate improves.

Additionally, you can improve the analysis rate by modifying your saved inspection event query to include more search parameters. Selecting more parameters reduces the number of inspection event URLs sent to the DD Analyzer. This improves the analysis rate and creates a more fine-tuned set of results.

For more information about the DD Analyzer, see the DD Analyzer documentation on the Trend Micro documentation site.

**To update the table results**

Click Refresh in the URL Threat Analyzer Configuration panel. The results panel limits the number of entries to 10,000 event URLs.

**To resubmit a URL to the DD Analyzer**

The SMS does not automatically resubmit event URLs to the DD Analyzer after the initial submission. However, if the DD Analyzer did not properly receive the event URL because of a NonComm status, for example, you can manually resubmit that URL.
To resubmit URLs to the DD Analyzer, right-click on one or more entries in the results table, and then select **URL Forwarding > Resubmit URL**.

**Note:** If you resubmit one or more entries, and if the number of entries in the results panel is already at 10,000, go to the DD device management console to view the results.

**To create a manual response**

Right-click on one or more entries in the results table, and then select **Create Response > Source IP Address**.

You can manually respond to a targeted host by specifying the IP address of the host and the policy that you want to trigger for that host. Create policies in Responder to provide more configuration options and to fine-tune your response. Responder supports multiple action sets that can be added to a response policy. For more information, see **Policies** on page 262.

**Table 23. URL Threat Analyzer Results panel**

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event Number</td>
<td>The order in which the event appeared in the SMS.</td>
</tr>
<tr>
<td>Event Time</td>
<td>The time on the IPS/TPS device that the traffic was first encountered.</td>
</tr>
<tr>
<td>Filter Name</td>
<td>The name of the filter that triggered the event.</td>
</tr>
<tr>
<td>URL</td>
<td>The event URL.</td>
</tr>
<tr>
<td>Risk Level</td>
<td>• <strong>NoRiskFound</strong> — The object did not exhibit suspicious characteristics.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Low</strong> — The object exhibited mildly suspicious characteristics that are most likely benign.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Medium</strong> — The object exhibited moderately suspicious characteristics.</td>
</tr>
<tr>
<td></td>
<td>• <strong>High</strong> — The object exhibited highly suspicious characteristics that are commonly associated with malware.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Unknown</strong> — The DD Analyzer was unable to determine the risk level. When a URL is resubmitted, the risk level resets to Unknown until the SMS receives the updated results from the DD Analyzer. Details are available for the entry in the DD device management console.</td>
</tr>
<tr>
<td>Column</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Status</td>
<td>Informational statuses:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Queued</strong> — The SMS sent the event to the DD Analyzer, but analysis has not begun.</td>
</tr>
<tr>
<td></td>
<td>• <strong>InProgress</strong> — The event is currently being analyzed by the DD Analyzer.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Complete</strong> — The event analysis is complete.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Canceled</strong> — The event analysis was canceled from the DD Analyzer user interface.</td>
</tr>
<tr>
<td></td>
<td>• <strong>NonComm</strong> — The SMS is not connected to the DD Analyzer. This condition may be caused by network connectivity issues.</td>
</tr>
<tr>
<td>Error statuses:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>BadURL</strong> — The URL format is incorrect.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Error</strong> — The DD Analyzer encountered an error.</td>
</tr>
<tr>
<td></td>
<td>Resubmit the URL by right-clicking the entry and selecting <strong>URL Forwarding &gt; Resubmit URL</strong>.</td>
</tr>
<tr>
<td></td>
<td>If resubmitting does not correct the condition, search for the corresponding URL in the <strong>Virtual Analyzer &gt; Submissions</strong> panel in the DD device management console for more specific information about the type of error.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Timeout</strong> — The URL entry has been in an active state (Queued, InProgress, or NonComm) for over 24 hours. After 24 hours, you can view the entry in the DD device management console.</td>
</tr>
<tr>
<td>HTML Reports</td>
<td>Link to the HTML or PDF formatted report generated by the DD Analyzer that provides a comprehensive summary of the event URL. The link only appears in the SMS URL Threat Analyzer Results panel if the submission is in a <strong>Complete</strong> state.</td>
</tr>
<tr>
<td>PDF Reports</td>
<td>Click the report link to download either report file. The content of the HTML and PDF reports is the same; only the format is different.</td>
</tr>
<tr>
<td>Source IP Address</td>
<td>Source IP address from the event. Expand this column for location details, including geography map, region, city, and named resource.</td>
</tr>
<tr>
<td>Column</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Device</td>
<td>Name of the IPS/TPS device that generated the event.</td>
</tr>
<tr>
<td>Segment/Rule</td>
<td>Segment for IPS/TPS-generated events, and rules for firewall-generated inspection events.</td>
</tr>
<tr>
<td>Submit Time</td>
<td>The time that the event was submitted from the SMS to the DD Analyzer.</td>
</tr>
</tbody>
</table>
Reports

As the SMS detects malicious attacks and manages network usage, event data is logged in the database. This information details the system’s behavior as it responds to network traffic. The SMS provides a set of options to generate reports about the compiled and stored log information. You can use reports in the SMS to generate up-to-the-moment data analysis to help you measure your network data. With an easy-to-use reporting wizard, you can customize existing reports or build them from scratch.

To open the Reports workspace, click Reports on the SMS toolbar.

For information about how you can report on a stack of devices, see Events and reports on page 529.

Navigate the Reports workspace

The Reports workspace displays reports of accumulated data compiled by the managed device and the SMS. These reports detail the threats that the system encounters, and they record processing trends. The Reports screen also provides IPS network statistics as well as report management and scheduling features.

The Reports workspace includes a Templates folder that displays the standard set of pre-defined report templates, a Saved Reports folder that displays the results and schedules for each saved report, and an All Schedules folder that displays the report schedule for each saved report.

From the Reports workspace, you can do the following:

• Find a report template. Use the Templates folder to quickly navigate to a set of reports in a particular category (Inspection Security, Inspection Application, Firewall, Reputation, Rate Limit, Device Traffic, Advanced DDoS, and Executive Inspection Security). Click the Expand All or the Collapse All icon on the left side of a template category to hide or show all reports for a category. See Templates on page 117.

• Display or run the report. Click a report title. Either the previously generated report appears, or you can apply criteria filters to run the report. See Run a report on page 110.

• Create, save, and schedule a report. Click Create Report (on the Saved Reports screen) to start a Create Report wizard that you need to follow to generate the report. Alternatively, you can save a report by selecting a report template and applying criteria filters. For example, you can create a report from scratch by uploading a logo, selecting default colors, editing criteria filters, and then saving it. The next time you need to run a report, you can select the saved report to automatically use what was saved from the report template. See Create a saved report on page 118.

• View saved report results and schedules. Click the Saved Reports folder to view a list of saved report results and originating report templates. You can modify the criteria filters and save customize a saved. You can also review, edit, or delete the report schedule. See Saved reports on page 117.
• **Export the data.** On saved reports, click **Export Result** to start an Export Result wizard that you need to follow to convert the report to a different format and to select an export type. See *Export report results* on page 114.

• **Manage report schedules.** Click **All Schedules** to view all of the report schedules that you created. From this screen, you can drill into a schedule, update any of the fields in a schedule, or delete the schedule. See *All schedules* on page 120

### AD User reports

The SMS report templates include two Security reports:

• Specific User  
• Top User  

The SMS also includes two Inspection Application report templates:

• Specific User  
• Top Users

### Inspection criteria panels

The following table lists the criteria panels that are available for the inspection report templates. For more information about how determine which criteria panels display and the order in which they appear on the report template, see *Customize the criteria panels* on page 112.

**Table 24. Inspection criteria panels**

<table>
<thead>
<tr>
<th><strong>Use this criteria panel...</strong></th>
<th><strong>To filter the report by:</strong></th>
</tr>
</thead>
</table>
| Filter Criteria               | Details including filter name and number, category, profile, severity, Reputation Type, and action.  
|                               | Attack filters are assigned a severity level which indicates the importance of attack traffic. Severities are color-coded to help you quickly identify and respond to attack traffic.  
|                               | The SMS uses the following severity levels:  
|                               | • **Critical** — Indicates critical attacks that must be looked at immediately.  
<p>|                               | • <strong>Major</strong> — Indicates major attacks that must be looked at soon. |</p>
<table>
<thead>
<tr>
<th>Use this criteria panel...</th>
<th>To filter the report by:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• <strong>Minor</strong> — Indicates minor attacks that should be looked at as time permits.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Low</strong>  — Indicates traffic that is probably normal, but may have security implications.</td>
</tr>
<tr>
<td>Filter Taxonomy Criteria</td>
<td>Classification, protocol, and/or platform. Click the Lookup icon to quickly search the list.</td>
</tr>
<tr>
<td>Network Criteria</td>
<td>Addresses and Ports, VLAN, country, and/or client IP.</td>
</tr>
<tr>
<td>User Info Criteria</td>
<td>Login IDs of source/destination users and user groups, and the IP addresses of the source/destination domains and machines.</td>
</tr>
<tr>
<td>Device, Segment, Rule Criteria</td>
<td>Segment, device or stack, and/or firewall profile and rules.</td>
</tr>
<tr>
<td></td>
<td>• Click <strong>Add</strong> to add a device, segment, or firewall profile.</td>
</tr>
<tr>
<td></td>
<td>• Click <strong>Delete</strong> to remove an existing device, segment, or firewall profile.</td>
</tr>
<tr>
<td>Report Options</td>
<td>Use the Report Options pane to specify various aspects of your report. Report Options selections provide options that directly correlate with how your Report appears.</td>
</tr>
<tr>
<td></td>
<td>The Report Options panel may include some or all of the following options:</td>
</tr>
<tr>
<td></td>
<td>• Chart Type</td>
</tr>
<tr>
<td></td>
<td>• Classification labels</td>
</tr>
<tr>
<td></td>
<td>• Include All Details Table</td>
</tr>
<tr>
<td></td>
<td>• Number of matching details</td>
</tr>
<tr>
<td></td>
<td>• Report logo</td>
</tr>
<tr>
<td></td>
<td>• Report style</td>
</tr>
<tr>
<td></td>
<td>• Security Classification label</td>
</tr>
<tr>
<td></td>
<td>• Inbound, Outbound, or both (Bandwidth reports)</td>
</tr>
</tbody>
</table>
Firewall templates

Firewall reports provide information that helps in analyzing bandwidth usage and effectiveness of the firewall rules. The firewall reports are folded in from firewall events.

**Note:** You must have a firewall device configured in the SMS before you can run firewall reports.

The SMS includes the following firewall report templates:

- Least Utilized Rules by Hit Count — The information this report provides can be helpful when deciding which criteria to exclude from your rules. Having access to this data helps in increasing the effectiveness of your rules.

- Top Applications by Bandwidth — This report lists the applications that are most frequently allowed by the firewall, organized by bandwidth width reports are only available for Permit events.

- Top Applications by Hit Count — The list in this report contains the applications most frequently allowed by the firewall.

- Top Blocked Applications — This report lists the applications that are most frequently disallowed by the firewall.

- Top IP Addresses by Bandwidth — The information in this report helps determine the most suitable devices to use as well as how best to implement them. Regardless of whether or not IP addresses this report cites are associated with a source or a destination, this information helps protect against potential malicious threats. Bandwidth reports are only available for Permit events.

- Top Users by Bandwidth— The list in this report specifies particular users by bandwidth and are only available for Permit events.

- Top Utilized Rules by Bandwidth — This report contains a list of the most frequently used firewall rules according to bandwidth. Bandwidth reports are only available for Permit events.

- Top Utilized Rules by Hit Count — This report contains a list of the most frequently used firewall rules, organized by the number of times a page is visited in a specified time span.

Firewall criteria panels

The following table lists the criteria panels that are available for the firewall report templates. For more information about how to dictate which criteria panels display and the order in which they appear on the report template, see *Customize the criteria panels* on page 112.
### Table 25. Firewall criteria panels

<table>
<thead>
<tr>
<th>Use this criteria panel...</th>
<th>To filter the report by:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application, Transaction and User Criteria</td>
<td>Application groups, individual applications in the digital vaccine, transactions of those applications, and/or specific users to be included or excluded.</td>
</tr>
<tr>
<td>Firewall Policy Criteria</td>
<td>Existing firewall profiles and rules. On this panel, you can also dictate severity and actions.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Device, Interface Criteria</td>
<td>Segment or device, and incoming and/or outgoing interfaces.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Network Criteria</td>
<td>Addresses and Ports, Security Zones, VLAN, and/or country.</td>
</tr>
<tr>
<td>Network Address Translation Criteria</td>
<td>Source NAT addresses, ports, and/or country and Destination NAT addresses, ports and/or country.</td>
</tr>
<tr>
<td>Schedule, Service Criteria</td>
<td>Included or excluded schedules and services.</td>
</tr>
<tr>
<td>Report Options</td>
<td>Use the Report Options pane to specify various aspects of your report. Report Options selections provide options that directly correlate with how your Report appears.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Use this criteria panel... | To filter the report by:
---|---
| • Number of matching details
| • Report logo
| • Report style
| • Security Classification label
| • Inbound, Outbound, or both (Bandwidth reports)

Reputation templates

Reputation reports provide data on malicious IP addresses or DNS domains. The SMS includes the following reputation report templates:

• All DNS Requestors
• All Reputation DNS Names
• All Reputation Events
• All Reputation IP Addresses
• Specific Reputation DNS Names
• Specific Reputation Events
• Specific Reputation IP Addresses
• Top DNS Requestors
• Top Reputation by Country
• Top Reputation DNS Names
• Top Reputation Events
• Top Reputation IP Addresses

Reputation criteria panels

The following table lists the criteria panels that are available for the reputation report templates. For more information about how to dictate which criteria panels display and the order in which they appear on the report template, see Customize the criteria panels on page 112.
Table 26. Reputation criteria panels

<table>
<thead>
<tr>
<th>Use this criteria panel...</th>
<th>To filter the report by:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter Criteria</td>
<td>Details including filter name and number, category, profile, severity, Reputation Type, and action. Attack filters are assigned a severity level which indicates the importance of attack traffic. Severities are color-coded to help you quickly identify and respond to attack traffic. The SMS uses the following severity levels:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Critical</strong> — Indicates critical attacks that must be looked at immediately.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Major</strong> — Indicates major attacks that must be looked at soon.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Minor</strong> — Indicates minor attacks that should be looked at as time permits.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Low</strong> — Indicates traffic that is probably normal, but may have security implications.</td>
</tr>
<tr>
<td>Filter Taxonomy Criteria</td>
<td>Classification, protocol, and/or platform. Click the Lookup icon to quickly search the list.</td>
</tr>
<tr>
<td>Network Criteria</td>
<td>Addresses and Ports, VLAN, country, URL, and/or client IP.</td>
</tr>
<tr>
<td>User Info Criteria</td>
<td>Source and destination information for users, domains, and machines.</td>
</tr>
<tr>
<td>Device, Segment, Rule Criteria</td>
<td>Segment, device or stack, and/or firewall profile and rules.</td>
</tr>
<tr>
<td></td>
<td>• Click <strong>Add</strong> to add a device, segment, or firewall profile.</td>
</tr>
<tr>
<td></td>
<td>• Click <strong>Delete</strong> to remove an existing device, segment, or firewall profile.</td>
</tr>
<tr>
<td>Report Options</td>
<td>Use the Report Options pane to specify various aspects of your report. Report Options selections provide options that directly correlate with how your Report appears.</td>
</tr>
<tr>
<td>Use this criteria panel...</td>
<td>To filter the report by:</td>
</tr>
<tr>
<td>--------------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td></td>
<td>The Report Options panel may include some or all of the following options:</td>
</tr>
<tr>
<td></td>
<td>- Chart Type</td>
</tr>
<tr>
<td></td>
<td>- Classification labels</td>
</tr>
<tr>
<td></td>
<td>- Include All Details Table</td>
</tr>
<tr>
<td></td>
<td>- Number of matching details</td>
</tr>
<tr>
<td></td>
<td>- Report logo</td>
</tr>
<tr>
<td></td>
<td>- Report style</td>
</tr>
<tr>
<td></td>
<td>- Security Classification label</td>
</tr>
</tbody>
</table>

**Rate Limit templates**

Rate Limit reports provide options for reporting the percentage of bandwidth used in a pipeline of traffic for rate limit action sets. You can generate reports by device and by rate limit action set. Rate limiting through an action set defines a maximum bandwidth that can be used by traffic that matches filters assigned to that action set. Incoming traffic in excess of this bandwidth is dropped. If two or more filters use the same rate limiting action set, then all packets matching these filters share the bandwidth.

The SMS includes the following rate limit report templates:

- Rate Limits by Specific Device
- Specific Rate Limit Action Set

**Rate Limit criteria panels**

The following table lists the criteria panels that are available for the rate limit report templates. For more information about how to dictate which criteria panels display and the order in which they appear on the report template, see *Customize the criteria panels* on page 112.

**Table 27. Rate Limit criteria panels**

<table>
<thead>
<tr>
<th>Use this criteria panel...</th>
<th>To filter the report by:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device / Rate Limit Criteria</td>
<td>Device or Rate Limit action set.</td>
</tr>
<tr>
<td></td>
<td>• Click <strong>Add</strong> to add a device.</td>
</tr>
</tbody>
</table>
Use this criteria panel... | To filter the report by:
---|---
Device Rate Limit Report Options | • Click **Remove** to select or clear Rate Limit action sets.

Report Options | Time (minute, hours, or days) and/or throughput.

Use the Report Options pane to specify various aspects of your report. Report Options selections provide options that directly correlate with how your Report appears.

The Report Options panel may include some or all of the following options:

- Chart Type
- Classification labels
- Include All Details Table
- Number of matching details
- Report logo
- Report style
- Security Classification label

**Device Traffic templates**

The Device Traffic report provides options for reporting statistical changes in network traffic patterns by device. The report documents the traffic units per unit time according to devices, detailing the direction of traffic tracked according to port. Device Traffic templates allow you to enhance reporting by configuring the traffic direction and data display as average bps or total bytes. The SMS includes one device traffic report template: IPS Physical Port.

For information about how you can report on a stack of devices, see *Events and reports* on page 529.

**Device Traffic criteria panels**

The following table lists the criteria panels that are available for the device traffic report template. For more information about how to dictate which criteria panels display and the order in which they appear on the report template, see *Customize the criteria panels* on page 112.
Table 28. Device Traffic criteria panels

<table>
<thead>
<tr>
<th>Use this criteria panel...</th>
<th>To filter the report by:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Criteria</td>
<td>Device or stack, or specific segment of a device.</td>
</tr>
<tr>
<td>Device Traffic Report Options</td>
<td>Time (minute, hours, or days), data display, data aggregation, and/or traffic direction.</td>
</tr>
<tr>
<td>Report Options</td>
<td>Use the Report Options pane to specify various aspects of your report. Report Options selections provide options that directly correlate with how your Report appears. The Report Options panel may include some or all of the following options:</td>
</tr>
<tr>
<td></td>
<td>• Chart Type</td>
</tr>
<tr>
<td></td>
<td>• Classification labels</td>
</tr>
<tr>
<td></td>
<td>• Include All Details Table</td>
</tr>
<tr>
<td></td>
<td>• Number of matching details</td>
</tr>
<tr>
<td></td>
<td>• Report logo</td>
</tr>
<tr>
<td></td>
<td>• Report style</td>
</tr>
<tr>
<td></td>
<td>• Security Classification label</td>
</tr>
</tbody>
</table>

Advanced DDoS templates

Advanced DDoS (Distributed Denial of Service) reports provide information about detected and blocked DDoS attacks against your network including SYN floods, Established Connection floods, and Connections Per Second (CPS) floods.

Note: Only devices that support Advanced DDoS have access to these reports. Only devices that have Advanced DDoS Protection filters can provide data for these reports. For more information on E-Series devices, contact your TippingPoint sales representative.

• Connection Flood — Describes the detection and block of Established Connection Flood attacks. In these attacks, a TCP established connection attack originates an attack from an IP connection considered safe by the network. This attack generates floods of full (3-way) established TCP connections using a safe or accepted IP address. It attempts to flood the proxy by sending more connections than
the system can handle. The report lists the number of connections and the statistics of the detection and block procedures.

- **Connections per Second** — Describes the detection and block of CPS Flood attacks. These attacks enact a flood of connections to your network, refusing legitimate traffic from your network. The report includes information on the maximum amount of allowed connections and the statistics of the detection and block procedures.

- **SYN Proxy** — Describes the detection and block of SYN flood attacks. These attacks enact a series of requests with false SYN flags that constantly request a connection. SYN Proxy enables the use of SYN traps to block all new TCP connection requests from a single attacker against a host.

The SMS includes one advanced DDoS report template: DDoS.

### Advanced DDoS criteria panels

The following table lists the criteria panels that are available for the advanced DDoS report template. For more information about how to dictate which criteria panels display and the order in which they appear on the report template, see [Customize the criteria panels](#) on page 112.

**Table 29. Advanced DDoS criteria panels**

<table>
<thead>
<tr>
<th>Use this criteria panel...</th>
<th>To filter the report by:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter Criteria</td>
<td>Inspection Profile and Advanced DDoS filters are required to run this report.</td>
</tr>
<tr>
<td>Segment Criteria</td>
<td>Segment or group for a device.</td>
</tr>
<tr>
<td>Advanced DDoS Report Options</td>
<td>Time (minute, hours, or days) and/or one or more DDoS types.</td>
</tr>
</tbody>
</table>
| Report Options            | Use the Report Options pane to specify various aspects of your report. Report Options selections provide options that directly correlate with how your Report appears. The Report Options panel may include some or all of the following options:  
  - Chart Type  
  - Classification labels  
  - Include All Details Table |
Executive reports templates

Executive Inspection Security reports provide a summary of the top attacks and can include specific report items from the following report areas:

- Security: Top attacks, top destinations, top sources
- Application: Top applications, top P2P peers
- Reputation: Top events, top IP addresses, top DNS names, top URLs

The SMS includes one executive inspection security report template: Executive.

Executive report criteria panels

The following table lists the criteria panels that are available for the executive inspection security report template. For more information about how to dictate which criteria panels are available and the order in which they appear on the report template, see Customize the criteria panels on page 112.

Table 30. Executive report criteria panels

<table>
<thead>
<tr>
<th>Use this criteria panel...</th>
<th>To filter the report by:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter Criteria</td>
<td>Details including filter name and number, profile, severity, and action.</td>
</tr>
<tr>
<td></td>
<td>Attack filters are assigned a severity level which indicates the importance of attack traffic.</td>
</tr>
<tr>
<td></td>
<td>Severities are color-coded to help you quickly identify and respond to attack traffic.</td>
</tr>
<tr>
<td></td>
<td>The SMS uses the following severity levels:</td>
</tr>
<tr>
<td></td>
<td>• Critical — Indicates critical attacks that must be looked at immediately.</td>
</tr>
<tr>
<td></td>
<td>• Major — Indicates major attacks that must be looked at soon.</td>
</tr>
<tr>
<td>Use this criteria panel...</td>
<td>To filter the report by:</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>----------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>• <strong>Minor</strong> — Indicates minor attacks that should be looked at as time permits.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Low</strong> — Indicates traffic that is probably normal, but may have security implications.</td>
</tr>
<tr>
<td>Filter Taxonomy Criteria</td>
<td>Classification, protocol, and/or platform. Click the Lookup icon to quickly search the list.</td>
</tr>
<tr>
<td>Network Criteria</td>
<td>Addresses and Ports, VLAN, country, and/or client IP.</td>
</tr>
<tr>
<td>Device, Segment, Rule Criteria</td>
<td>Segment, device or stack, and/or firewall profile and rules.</td>
</tr>
<tr>
<td></td>
<td>• Click <strong>Add</strong> to add a device, segment, or firewall profile.</td>
</tr>
<tr>
<td></td>
<td>• Click <strong>Delete</strong> to remove an existing device, segment, or firewall profile.</td>
</tr>
<tr>
<td>Report Options</td>
<td>Use the Report Options pane to specify various aspects of your report. Report Options selections provide options that directly correlate with how your Report appears.</td>
</tr>
<tr>
<td></td>
<td>The Report Options panel may include some or all of the following options:</td>
</tr>
<tr>
<td></td>
<td>• Chart Type</td>
</tr>
<tr>
<td></td>
<td>• Classification labels</td>
</tr>
<tr>
<td></td>
<td>• Include All Details Table</td>
</tr>
<tr>
<td></td>
<td>• Number of matching details</td>
</tr>
<tr>
<td></td>
<td>• Report logo</td>
</tr>
<tr>
<td></td>
<td>• Report style</td>
</tr>
<tr>
<td></td>
<td>• Security Classification label</td>
</tr>
</tbody>
</table>
Traffic Analysis templates

Traffic Analysis reports provide security teams with a holistic view of traffic patterns by sampling a random flow of traffic using the sFlow® feature. The data gets sent to a collector server for analysis. Security administrators can establish a baseline of typical application traffic to identify unusual patterns.

The data that is sampled gets sent as an sFlow datagram packet to a collector server where analysis occurs. The SMS includes the following traffic analysis report templates:

- Top IP by Bandwidth
- Top Protocol by Bandwidth
- Top Service by Bandwidth

**Note:** The option to generate a Traffic Analysis report is available only for SMS-managed NX-Platform IPS devices running TOS v 3.6.0 or later and TPS devices running TOS v5.0.0 or later. Traffic sampling using sFlow is not supported on vTPS devices.

Traffic Analysis criteria panels

The following table lists the criteria panels that are available for the Traffic Analysis report templates. For more information about how to dictate which criteria panels display and the order in which they appear on the report template, see *Customize the criteria panels* on page 112.

**Table 31. Traffic Analysis criteria panels**

<table>
<thead>
<tr>
<th>Use this criteria panel...</th>
<th>To filter the report by:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocols, Services Criteria</td>
<td>Protocols, such as GGP, ICMP, TCP, and UDP, and services to be included or excluded.</td>
</tr>
<tr>
<td></td>
<td>Services are defined collections of TCP/UDP ports, IP protocols, or ICMP type and code values. Service groups are collections of services and are available for selection in this same list.</td>
</tr>
<tr>
<td>Segment, Device Criteria</td>
<td>Available physical segments and devices.</td>
</tr>
<tr>
<td></td>
<td>• Click <strong>Add</strong> to add a device or stack, device group, or physical segment.</td>
</tr>
<tr>
<td></td>
<td>• Click <strong>Remove</strong> to remove an existing device, device group, or physical segment.</td>
</tr>
</tbody>
</table>
Use this criteria panel... | To filter the report by:
--- | ---
Network Criteria | Source and destination addresses and ports, and VLAN.
Report Options | Use the Report Options pane to specify various aspects of your report. Report Options selections provide options that directly correlate with how your report appears.

The Report Options panel may include some or all of the following options:

- Chart type and report logo and style options
- Security Classification label
- Bandwidth: Inbound, Outbound, or Both
- Endpoint: Inbound, Outbound, or Both

**Run a report**

When you open a report, it appears with a variety of criteria panels at the top of the screen. By using the criteria panels, you can look at your data from multiple angles. The available criteria panels depend on the type of report that you select. A basic report in the SMS is broken up into two parts:

- **Criteria panels.** This section is at the top of the screen. You can use it to filter and perform other options on a report. For example, you can use the Report Options to choose a chart type and classification label, determine the number of data to include, upload your company logo, and select a color and font as the report style.

- **Generated report.** This section shows the report itself. What is visible depends on the construction of the report and what you have permission to see in the SMS. The report is then ready for instant viewing using a built-in viewer component on the screen, printing, and saving/exporting to other popular document formats like DOCX, PDF, HTML, RTF, XLS, ODT, CSV, or XML.

**Run a report**

1. On the navigation pane for the Reports workspace, expand **Templates**, expand the appropriate Template group, and then select a report.

   The Report screen for the selected report template opens.

2. Click the arrow on the left side of the report template name, and use the criteria panels to limit the results of your report.
Depending on the report, some filters are selected by default (i.e., every severity filter is selected for the All Destinations reports) and others include required fields that must be completed before you can run a report (i.e., you must provide a filter name or filter number to run the Specific Attack report). Your applied filters display in italics to the right of the criteria panel name.

3. (Optional) Click Customize Query to build a custom report formula. For more information about building a criteria query, see Customize a query on page 113.

4. (Optional) From the Last Hour drop-down list, adjust your time frame from the following:
   - Last — Select a standard time interval, such as last minutes, hours, days, or month.
   - User Defined — Type in the field, or click the calendar to select a time duration between two dates (Start Time and the End Time).
   - General — Click Edit to choose a custom range by selecting a day of the month or day of the week, and then specifying the duration in hours and 5-minute intervals.

The first drop-down list relates to the day of the month — From (1st to 31st), To (1st to 31st), and Of (previous or current month). The second drop-down list relates to the day of the week. If you select a day of the month, you cannot select a day of the week and vice versa, unless you select of previous month or current month. The third drop-down list relates to the duration of the report in a 24-hour clock. The fourth drop-down list relates to the duration of the report in five minute increments.

5. Click Run to apply your selected filters.

The report reappears based on the filters you defined. Every report has some document-specific information, such as the name of the report, the page size, and its orientation (landscape).

**Important:** The time required to process a report varies, as many variables affect the amount of time needed for a report to process, such as the time range, the number or type of filters, the number of events accumulated within the time range, and other activities processed by SMS when the report runs including the number of events, additional reports or queries executed at that time, and any database maintenance. Reports run with Last Hour criteria do not include a full hour of data due to an extract, transform, and load (ETL) process that occurs every five minutes. Reports are typically missing a five minute window of events that haven’t been processed through ETL.

**Note:** Percentages in reports are usually rounded to the nearest integer; therefore, total percentages do not always add up to 100.

6. From the generated report, you can perform a variety of functions:
   - **Drill down in to view Event details.** Click a Filter Name in the report to view the Reputation Events for the selected filter name. The criteria for the event matches the criteria that was assigned when the report was generated, such as the name of the filter and the IP address.
   - **Save the report.** Click the save icon to save a report to your computer or a network location; however, if you ultimately want to save the report as a custom template, click Save Report. For more information about saving a report template, see Create a saved report on page 118.
• **Print the report.** Click the print icon to print the whole report, a single page, or a page range. From the print dialog, you can also select the number of copies.

• **View a specific report page.** Use the arrows to go to the next, last, previous, or first page. Alternatively, you can type a page number in the field. By default, the report automatically opens to the first page.

• **Render the report using three zoom types.** Use the document icons to alternate between actual size, fit page, and fit width.

• **Zoom into or out of a report by ratio.** Use the zoom icons to zoom into a report by a ratio that best suits your needs. Alternatively, you can use the zoom drop-down list to set the ratio from 50% to 800%.

**Clear filters**

If you have reports with advanced filters, you can easily reset the filters to expand the results.

1. Open the report to which you applied filters.
2. To the right of a criteria panel, click *Reset* to remove a filter.
3. Click *Reset All* to quickly clear all filters.

**Customize the criteria panels**

Use the Customize Panels feature to dictate how many of the criteria panels you see on the report. At any time, you can configure these panels. The report template dictates which filters are available.

**Change the criteria panels that display on a report**

1. Click the arrow on the left side of the report template name.
   
   The SMS displays the available criteria panels for the selected report.

2. Click *Customize Panels*.
   
   The Criteria Panels dialog opens, and all panels for the report are divided into two list boxes: Available Criteria Panels and Selected Criteria Panels. The panels listed under the Selected Criteria Panels list box are the panels that currently display on the Reports screen.

3. Select a panel name, and then use the directional arrows to add or remove it from your display, respectively. To quickly move all panel names, use the double arrows.

4. Click *OK*.
   
   The Reports screen opens, and your criteria panels reflect your changes.
Customize a query

When defining filters in the criteria panels section of a report, you can select criteria and then customize a query to change the logical operators or criteria grouping.

Create a custom query for a report

1. Click the arrow on the left side of the report template name.
2. The SMS displays the available criteria panels for the selected report.
3. Click Customize Query.
   The Query Structure Editor dialog appears.
4. Type your query in the Query Structure field.
   As you type your query, the syntax displays in the Full Query Expression list box. Syntax that contains errors will automatically display bold, and you will not be able to proceed.
5. Click OK.

Report results

When you run a saved report on the fly or according to schedule, it is added to the Report Results table. The Reports Results table lists the report title, the user who created the report, and the date and time the report was generated. All reports are sorted in reverse chronological order. The number of generated results displays in parenthesis next to the report title.

Open a saved report

1. Expand a saved report title, and then click Results.
2. Select a report title, and then click Open.
3. From the report result, you can perform a variety of functions:
   • Export the report result. Click Export Result to export a report result to a local file, email, or external source.
   • Save the report. Click the save icon to save a report to your computer or a network location.
   • Print the report. Click the print icon to print the whole report, a single page, or a page range. From the print dialog, you can also select the number of copies.
   • View a specific report page. Use the arrows to go to the next, last, previous, or first page. Alternatively, you can type a page number in the field. By default, the report automatically opens to the first page.
• **Render the report using three zoom types.** Use the document icons to alternate between actual size, fit page, and fit width.

• **Zoom into or out of a report by ratio.** Use the zoom icons to zoom into a report by a ratio that best suits your needs. Alternatively, you can use the zoom drop-down list to set the ratio from 50% to 800%.

**Edit result settings and permissions**

1. Expand a saved report title, and then click **Results**.
   - The Report Results table opens.

2. Select a report title, and then click **Edit**.
   - The Edit Report Result wizard opens.

3. On the Result Settings screen, provide the following information:
   - a. Saved Result Name — Update the existing report title as needed.
   - b. Specified Cleanup Date — Select this option, and then click to schedule a date in which the report will be kept until. After this date/time, the report result will be deleted from the SMS.
   - c. No Cleanup — Select this option to keep all report results.

4. Click Permissions, and then select the check boxes to designate who has permission to view the report.

5. Click **OK**.

**Delete a saved report**

1. Expand a saved report title, and then click **Results**.
   - The Report Results table opens.

2. Select a report title. Hold the **SHIFT** key to select multiple sequential reports; hold the **CTRL** key to select two or more non-sequential reports.

3. Click **Delete**.
   - The report is removed from the Saved Reports table and the Reports navigation pane.

**Export report results**

After you save a report, you can export the report data. The main reason to export a reports into another format is to allow more people to view those reports. For example, it may be useful to transform the reports into other, more popular formats like PDF, DOCX, XLS, CSV, HTML, or XML. This way, users can view those reports without having to install special viewers on their systems, which is especially important in the case of documents sent over a network.
Exported results can be in the following formats:

- **PDF** — Generated PDF file accessed using Adobe Reader. This option can include images of graphs.
- **DOCX** — A Microsoft Word document.
- **HTML Attached** — Attached or Embedded Hyper Text Markup Language (a Web page). This option can include images of graphs. These files save in zip files, containing the HTML file and any associated image files.
- **XML** — XML files containing the data for the reports. This file can be used by applications that import XML.
- **CSV** — Comma-Separated-Values file. This file can be opened from common spreadsheet applications including Microsoft Excel.

**Important:** CSV views are unlimited. Exported CSV files could become rather large and cause potential issues when emailing them.

### Export a report result

1. Expand a saved report title, and then click **Results**.

   The Report Results table opens.

2. Select a report title on the Report Results table, or open a saved report, and then click **Next**.

   - **Export to local file** — Browse to and select a file.
   - **Export via email** — Add all the email address that apply, separated by commas; select whether to include a link to the online report; and select one or more report formats.
   - **Export to an external source** — Select whether to include a remote copy/archive. If you select SMB, NFS, or SCP, select one or more formats, and then provide the directory, server, filename, and user credentials.

3. Click **Finish**.

### Report schedules

When you create a report schedule, schedule information is added to the Schedules table. The Schedules table lists the name of the schedule, the report title, the report recurrence, the set end date, and the report status. All schedules are sorted in the order in which they were created. The number of schedules displays in parenthesis at the top of the title.

### Create a new schedule

1. Expand a saved report title, and then click **Schedules**.
The Schedules table opens.

2. Click **New**.

   The Create Schedule wizard opens.

3. On the Schedule screen, select one of the following:
   - Run Now — Immediately execute the report. “Immediate execution” will display on the Report Results and Schedules tables.
   - Run on Schedule — Specify the following:
     - Schedule Name — Enter a name for the schedule in the Schedule Name field.
     - Time — Specify the time. First select a time range option, and then for the selected option, create a custom range. For example, if you want to look at a weekly report, select Weekly, and then define the interval.
     - Duration — Specify when the report schedule will end.

4. Click **Permissions** (or click **Next**), and then select the check boxes to designate who has permission to view the report.

5. Click **Export Results** (or click **Next**), and then do the following:
   a. Email Results — Add all the email address that apply, separated by commas. Alternatively, click **Current User Email** to use the email address of the currently logged in user.
   b. (Optional) Select the **Include HTTP(s) link to online web report** check box to include the logged in user.
   c. Format — Decide in what format you want to send the report.
   d. Remote Copy/Archive — Use the radio buttons to select whether you want to archive the report and enter the remote directory, server, filename, and user credentials. From — Enter the email address where the notifying email originates.

6. Click **Finish**.

   The schedule is added to the Schedule and All Schedules tables.

**Edit an existing schedule**

1. Expand a saved report title, and then click **Schedules**.
2. Select a report title, and then click **Edit**.
3. Edit the report schedule as needed.
4. Click **Finish**.
Delete a schedule

1. Expand a saved report title, and then click **Schedules**.
2. Select a schedule title. Hold the **SHIFT** key to select multiple sequential reports; hold the **CTRL** key to select two or more non-sequential reports.
3. Click **Delete**.

Templates

The SMS includes different types of report templates. Click **Templates** to view a table of all of the template groups and the number of reports available for each template.

To create a report, select a template and modify its settings. All reports are displayed as charts and are listed in a table; depending on the type of report that you select, you may choose a chart type to dictate how you want your data visually presented.

Report permissions

To protect reported data, reporting functions limit access according to user administration settings. All report visibility functions are based on the access level of the user and the security settings for segment groups.

When you create a report, you become the owner of the report. If a report has no owner, then the report and its schedule items and results are visible only to SuperUsers. Saved reports are only visible if the user’s user group has permission to the report. For more information about setting report permissions, see *Managing user groups* on page 560.

Saved reports

The Saved Reports folder (on the Reports navigation pane) displays the report title, results, and schedules for each saved report. From here, you can:

- **Create a saved report.** A fast and easy way to generate a report is to customize an existing report template by using the Create Report wizard to determine the schedule, to set permissions, and to configure where to export the data to.

- **Maintain your saved report library.** Click a report title to view its current template and to run the report. You can update an existing report as needs arise; use a saved report as a template to create a new saved report; and delete unnecessary reports.

- **Track report results.** Use the Report Results table to review a list of every time the report was generated. You can open a report result in a new window; edit the result settings and permissions of a report result; export a report result to a local file, email, or external source; save the report result to a
Create a saved report

The Create Report wizard guides you through the steps for creating a custom report. At a minimum, you must name your report and select a template. Use the icons located in the navigation pane to quickly see if all of the required fields for a category are complete; incomplete categories display a red x, complete categories display a green check mark.

1. On the navigation pane for the Reports workspace, select Saved Reports.

The Saved Report screen displays a table that lists the report title and its corresponding report template.

2. Click Create Report.

The Create Report wizard opens.

Note: You can also access the Create Report wizard if you click Save Report on a report template or Save As on a saved report. For details, see Run a report on page 110.

3. On the Report Name screen, provide the following information:
   
   • Name — Enter a title for the report in the Name field.
   
   • Description — (Optional) Type a description that will help you remember the purpose of the report.
   
   • Template — Select the desired report template from the Template drop-down list.

4. Click Template (or click Next), and then do the following:
   
   a. Report Time Period — From the Last Hour drop-down list, adjust your time frame from the following:
      
      ◦ Last — Select a standard time interval, such as last minutes, hours, days, or month.
      
      ◦ User Defined — Type in the field, or click the calendar to select a time duration between two dates (Start Time and the End Time).
      
      ◦ General — Click Edit to choose a custom range by selecting a day of the month or day of the week, and then specifying the duration in hours and 5-minute intervals.

The first drop-down list relates to the day of the month — From (1st to 31st), To (1st to 31st), and Of (previous or current month). The second drop-down list relates to the day of the week. If you select a day of the month, you cannot select a day of the week and vice versa, unless you select of previous month or current month. The third drop-down list relates to the duration of the report.
in a 24-hour clock. The fourth drop-down list relates to the duration of the report in five minute
increments.

b. Report Row Limit — To help further narrow your result set, enter the number of rows to display
from 1 to 10,000.

5. Click Schedule (or click Next), and then do the following:
   a. Run Now — Select the Run Now check box to immediately execute the report. “Immediate
      execution” will display on the Report Results and Schedules tables.
   b. Run on Schedule — Select the Run on Schedule check box, and then do the following:
      ◦ Schedule Name — Enter a name for the schedule in the Schedule Name field.
      ◦ Time — Specify the time. First select a time range option, and then for the selected option,
        create a custom range. For example, if you want to look at a weekly report, select Weekly, and
        then define the interval.
      ◦ Duration — Specify when the report schedule will end.

6. Click Permissions (or click Next), and then select the check boxes to designate who has permission to
   view the report.

7. Click Export Results (or click Next), and then do the following:
   • Email Results — Add all the email address that apply, separated by commas. Alternatively, click
     Current User Email to use the email address of the currently logged in user.
   • (Optional) Select the Include HTTP(s) link to online web report check box to include the logged
     in user.
   • Format — Decide in what format you want to send the report.
   • Remote Copy/Archive — Use the radio buttons to select whether you want to archive the report
     and enter the remote directory, server, filename, and user credentials. From — Enter the email
     address where the notifying email originates.

8. Click Finish.

   The report is added to the Saved Reports folder (sorted in alphabetical order) and the All Schedules
   table.

Run a saved report

1. Click a saved report title.

   The Report screen for the saved report template opens.

2. Use the criteria panels to limit the results of your report. For details, see Run a report on page 110.

3. Click Run to apply your selected filters.

   The report reappears based on the filters you defined; the report is also added to the Results table.
Edit a saved report

1. Click a saved report title.

   The Report screen for the saved report template opens.

2. Edit the report as needed.

   **Note:** You must edit at least one filter in the report to enable the Save button.

3. Click **Save** to updated the saved report.

Save as a new report

1. Click a saved report title.

   The Report screen for the saved report template opens.

2. Edit the report as needed.

   **Note:** At a minimum, you must enter a different report title to save as a new report.

3. Click **Save As**.

   The Create Report wizard opens. For details, see *Create a saved report* on page 118.

   When you save the new report, the SMS adds it to the Saved Reports folder on the Reports navigation pane.

All schedules

When you schedule a report, the SMS stores the schedule details in two areas: Saved Reports, which separates the schedules for each saved report; and All Schedules, which displays the compiled schedules for all of your saved reports. The All Schedules screen displays the Schedules table. The number of schedules displays in parenthesis. For each schedule, the table lists the custom schedule name, the name of the report, the schedule recurrence and end date, and report status.

From here, you can:

- Drill into the schedule details for a saved report.
- Edit a report schedule.
- Delete a report schedule.

To view schedule details for a report, double-click a schedule.

**Note:** You cannot create a new schedule from the All Schedules screen, nor can you clone an existing schedule. If you want to create a new schedule, go to the Schedules folder for a Saved Report.
**Edit a report schedule**

1. On the navigation pane for the Reports workspace, select **All Schedules**.
2. Select a schedule, and then click **Edit**.
3. Edit the report schedule as needed.
4. Click **Finish**.

**Delete a report schedule**

1. On the navigation pane for the Reports workspace, select **All Schedules**.
2. Select a schedule title. Hold the **SHIFT** key to select multiple sequential reports; hold the **CTRL** key to select two or more non-sequential reports.
3. Click **Delete**.
Profiles

Profiles are a collection of filters on page 152 or rules that provide a method for setting up security configuration options for TippingPoint solutions. The SMS ships with a default Inspection profile on page 135 and a Firewall profile on page 235, along with a standard Digital Vaccine with filters that address known security issues. TippingPoint provides regular updates to the Digital Vaccine along with other tools and services to monitor and respond to security threats to your network.

Planning and using profiles

As you create, import, and customize filter settings and shared settings, the SMS monitors the changes to the profile. The profile acts as a package that encapsulates all filter setting modifications. Every time you distribute updates, you must distribute the profile. You can selectively determine what filter settings and updates to distribute by creating and maintaining multiple profiles. Each profile can be distributed separately to specific devices. When you distribute a profile, you also distribute shared settings, such as action sets, notification contacts, and services.

Note: When SuperUser or Admin User access or authority is specified, the user must have the respective SuperUser or Admin capabilities to perform those tasks. See Authentication and authorization on page 542.

When devising your network security using the TippingPoint system, you should plan to create profiles based on your security needs. For example, you can create custom filter settings or exceptions for profiles to protect external and internal services. In addition, you might have different models of inspection or firewall devices in a sector of your network. You should consider these options and the architecture of devices and related versions as you create, configure, customize, and update profiles on the SMS.

All of the features provided through Profiles affect your system in three levels of security protection:

- **Enterprise-wide** - These settings affect all devices and segments on your network. Examples of enterprise-wide security include shared settings on page 123 and security filter exceptions on page 171 or restrictions on page 170. Digital Vaccines on page 188 and Digital Vaccine Toolkit on page 201 packages also fall under this type of protection, as you can distribute these packages to all of your devices.

- **Device-wide** - These settings affect all of the segments on a particular device. Digital Vaccine on page 188 and Digital Vaccine Toolkit on page 201 packages also fall under this type of protection, as you can distribute these packages to individual devices.

- **Segmental** - (Inspection only) These settings affect only a particular segment or segment group on page 419; segmental settings do not affect an entire device. An example of these includes an inspection profile distributed to a segment group.

Types of profiles

The SMS supports the following types of network security profiles:
• **Inspection profiles** on page 135 — Inspection profiles are a collection of filters that protect and prevent malicious invasion on your network and data.

• **Firewall profiles** on page 235 — Firewall profiles are a collection of rules created to permit or block network traffic between devices separated by the firewall.

## Shared settings

Shared settings include common configuration objects that are shared *enterprise-wide by all profiles on the SMS* on page 122; the SMS does not create a set of shared settings for each profile.

Shared settings include:

- **Action sets** on page 123 — Determine system policy when traffic matches a filter or firewall rule.
- **Notification contacts** on page 129 — Create collections of email, syslog, or SNMP contacts that are used for notification when a policy event occurs.
- **Services** on page 131 — Configure additional ports associated with specific applications, services, and protocols to expand scanning of traffic.
- **SSL servers** on page 132 — Configure threat protection for inbound SSL traffic.

**Note:** To distribute shared settings, you must *distribute the profile* on page 142.

## Firewall shared settings

- **Application groups (Firewall only)** on page 238 — Create groups of applications using query criteria or by selecting applications individually so the groups can be used in other policy settings.
- **Schedules (Firewall only)** on page 237 — Create and manage schedules specifying when to include or exclude traffic evaluation.
- **Security zones (Firewall only)** on page 236 — Create groups of interfaced from one or more devices that can be used to define policy.
- **Service groups (Firewall only)** on page 238 — Create groups of services to make management of services easier.

## Action sets

Action sets determine what the device does when a packet matches a filter. An action set can contain more than one action, and more than one type of action. When you modify or add an action set, the settings change *enterprise-wide* on page 122 for all filters using the action set.

**Note:** To distribute the action set, you must *distribute the profile* on page 122.
Default action sets

The SMS provides default action sets that can be customized for your security policy.

Table 32. Action sets

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Block</td>
<td>Blocks a packet from being transferred to the network.</td>
</tr>
<tr>
<td>Block + Notify</td>
<td>Blocks a packet from being transferred and notifies the SMS management console in the form of an event listing.</td>
</tr>
<tr>
<td>Block + Notify + Trace</td>
<td>Blocks a packet from being transferred, notifies the SMS management console in the form of an event listing, and logs all information about the packet according to the packet trace settings.</td>
</tr>
<tr>
<td>Permit + Notify</td>
<td>Permits a packet and notifies the SMS management console in the form of an event listing.</td>
</tr>
<tr>
<td>Permit + Notify + Trace</td>
<td>Permits a packet, notifies the SMS management console in the form of an event listing, and logs all information about the packet according to the packet trace settings.</td>
</tr>
<tr>
<td>Trust</td>
<td>Allows the traffic stream to continue without comparing it with any other filter rules.</td>
</tr>
</tbody>
</table>

Create or edit an action set

1. Select Profiles > Shared Settings > Action Sets.
2. Do one of the following:
   - Click New to create a new action set.
   - Select an existing action set, and click Edit.
3. Enter a Name for the action set.
4. Select a Flow Control to specify the actions taken with a packet after it triggers a rule.
Table 33. Action sets

<table>
<thead>
<tr>
<th>Select this option:</th>
<th>To ...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Permit</td>
<td>Allow a packet to reach its intended destination.</td>
</tr>
</tbody>
</table>
| Block               | Discard a packet.  
|                     | Select **TCP Reset** to enable the device to reset TCP flows (Source IP, the Destination IP, or both), which ends the session. |
| Quarantine          | Manage internal and external threats by quarantining network connections.  
|                     | This option provides the ability to automate sophisticated responses to security events.  
|                     | When you want to quarantine network traffic on a stack, use an Active Responder policy in the SMS to propagate the IPS Quarantine action set to the stack. For more information, see [Security policy configuration](#) on page 526.  
|                     | When an IP address (address group)/system is quarantined, go to **Responder > Response History** to review the list and manage the status of these systems. |
| Rate Limit          | Define a maximum bandwidth that can be used by traffic that matches filters assigned to the action set.  
|                     | Incoming traffic exceeding this bandwidth is dropped.  
|                     | If two or more filters use the same Rate Limit action set, then all packets matching those filters share the bandwidth. For example, filters 164 (ICMP Echo Request) and 161 (ICMP Redirect Undefined Code) use the same 10 Mbps pipe instead of each filter getting a dedicated 10Mbps pipe.  
|                     | Supported rates are subject to restrictions according to device model. Any of the predefined rates can be used as long as it does not exceed 25 percent of the total bandwidth of the product. |
| Trust               | Allow a packet from a specific IP address to flow through. |

5. Select **Notifications** to establish the contacts to notify about the event.  

   All Email and SNMP contacts are also listed under **Notification Contacts** on page 129.
### Table 34. Notifications

<table>
<thead>
<tr>
<th>Select this option:</th>
<th>To ...</th>
</tr>
</thead>
</table>
| **Management Console** | Notify the SMS and generate an Event when a filter hits.  
**Note:** The Management Console encompasses both the SMS and device LSM, firewall, email addresses, and SNMP servers. The Management Console is a default contact; other contacts must be added on the SMS. |
| **SMS Response** | Associate a Responder Policy when a filter hits.  
**Note:** The Responder Policy must have **Enable Policy** selected to appear in this list. See **Responder** on page 251. |
| **Remote Syslog** | Send filter alerts, which must be configured for every device using that contact, to a syslog server on your network.  
Go to **Admin > Server Properties** to set up the remote syslog server.  
**Caution:** Only use a remote syslog on a secure, trusted network. Remote syslog, in adherence to RFC 3164, sends clear text log messages using the UDP protocol. It does not offer any additional security protections. Therefore, you should not use remote syslog unless you can be sure that syslog messages will not be intercepted, altered, or spoofed by a third party. |
| **Email** | Generate an email message for each contact listed when a filter hits. |
| **SNMP** | Generate an SNMP trap for each contact listed when a filter hits.  
**Note:** SNMP notification contacts require SNMPv2. |

6. Select **Packet Trace** to track the packet. (This option is not available if you select Rate Limit as the Flow Control in Step 4).
Table 35. Packet trace

<table>
<thead>
<tr>
<th>Select this option:</th>
<th>To ...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packet Trace</td>
<td>Capture all or part of a packet.</td>
</tr>
<tr>
<td>Level</td>
<td>Determine how much of a packet to trace.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Full</strong>: The whole packet is recorded.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Partial</strong>: Select how many bytes (64-25,618) the packet trace log records.</td>
</tr>
<tr>
<td>Priority</td>
<td>Set the importance of the information captured.</td>
</tr>
<tr>
<td></td>
<td>If there is a resource shortage, Low priority items are discarded before Medium priority items.</td>
</tr>
</tbody>
</table>

7. If you select Quarantine as the Flow Control in Step 4, select **Quarantine Settings** and **Quarantine Exceptions**.

Table 36. Quarantine settings

<table>
<thead>
<tr>
<th>Select this Quarantine Setting option:</th>
<th>To ...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Thresholds</td>
<td>Configure the Hit Count (1-10,000) and threshold Period in minutes (1-60). You can determine whether to Permit or Block traffic before the threshold period is reached. Select <strong>TCP Reset</strong> to enable the device to reset TCP flows (Source IP, the Destination IP, or both), which ends the session.</td>
</tr>
<tr>
<td>Web Requests</td>
<td>Manage all HTTP traffic from the quarantined addresses. You can configure the SMS to:</td>
</tr>
<tr>
<td></td>
<td>• Block the requests entirely</td>
</tr>
<tr>
<td></td>
<td>• Redirect the client to another Web server that you specify</td>
</tr>
</tbody>
</table>
### Select this Quarantine Setting option:

<table>
<thead>
<tr>
<th>To ...</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Display the quarantined Web page according to options you select.</td>
</tr>
<tr>
<td><strong>Note:</strong> Do not use <code>&lt;frameset&gt;</code> or <code>&lt;form&gt;</code> HTML tags for the message.</td>
</tr>
</tbody>
</table>

### Other Traffic

Configure the response (Block or Permit) to other non-HTTP traffic from hosts listed in the Response History queue.

Go to **Responder > Response History** to review the list.

### Table 37. Quarantine exceptions

<table>
<thead>
<tr>
<th>Select this Quarantine Exception option:</th>
<th>To ...</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Restrictions</strong></td>
<td>Create, edit, or delete a blacklist of IP address groups. This option limits the quarantine action to specific IP addresses within the address groups.</td>
</tr>
<tr>
<td><strong>Exceptions</strong></td>
<td>Create, edit, or delete a whitelist of excluded IP address groups. When a filter hits, the specific IP addresses within the address groups do not receive a response action.</td>
</tr>
<tr>
<td><strong>Quarantine Access</strong></td>
<td>Create, edit or delete a list of IP address groups that hosts can still access regardless of being quarantined. For example, when a host is detected as malicious and is quarantined, you might...</td>
</tr>
</tbody>
</table>

Do one of the following:

- Click **New** to create a new quarantine restriction, exception, or quarantined host.
- Select an existing quarantine restriction, exception, or quarantined host, and click **Edit**.

a. (Optional) Enter a **Name**.

b. To create an unnamed IP address group:

   - Enter the IP address in the **Source** field for the quarantine restriction or exception.
   - Enter the IP address in the **Destination** field for the quarantined host.

   (After you create the action set, go to **Admin > Named Resources > IP Address Groups > Show Unnamed Items** to view this IP address group).

c. To create a named IP address group:

   - Click the **Right arrow** next to the **Source** field for the quarantine restriction or exception.
Select this Quarantine Exception option:

need to allow access to a specific website to remedy the situation.

<table>
<thead>
<tr>
<th>To ...</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Click the Right arrow next to the Destination field for the quarantined host.</td>
</tr>
<tr>
<td>From here, you can search for, select, or create a new IP address group. For more information, see Create or edit named resource groups on page 644.</td>
</tr>
<tr>
<td>(After you create the action set, go to Admin &gt; Named Resources &gt; IP Address Groups to view this IP address group).</td>
</tr>
</tbody>
</table>

8. Click Finish.

To distribute the action set, you must distribute the profile on page 142.

Notification contacts

Alerts are messages that are sent to a specific recipient (either human or machine) when traffic matches a filter that requires notification. These alerts are sent to the notification contact selected on an action set on page 124. When you modify or add a notification contact, the settings change enterprise-wide on page 122.

Note: To distribute the notification contact, you must distribute the profile on page 142.

Set aggregation settings for global contacts

Because a single packet can trigger an alert, attacks featuring large numbers of packets could potentially flood the alert mechanism.

Alert aggregation enables you to receive alert notifications at intervals to prevent this flooding. The first time a particular filter is triggered, a notification is sent to the filter contacts. At the same time, the aggregation timer starts counting down the aggregation period. During the aggregation period, the system counts other matching packets, but no notification is sent. At the end of the aggregation period, a second notification, including the packet count, is sent. The timer and the counter are reset, and continue to cycle as long as matching packets continue to arrive.

Caution: Short aggregation periods can significantly affect system performance. The shorter the aggregation period, the higher the system load. In the event of a flood attack, a short aggregation period can lead to system performance problems.

1. Select Profiles > Shared Settings > Notification Contacts.
2. Enter a Management Console Aggregation in minutes from 0 to 10,800.
3. Enter a **Device Remote Syslog Aggregation** in minutes from 0 to 10,800.
4. Click **Save**.

**Create or edit an email notification contact**

To use email contacts, you must complete the Mail Server panel of the Configuration window for each device.

1. Select **Profiles > Shared Settings > Notification Contacts**.
2. Under **Email Contacts**, do one of the following:
   - Click **New** to create a new email notification contact.
   - Select an existing contact, and click **Edit**.
3. Enter the **Name** of the contact.
4. Enter the **Email Address** (up to 36 characters) for the contact.
5. Set the **Aggregation** for the number of minutes that the device will accrue alerts before it sends a notification.

   The SMS limits the number of email alerts sent in a minute. By default, the SMS sends 10 email alerts per minute. On the first email alert, a one minute timer starts, counting the number of email alerts to send according to the configured limit. Email alerts beyond the limit in a minute are blocked. After one minute, the system resumes sending email alerts. If any email alerts were blocked during that minute, the system logs a message to the system log.

6. Click **OK**.

To distribute the notification contact, you must *distribute the profile* on page 142.

**Create or edit an SNMP notification contact**

SNMP notification contacts require SNMPv2 and will not work when SNMPv2 is disabled.

1. Select **Profiles > Shared Settings > Notification Contacts**.
2. Under **SNMP Contacts**, do one of the following:
   - Click **New** to create a new SNMP notification contact.
   - Select an existing contact, and click **Edit**.
3. Enter the **Name** of the contact.
4. Enter the **SNMP Host** for the contact.
5. Enter the **Port** number for the contact’s SMNP host (the default port number is 162).
6. Enter the **SNMP Community String**.
This must be the same community string that is set up on the SNMP host used to receive the notification.

7. Set the **Aggregation** for the number of minutes that the device will accrue alerts before it sends a notification.

8. Click **OK**.

To distribute the notification contact, you must *distribute the profile* on page 142.

**Services**

To enhance scanning and detection of malicious traffic, the SMS provides management of services. You can configure additional ports associated with specific applications, services, and protocols to expand scanning of traffic. When filters scan traffic against the standard ports for listed services, the SMS accesses and scans traffic against the list of additional ports.

**Note:** You can configure up to 16 additional ports for each service other than HTTP. For HTTP, only eight additional ports are allowed.

**Add or edit a non-standard port for a service**

1. Select **Profiles > Shared Settings > Services**.
2. Select a **Service**, and click **Edit**.
3. Select **TCP/UDP Ports** to view the TCP and UDP ports for the selected service.
4. Do one of the following:
   - Click **Add** to specify a TCP or UDP protocol and assign a port range or a single port.
   - Select an existing port, and click **Edit**.
5. Specify a **Protocol**.
   - Select **Both** to create a protocol with the same port information TCP and UDP. This option is only available when you create a new protocol.
6. Do one of the following:
   - Select **Port**, and enter a port number to assign a single port.
   - Select **Range**, and enter a Start and End port number.
7. Click **OK**.

After you modify a non-standard port for a service, you must *distribute the profile* on page 142.
SSL servers

You can add an SSL server to specify the SSL server configuration, including the SSL service that is accepted on the SSL detection port.

For secure HTTP, IMAP, and POP3 traffic, create a separate SSL server to enable DV filtering on the decrypted SSL service. For example, if the web server accepts POP3S traffic on port 2000, add an SSL server with a Detection Port of 2000 and a Decrypted Service of POP3 to enable DV filters for POP3.

For other SSL services, such as SMTPS, create an SSL server with a Detection Port that identifies the secure traffic, and a Decrypted Service of Other. The 2200T applies DV filters to the incoming traffic, but does not apply DV filters to the decrypted SSL service.

To inspect more than one decrypted service on a particular SSL server, define the same server IP for each service you want. For example, you can define a server with IP 1.1.1.1 and port 443 (HTTPS), and another server with IP 1.1.1.1 and port 995 (POP3S), and associate them with the same SSL inspection profile.

Add or edit an SSL server

From the SMS, add an SSL server to specify the SSL server configuration, including the SSL service that is accepted on the SSL detection port.

**Tip:** To view a summary of the existing SSL server configurations, click **Profiles** on the SMS toolbar. Then, in the navigation pane, select **Profiles > Shared Settings > SSL Servers**.

For secure HTTP, IMAP, and POP3 traffic, create a separate SSL server to enable DV filtering on the decrypted SSL service. For example, if the web server accepts POP3S traffic on port 2000, add an SSL server with a Detection Port of 2000 and a Decrypted Service of POP3 to enable DV filters for POP3.

For other SSL services, such as SMTPS, create an SSL server with a Detection Port that identifies the secure traffic, and a Decrypted Service of Other. The TPS applies DV filters to the incoming traffic, but does not apply DV filters to the decrypted SSL service.

To inspect more than one decrypted service on a particular SSL server, define the same server IP for each service you want. For example, you can define a server with IP 1.1.1.1 and port 443 (HTTPS), and another server with IP 1.1.1.1 and port 995 (POP3S), and associate them with the same SSL inspection profile.

To add or edit an SSL server

1. Select **Profiles > Shared Settings > SSL Servers**.
2. In the SSL Server tab of the SSL Servers panel, click **New** or **Edit**.
3. In the **SSL Server** tab, specify the following settings:
   - **Name**: Enter the server name, for example, `myapp_pop3`.
     (Best Practice) Name the server so that you easily associate it with your web server.
   - **Destinations**: Specify the server IPv4 address or CIDR range.
Detection Ports: Specify the port range of the encrypted application traffic. For example, if the web server accepts POP3S traffic on port 2000, specify 2000.

Certificate: Select the SSL certificate for your web server. You can import a certificate now, or if you have already imported a certificate into the SMS certificate repository, simply choose the one you want.

Decrypted Service: Choose the SSL service that is accepted on the SSL Detection Port to enable filtering for that particular service. If the SSL service you want is not listed, choose Other.

Rekey Interval: Specify the interval, in seconds, that your web server forces renegotiation of the shared SSL key. If your web server does not offer renegotiation of the shared SSL key, leave this blank.

Enable logging: Select this option to enable the TPS to write log information about SSL inspection to the external user disk (CFast or SSD). This option collects detailed logging information and should only be enabled for troubleshooting purposes. For example, enable this option if, after you set up SSL inspection, the TPS device does not see SSL session activity. By default, this option is disabled. For information about viewing log information, see Verify SSL inspection activity on page 669.

Allow compression: Select this option to allow the SSL compression algorithm to be negotiated during the SSL handshake. If your web server does not offer negotiation of SSL compression, disable this option. By default, this option is disabled. If you select this option, and your web server does not offer SSL compression, this setting is ignored.

Send TCP reset to server for blocked sessions: Select this option to always send a TCP reset to the server whenever the TPS blocks an SSL session. This option overrides the TCP reset action set, if enabled, on a DV filter.

(Best Practice) Enable this option so that protected servers can release network resources quickly if flows are blocked. When this option is disabled, the TCP reset action, if enabled on a DV filter, still applies.

4. In the Cipher Suites tab, choose the protocols and algorithms that are supported by your web server.

The Cipher Suite list automatically updates based on your selections. Deselect any cipher suites that you do not want.

5. Click OK.

6. Assign the SSL Server to an SSL inspection policy. See the next section for more information.

Refresh certificate status

Click Refresh Certificate Status to update the status of the certificate. This status displays on the tooltip on the list of SSL Servers defined on the SMS. They are used in SSL Inspection policies that are part of an Inspection profile.
SSL Inspection policy

On the SMS, you can add an SSL Inspection policy to specify the SSL traffic that you want to protect for particular segments on a managed device. An SSL Inspection policy is a set of SSL profiles, each of which specifies an SSL server and a list of source IP address groups exceptions. Assign the SSL inspection policy to the inspection profile that carries the traffic of interest.

1. Select Profiles > Inspection Profiles > [Profile Name] > SSL Inspection Policy.
2. Do one of the following:
   - Click New to create a new SSL inspection policy.
   - Select an existing SSL inspection policy, and click Edit.
3. Select the Locked check box to lock the SSL inspection policy.
4. Enter a Name for the SSL inspection policy.
5. Specify the following settings:
   - **Enabled:** Clear the check box to exclude this SSL server policy from the SSL inspection profile. By default, this option is selected.
   - **Server:** Choose a server to include in the SSL inspection policy.
   - **Source Exceptions:** Do one of the following:
     - Click Add to create a new source exception.
     - Select an existing source exception, and click Edit.
       a. (Optional) Enter a Name.
       b. To create an unnamed IP address group, enter the IP address in the Source IP Address field.
          (After you create the SSL inspection policy, go to Admin > Named Resources > IP Address Groups > Show Unnamed Items to view this source IP address group).
       c. To create a named IP address group, click the Right arrow next to the Source IP Address field.
          From here, you can search for, select, or create a new IP address group. For more information, see Create or edit named resource groups on page 644.
          (After you create the SSL inspection policy, go to Admin > Named Resources > IP Address Groups to view this source IP address group).
6. Click OK.
Inspection profiles

Each profile contains a set of filters on page 152 that you can modify with custom settings, including action sets, exceptions, and selected notification contacts. The SMS supports individual and multi-filter edits. You can also edit multiple profiles.

After you copy/create filters, modify settings, and update shared settings, you must distribute the changes to the devices managed by the SMS.

Note: When you edit filters from Events on page 58, the system accesses the last profile distributed to the device. The profile must be distributed to the device before those changes take effect.

Table 38. Inspection profile tasks

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Import Profiles</td>
<td>Import as a new profile, or replace an existing profile with the option to add new settings or change existing settings.</td>
</tr>
<tr>
<td>Export Profiles</td>
<td>Export an existing profile to either a local file, the SMS http server, or an external SMB or NFS server.</td>
</tr>
<tr>
<td>Distribute Profiles</td>
<td>Distribute a profile to devices in your network.</td>
</tr>
<tr>
<td>Create Profiles</td>
<td>The SMS builds the profile based on the currently activated Digital Vaccine settings on page 188.</td>
</tr>
<tr>
<td>Copy Profiles</td>
<td>Save an existing profile using a different name. When you create a copy of a profile, you create a complete duplicate of the original profile. The name has the words “Copy of” with the original name appended to it. You can edit the name of the profile on page 140.</td>
</tr>
<tr>
<td>Compare Profiles</td>
<td>Select up to three profiles to compare the differences between profiles, such as category settings and filters.</td>
</tr>
<tr>
<td>View Profile Details</td>
<td>View profile details and edit the Deployment Mode on page 136.</td>
</tr>
</tbody>
</table>
### Task

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete Profiles on page 149</td>
<td>Remove a profile.</td>
</tr>
</tbody>
</table>

### Default Inspection profile

The SMS ships with a **Default** profile that can be used out-of-the-box to start protecting your network. The Default Inspection profile includes the default set of filters on the SMS. You can [copy the Default profile](#) on page 138. You can also [edit the filters within this profile](#) on page 166 or [edit the profile details](#) on page 140.

### Inspection profile inventory

You can view a list of all of the Inspection profiles on the SMS including top-level information and profile hierarchy. To see all the profiles in a hierarchy, expand the top-level profile entry. Every profile includes a [version number](#) on page 140 and Deployment Mode on page 136. **Changed** indicates whether the profile has changed since the last time it was distributed or if the current version on the SMS is the same version that was distributed to your devices.

### New profiles

When you create a new profile, the following options can help you to target specific deployments and leverage existing profiles.

### Deployment mode

TippingPoint Digital Vaccines (DV) version 3.2 and later contain deployment settings for filters that address specific types of deployments.

When you create a new profile, you can use the **Default** deployment mode or choose from a list of available deployment modes, and the device will use the recommended filter configuration for that deployment.

Depending on your network, it might be necessary to tune the selected deployment mode by [overriding specific filters](#) on page 166 or [categories](#) on page 166.

### Table 39. Deployment modes

<table>
<thead>
<tr>
<th>Deployment mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>Provides a balance between high quality security and appliance performance and are suitable for most deployments.</td>
</tr>
<tr>
<td>Deployment mode</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Security-Optimized</td>
<td>Favors additional security over network performance or application adherence to protocol standards and is a subset of the Hyper-Aggressive deployment mode. Enables more Zero Day Initiative (ZDI) protection than other deployment modes.</td>
</tr>
<tr>
<td>Performance-Optimized</td>
<td>Emphasizes network performance over security and is not recommended for use in a production environment. It is intended for testing purposes only.</td>
</tr>
<tr>
<td>Core [Deprecated]¹</td>
<td>Offers improved performance for devices that are deployed on the interior of a network, with the expectation that perimeter-facing devices block most malicious Internet traffic.</td>
</tr>
<tr>
<td>Edge [Deprecated]¹</td>
<td>Ideal for Web farms and DMZs that typically expose services to the Internet.</td>
</tr>
<tr>
<td>Perimeter [Deprecated]¹</td>
<td>Offers optimal security for devices deployed on the perimeter of a network and protects the network from Internet traffic.</td>
</tr>
</tbody>
</table>

¹ Deprecated deployment modes include new filters added to the DV, but the new filters in the deprecated deployment modes have the same characteristics as the Default deployment mode.

**Note:** To use this feature, a v3.2 or later DV must be activated on the SMS. The deployment mode setting is available only for DV versions that support this option. For more information, see the Digital Vaccine documentation on the TMC.

**Inheritance**

Profiles can be set up with a hierarchy and profile attributes can be inherited. Profiles with inherited setting cannot be edited if the main profile is locked. For each profile in the hierarchy, the following items can be inherited from the profile in the next level up:

- *Security filter exceptions and restrictions* on page 170
- *Application filter restrictions* on page 172
- *Reputation exceptions* on page 178
- *Category settings* on page 166
• Filters from the *DV* on page 188, *Auxiliary DV* on page 198 and *Digital Vaccine Toolkit Packages* on page 201

• *Advanced DDoS filters* on page 173

• *Reputation filters* on page 175

• *Traffic Management filters* on page 185

**Create a new profile**

**Note:** If a filter has inherited settings and the base filter is locked, the filter with inherited settings cannot be edited.

1. Select **Profiles > Inspection Profiles**.
2. Click **New**.
3. Enter the following information for the profile:
   a. Enter a **Name** for the profile.
   b. Select a **Deployment Mode** on page 136.
   c. Select the **Client IP (X-Forwarded-For & True-Client-IP)** check box if you want the profile to identify whether packets associated with an inspection event were forwarded for another IP address. When possible, the device will detect this and provide the original Client IP address in the Inspection Events.
   d. Select the **HTTP Context (Hostname, URI, Method)** check box if you want the profile to identify information associated with any HTTP URI. When possible, the devices will detect this and provide the HTTP hostname, URI, and method in the Inspection event.
   e. **Inheritance** — Option to choose a profile for inherited settings on page 137.
   f. **Description** — Brief description for the profile.
4. Click **OK**.

**Use the ‘Save As’ option to copy a profile**

Saves an existing profile using a different name.

1. On the Profiles navigation pane, expand **Profiles**, and then click **Inspection Profiles**.
2. Select a profile from the Inventory pane, and then click **Save As**.

   The Save Profile As dialog box displays. The selected profile is copied with “Copy of” and the name appended of the original as the profile name. This copied profile includes all filters of the original profile.
3. Enter a **Name**.

   The default name is “Copy of” added to the copied profile name.
4. Select the **Capture Client IP** check box if you want the profile to identify whether packets associated with an inspection event were forwarded for another IP address. When possible, the devices will detect this and provide the original Client IP address in the Inspection event.

5. For **Inheritance**, select **Profile** and specify profile for inherited settings if you want the profile to inherit settings from another profile. Leave **None** selected if you do not want to inherit settings.

6. Enter a **Description**.

7. Click **OK**.

**View profile details and versions**

For every inspection profile you create, the SMS tracks information about the profile when you distribute the profile to a device.

Select **Profiles > Inspection Profiles > [Profile Name] > Details** or **Versions** to access this information. Alternatively, you can double-click a profile in the navigation pane to access the individual tabs.

**Details**

The **Details** tab provides the most current profile information including details about the profile, the profile distribution schedule, and the profile distribution details.

**Profile details**

Profile details include the following:

- **Name** - Name of the profile.
- **Inheritance** - Profile name or series of profile names that indicate the hierarchy for the inherited settings.
- **Active Version** - Version number of the profile that is currently active.
- **Deployment Mode** - Deployment settings for DV filters that address specific types of deployments.
- **Capture Additional Event Information** - Configuration for identifying a request’s source IP address before it is overwritten by a forwarding proxy IP address, and for identifying the true source of an HTTP request.
- **Last Modified** - Date and time changes were made to the profile.
- **Description** - Brief description of the profile.

**Profile distribution schedule**

The profile distribution schedule displays information about scheduled distributions. From here, you can create a **New Schedule** for the profile.

**Profile distribution details**
The profile distribution details area displays information on the distribution of the selected profile to your devices. Profile distribution details include the following:

- **Distribution Target** - Segment or segment group that received the profile distribution.
- **Distributed** - Date and time of the last profile distribution.
- **Version** - Version of the profile that was distributed.
- **Changed** - Yes indicates there is a changed version of the profile that has not been distributed.

**Versions**

For every inspection profile you create, the **Versions** tab provides the most current profile information about all versions of the selected profile including, whether the profile is active, its version number, when last distributed to your devices, and any comments.

As you modify or make changes to a profile, the version for that profile displays as a point release. For example, three changes to a profile moves the version from 1.0 to 1.3. When you distribute or create a snapshot of this profile, the version is committed and is displayed on the screen as 1.3. Subsequent changes to that profile move the version number up a major level to 2.0. Any changes made prior to the next distribution of the profile are indicated as a minor or point release number. Changes made after the distribution of a profile begin with a major number allowing you to keep track of distributed profile versions.

**All Versions**

The All Versions area includes the following items:

- **Active** - Displays a check mark for the active version of the profile.
- **Version** - Version of the profile.
- **Created** - Date and time the profile was created.
- **Distributed** - Date and time of the last profile distribution.
- **Comment** - Profile comments.

**Edit profile details**

1. Review the information in *New profiles* on page 136.
2. Select the **Profiles > Inspection Profiles > [Profile Name] > Details** tab.
3. Click **Edit Details**.
4. Make any necessary changes:
   - Enter a **Name** for the selected profile.
   - Select a **Deployment Mode** for filters related to specific types of deployments. See *New profiles* on page 136.
• Select the **Client IP** check box to capture the originating IP address of a client using X-Forwarded-For (XFF) or True-Client-IP technology.

• Select the **HTTP Context** check box to convert the relative URI value to an absolute value.

  **Note:** This check box must be selected if URL Reputation filtering is enabled for the profile.

• Enter a **Description** for the selected profile.

5. Click **OK**.

### Create a snapshot of a profile version

1. Select **Profiles > Inspection Profiles > [Profile Name] > Details**.

2. Click **Snapshot**. A snapshot of the current version of the profile is created.

  **Note:** If you delete a profile, you will lose all snapshots associated with the profile. Profile snapshots are saved as part of the profile data and will be deleted along with the other data.

3. Click the **Versions** tab.

   The new entry displays in the All Versions table.

### Activate a profile version

**Named IP address groups**

When you activate a profile that contains a named IP address group (for a *filter exception* on page 168, a *quarantine exception* on page 128, an *Advanced DDoS filter* on page 173, an *SSL inspection policy* on page 134, or a *Traffic Management filter* on page 186), the SMS verifies whether the named IP address group already exists. This ensures that the enforcement of policies, including exceptions, are restored when you activate a previous profile snapshot.

• The SMS assigns one IP address group for each imported IP address group.

• If the named IP address group exists and the values are an exact match (IP address group contains the same IP addresses), then the SMS keeps that existing named IP address group for the profile.

• If the named IP address group exists but the values are not an exact match, then the SMS adds each named IP address group, and each named IP address group is identified with an underscore and a number (for example **NamedIPAddress_1**, **NamedIPAddress_2**, **NamedIPAddress_3**, and so on).

• If the named IP address group does not exist on the SMS, the SMS adds it as an unnamed resource. See **Named resources** on page 642.

1. Review the information in **View profile details and versions** on page 139.

2. Select the **Profiles > Inspection Profiles > [Profile Name] > Versions** tab.

3. Select a profile version, and click **Activate**.
The selected profile activates as the current profile and replaces all filter changes with changes from the snapshot.

**Distribute profiles**

When you distribute a profile, you send the modified and updated profile to selected segments or devices. To control which updates segments receive, you can create segment groups. Segment groups manage segments into specific groups within the system. You can then send profile updates, including all custom changes to filters, shared settings, action sets, and notification contacts according to the group.

When distributing a profile, you can also select to distribute to the entire segment group, a single segment, several segments, or a combination of segments and segments groups. See *Virtual segments* on page 416.

For ease of monitoring, Profile Distribution dialog groups the distribution tasks by status. The groups include Pending, Succeeded, Failed or Canceled.

⚠️ **Caution:** When you enter a significant number of changes to filters within a profile, the period of time required for distributing the profile increases. If you unsuccessfully distribute profiles due to time-out, contact a TippingPoint technical support representative to assist in extending the time-out setting for your profile distribution needs.

Review the following considerations before you distribute a profile.

**Segment groups**

Create a profile for specific segments before you create a segment group.

**Required distributions**

Filter modifications that require a distribution include the following items:

- New, modified, or deleted shared and custom filter exceptions.
- New, modified, or deleted filters.
- Modified traffic management filters, or when you change the order of the traffic management filters. For more information, see *Traffic Management filters* on page 185.

**DV version verification**

When you distribute a profile, the SMS verifies that all managed devices run the same Digital Vaccine (DV) and DV Toolkit version. The SMS displays an alert if a device will receive a profile with a different DV or DV Toolkit version from the version that is installed on the device. You can avoid this warning and maximize the effectiveness of your profile filters if you distribute the active DV or DV Toolkit to the device before you distribute the profile.

**High/low priority distributions - performance**

When you distribute a profile, you can select a high or low priority, which aids in the performance of the device.
• High priority updates run before low priority updates.
• Low priority updates are regulated to ensure the best performance of the system.

During high priority updates, you may experience dropped packets as traffic and performance are hampered during the update. To avoid losing packets, you can select a low priority. From a device perspective, when the traffic through the device is low (or in Layer-2 Fallback), you should always do high priority updates from the SMS. Selecting low priority updates can take hours to perform a full update but there is less risk of loss in traffic packets.

To designate a distribution as High Priority, select the High Priority check box at the bottom of the Inspection Profile Distribution dialog.

Named IP address groups

IPS devices are not aware of Named Resources - the SMS maps IP addresses to Named Resources to provide an improved user experience.

When you distribute a profile that contains named IP address groups, the SMS sends every combination of the source and destination IP address pairs to the device. For example, if a filter exception has a source and destination named IP address group and each group has two IP addresses, then the SMS will send four filter exceptions to the device, and each exception will contain a pair of source and destination IP addresses. You can view these combinations on the device LSM.

The SMS enforces the maximum number of Traffic Management filters that can be distributed to a device based on device capacity. For more information, see Traffic Management filters on page 185.

Manual profile distribution

The SMS provides a straightforward method that allows you to manually distribute a profile to a device segment or group.

Cancel a distribution in progress

1. On the Profiles navigation pane, expand Profiles, and then click Inspection Profiles.
2. Select a profile in the Distribution Progress pane.
3. To view distribution progress, click Details or right-click and select Details.
4. Click Stop Distribution.

Note: A profile distribution can only be cancelled before it enters the installing state. After a device begins installing the package, the distribution cannot be cancelled. If the cancel button is grayed out, the distribution cannot be cancelled.
Distribute multiple profiles

Selecting multiple profiles to distribute together allows you to save time. Each profile must still be targeted to a specific group, but you can configure the distribution of the profiles so they will all start distributing when you click OK.

There is a safety feature built into the Inspection Profile Distribution dialog when you have selected multiple profiles. To avoid accidentally distributing a profile, you can deselect the Distribute this profile when I click ‘OK’ check box. This will do two things:

- Prevent you from editing the targets for the profiles
- Cancel distribution of the profiles if you click OK. This allows you to distribute some profiles when you click OK, but not distribute others without losing work. For example, if you have spent the past 20 minutes configuring the profile distribution of 5 profiles and realize you don’t have the information you need to distribute the 6th profile, you can select that profile and deselect the check box. When you click OK, the other profiles will distribute but the 6th profile will not.

1. On the Profiles navigation pane, expand Profiles, and then click Inspection Profiles.
2. Select the profiles in the Inventory pane, and then click Distribute. The Inspection Profile Distribution dialog displays. The selected profiles will display in the left panel. Select the first profile you want to distribute.
3. To distribute a profile to IPS Segments:
   a. Select the IPS Segments tab.
   b. To Allow Segment Selection, choose one of the following items from the Organize By drop-down box:
      • Segment Group
      • Device
4. For a high priority distribution, select the High Priority check box.
5. Repeat steps 3-6 until you have finished configuring all of the profiles.
   If there is a profile you do not want to distribute at this time, clear the Distribute this profile when I click ‘OK’ check box for that profile.
6. Click OK.

The system begins the distribution of the profile to all devices in the selected segment group. The progress of the profile according to device displays in the Distribution Progress section. See Segment groups on page 419 and Distribution queue configuration – TPS and IPS (S-Series, N-Platform, and NX-Platform) on page 345.

⚠️ Caution: When you enter a significant number of changes to filters within a profile, the period of time required for distributing the profile increases. If you un successfully distribute profiles due to time-
out, contact a TippingPoint technical support representative to assist in extending the time-out setting for your profile distribution needs.

Distribute an inspection profile to inspection segments

**Note:** When you enter a significant number of changes to filters within a profile, the period of time required for distributing the profile increases. If you unsuccessfully distribute profiles due to time-out, contact a TippingPoint technical support representative to assist in extending the time-out setting for your profile distribution needs.

1. Select **Profiles > Inspection Profiles**.
2. Select a profile, and click **Distribute**.
3. To distribute the profile to inspection segments:
   a. In the Targets section, select the **Inspection Segments** tab.
   b. To Allow Segment Selection, choose one of the following items from the **Organize By** drop-down box:
      - Segment Group
      - Device
   c. Select the appropriate group(s).

   For information about how you can distribute inspection profiles to a stack of devices, see *Security policy configuration* on page 526.

4. For a high priority distribution, select the **High Priority** check box.

Compare profiles

You can select up to three profiles to compare the differences between profiles, such as category settings and filters.

1. Select **Profiles > Inspection Profiles**.
2. Do one of the following:
   - Press the **SHIFT** key and select up to three profiles from the list, and then click **Compare**.
   - Press the **CTRL** key and select up to three profiles from the list, and then click **Compare**.

   The Profile Compare screen displays with tabs for the following areas of comparison: category settings, filters, traffic management filters, advanced DDoS filters, reputation filters, and profile settings.

3. Select the **Filter** tab, and then select the **Show Differences Only** check box to only view the differences in the selected profiles. A yellow triangle in the **Diff** column indicates that one or more entries in that row are different.
4. To make changes, select:
Import profiles

You can import an existing profile from a local file, from a device segment, or from another SMS.

Profile import filter behaviors

When you import a profile, certain changes take place depending on the type of filters in the profile and the option (new, replace, combine) that you select. For example, when you import a profile that has shared settings, such as services running on non-standard ports, all existing profiles will receive the additional ports.

Table 40. Profile import filter behaviors

<table>
<thead>
<tr>
<th>Filter</th>
<th>New</th>
<th>Replace</th>
<th>Combine (add)</th>
<th>Combine (change)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traffic Management</td>
<td>Adds new</td>
<td>Delete and add all new</td>
<td>Adds all at top of list (default).</td>
<td>Adds all at top of list (default).</td>
</tr>
<tr>
<td>Advanced DDoS</td>
<td>Adds new</td>
<td>Delete and add all new</td>
<td>Adds all (unordered).</td>
<td>Adds all (unordered).</td>
</tr>
<tr>
<td>Category Settings</td>
<td>Adds all new</td>
<td>Delete and add all new</td>
<td>Adds individual category if non-DV default. Does NOT overwrite user-modified filters.</td>
<td>Adds individual category if non-DV default. Overwrites user-modified filters.</td>
</tr>
<tr>
<td>Profile Settings</td>
<td>Adds all new</td>
<td>Delete and add all new</td>
<td>Adds non-duplicated address pairs.</td>
<td>Adds non-duplicated address pairs.</td>
</tr>
</tbody>
</table>

Named IP address groups

When you import a profile that contains a named IP address group (for a filter exception on page 168, a quarantine exception on page 128, an Advanced DDoS filter on page 173, an SSL inspection policy on page
134, or a *Traffic Management filter* on page 186), the SMS verifies whether the named IP address group already exists.

- The SMS assigns one IP address group for each imported IP address group.
- If the named IP address group exists and the values are an exact match, then the SMS keeps that existing named IP address group for the profile.
- If the named IP address group exists but the values are not an exact match, then the SMS adds each named IP address group, and each named IP address group is identified with an underscore and a number (for example NamedIPAddress_1, NamedIPAddress_2, NamedIPAddress_3, and so on).
- If the named IP address group does not exist on the SMS, the SMS adds it as an unnamed resource. See *Named resources* on page 642.

**Import a profile**

1. Select **Profiles > Inspection Profiles**.
2. Click **Import**.
3. On the Profile Import wizard, do one of the following, and then click **Next**:

**Table 41. Import options**

<table>
<thead>
<tr>
<th>Select this option:</th>
<th>To ...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Import from local file</td>
<td>Browse to and select an inspection profile.</td>
</tr>
<tr>
<td>Import from Device Segment</td>
<td>Select a segment.</td>
</tr>
<tr>
<td>Import from another SMS</td>
<td>Select an SMS Server, enter and confirm your login credentials, and select an Inspection profile.</td>
</tr>
</tbody>
</table>

4. On the Import Action wizard, do one of the following, and then click **Next**:
Table 42. Create, combine, or replace profile

<table>
<thead>
<tr>
<th>Select this option:</th>
<th>To ...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create</td>
<td>Create a new profile name. Select the <strong>Use name embedded in package file</strong> check box to use the embedded name, if available. Select an <strong>Inheritance</strong> option to inherit profile attributes. See <em>New profiles</em> on page 136.</td>
</tr>
<tr>
<td>Combine</td>
<td>Combine the existing profile with the imported profile, and select an Inspection profile.</td>
</tr>
<tr>
<td>Replace</td>
<td>Replace the existing profile with the imported profile, and select an Inspection profile.</td>
</tr>
</tbody>
</table>

5. Review the summary information, and click **Finish**.

### Export profiles

You can export an existing profile to a local file, the SMS HTTP server, or an external SMB or NFS server.

1. Select **Profiles > Inspection Profiles**.
2. Select a profile, and click **Export**.
3. Do one of the following, and then click **Next**:

Table 43. Export profile options

<table>
<thead>
<tr>
<th>Select this option:</th>
<th>To ...</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Export to local file</strong></td>
<td>Browse to the local destination, and enter the package name.</td>
</tr>
<tr>
<td><strong>Export to local SMS Exports and Archives</strong></td>
<td>Enter the package name and export the profile to a local SMS. The exported file can be viewed and accessed from the Exports and Archive section of the SMS Web interface. See <em>Exports and archives</em> on page 645.</td>
</tr>
<tr>
<td><strong>Export to External Source</strong></td>
<td>Select <strong>SMB</strong> or <strong>NFS</strong>, and complete the required information.</td>
</tr>
</tbody>
</table>
Select this option: | To ...
---|---
| To export to a NFS Server, the SMS must have write-permission for the anonymous user on the directory exported by the specified NFS server.

Export directly into one or more SMS servers

Click Add, and provide the SMS Server IP address and credentials. If you are exporting the profile to one or more SMS servers, you have the option to create a new profile or merge the profile with the existing profile. Choose one of the following options:

a. Create a new profile: Enter the Profile Name and specify any inheritance information.

b. Use an existing profile: Select an existing profile with the imported profile. Select Combine or Replace, and then select an existing profile from the drop-down list.

4. Review the summary information, and click Finish.

Delete profiles

When you delete a profile, you delete all data relating to that profile including profile snapshots. However, events that have been generated by the profile will remain accessible.

1. Select Profiles > Inspection Profiles.
2. Select one or more profiles, and click Delete.

Inspection profile filters

Profiles provide a management facility for packaging and distributing filters to your devices. Filters provide information and instructions for the devices protecting your network against malicious attacks. These filters enable your devices to monitor and respond to network traffic according to a particular pillar, or type. These pillars separate filters into types that apply to different attacks and sections of your network. You can create, modify, and manage these filters to block and protect against malicious attacks and piracy of your bandwidth and network services. Each filter consists of customizable options and settings that detail how the system should monitor, investigate, process, and block traffic.

If the SMS identifies traffic that matches a filter, it responds to that traffic based on the instructions defined in the action set for the filter. All action sets require a flow control action—the SMS can block, permit, or a react in a combination of ways to the traffic. As an added measure of safety and information dissemination, you can configure alerts to inform interested parties about detection and responses to malicious attacks and usage by notifying the SMS and device LSM management consoles or sending emails to specified email
addresses. You can also log information about matching traffic to a packet trace log or a remote syslog server for review and reporting.

All filters are assigned to protect a segment on your system. When you change the settings of these filters, only the target distribution segments receives the changes. You can also create Segment Groups on page 419 to configure filter settings to a grouping of selected segments.

**Note:** When a device is added on the SMS, any unused virtual ports (those that are not in a virtual segment in a profile) are deleted on the SMS. To keep any unused virtual ports, put them into a virtual segment as SMS valid combinations before adding your device. See Virtual segments on page 416.

**Filters**

Filters are a key to protection and prevention of malicious invasion on your network. The SMS includes the following sets of filters:

- Security filters on page 169
- Application filters on page 172

**Profile overview**

You can view detailed information regarding modifications of a specific Inspection profile including category settings, filters, restrictions and exceptions, and shared settings. You can create a snapshot of a profile version on page 141. You can also distribute the profile on page 142.

**Table 44. Profile overview**

<table>
<thead>
<tr>
<th>Click this tab:</th>
<th>To ...</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Category Settings</strong></td>
<td>View the state of each category (Enabled or Disabled), and the action set on page 123 for the category (Recommended is the default setting for filters). You can edit the category settings on page 166 for a group of filters.</td>
</tr>
</tbody>
</table>

- Application Protection filters on page 152 — Defend against exploits targeting applications and operating systems. These filters include a variety of security filters on page 169 and application filters on page 172.
- Infrastructure Protection filters on page 155 — Protect network bandwidth and network infrastructure elements.
- Performance Protection filters on page 156 — Allow key applications to have prioritized access to bandwidth ensuring that mission critical applications have adequate performance during times of high congestion. Types of filters in this group include Peer-to-Peer, Instant Messaging, and Streaming Media.
Click this tab: | To …
---|---
Filters | View filters you modified on page 166 in the profile or view Traffic Management filters on page 185.
Profile settings | View Attack filter restrictions and exceptions, and Performance Protection restrictions.
Reputation Exceptions | View exceptions for reputation IP addresses, domain names, and URLs.
Shared Settings | View action sets on page 123, notification contacts on page 129, and services on page 131 used by the Inspection profile.

**Filter details**

When you search for and select a filter, you can review the settings and details for the filter. TippingPoint assesses each filter and assigns a category, severity, and recommended action. You can also view the filter name, and the dates the DV filter was distributed or last modified, and the name of the profile the filter is assigned to.

**Dates the filter was released or last modified**

You can view the date that indicates when the filter was released by TippingPoint DV Labs. When a filter gets updated, the SMS displays the date on which the filter was last modified. If available, you can also view the date a filter was publicly disclosed.

*Note:* You must activate a new DV on page 194 before you can search for filters on page 158 by released or last modified dates or view the dates in the Search Results on page 163.

**Severity**

Filters are assigned a severity level to indicate the severity of the potential attack traffic. Severities are color-coded, allowing you to quickly identify and respond appropriately to attack traffic:

- **Red/Critical** — Critical attacks that must be looked at immediately.
- **Yellow/Major** — Major attacks that must be looked at soon.
- **Cyan/Minor** — Minor attacks that should be looked at as time permits.
- **Gray/Low** — Traffic that is probably normal but may have security implications.
Adaptive filtering

Adaptive Filter Configuration, or AFC, is a proprietary technology developed by Trend Micro TippingPoint in order to preserve device performance when it is experiencing heavy congestion. During such congestion, the IPS engine will automatically select filters which are experiencing an excessive number of triggering events without matching the corresponding filters, or the logic of filter required to match network traffic is taking an excessive amount of time to complete. Any filters meeting this criteria will be disabled with a corresponding AFC notification in the system log. The SMS lists any filters for each device which are disabled. These filters are listed in the Events area under Device Configuration.

Most filters provide configuration settings for adaptive filtering. If you do not want a filter to be subject to adaptive filtering, you can edit the filter and disable Adaptive Filtering. You can also modify the device-wide adaptive filter configuration for a device using the Device Configuration wizard. The Adaptive Filter Configuration (AFC) is under the AFC section of the Device Configuration. For more information, see AFC settings on page 360.

Note: If a filter is disabled on a device due to adaptive filtering, the current state of the filter is displayed on the Events screen for the device (Devices > All Devices > [device] > Events).

Filter categories

Filters are a part of Inspection profiles and can be customized for your network security needs. Filters are policies with settings and rules for managing and blocking traffic on a network. Each filter includes an action set on page 123 that contains instructions for managing data and a category setting. As security threats are recognized, the Threat Management Center (TMC) creates and releases filter updates to protect potentially vulnerable systems.

Specific devices may not support certain types of filters.

Table 45. Filter categories

<table>
<thead>
<tr>
<th>Filter</th>
<th>Location on the SMS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Protection Group</td>
<td></td>
</tr>
<tr>
<td>Exploits</td>
<td>Security Filters on page 169</td>
</tr>
</tbody>
</table>

Exploits

Exploits are attacks against a network using weaknesses in software such as operating systems and applications. These attacks usually take the form of intrusion attempts and attempts to destroy or capture data. These filters seek to protect software from malicious attacks across a network by detecting and blocking the request.
<table>
<thead>
<tr>
<th>Filter</th>
<th>Location on the SMS</th>
</tr>
</thead>
<tbody>
<tr>
<td>The two most common methods for exploiting software include email and Web browsing. All Web browsers and many email clients have powerful capabilities that access applications and operating systems. Attackers can create attachments that scan for and exploit this software.</td>
<td>Security Filters on page 169</td>
</tr>
<tr>
<td><strong>Identity Theft</strong></td>
<td></td>
</tr>
<tr>
<td>Identity Theft involves various methods of obtaining key pieces of data related to personal or financial information and using that information to gain goods and services.</td>
<td>Security Filters on page 169</td>
</tr>
<tr>
<td><strong>Reconnaissance</strong></td>
<td></td>
</tr>
<tr>
<td>Reconnaissance filters protect your system against malicious traffic that scans your network for vulnerabilities. These filters constantly monitor incoming traffic, looking for any sign of network reconnaissance. These attacks probe your system, seeking any weakness that can be exploited by attacks. In effect, the attacks attempt to perform reconnaissance of your network to report its strengths and weaknesses for further attacks. By default, Reconnaissance filters are either disabled or set to Block/Notify. Attackers may try to scan a network for available ports or try to infiltrate a host system through its ports and software. These attacks provide entry points for introducing malicious code to further enact attacks through your host and ports. Scan and sweep attacks can consist of multiple probe attacks in large amounts, sending numerous requests for access and information at once. Scans and sweeps filters protect against scan attacks and possible exceeded threshold limits against your ports and hosts.</td>
<td>Security Filters on page 169 Application Filters on page 172</td>
</tr>
<tr>
<td><strong>Scan and sweep filters</strong></td>
<td></td>
</tr>
<tr>
<td>Scan and sweep filters constantly analyze traffic across several sessions and packets against potential scan and sweep attacks against a network. As a result, the Block action setting functions differently for these filters. If the Block action is configured with TCP Reset functions, the TCP Reset does not occur as the network traffic is not tied to a single network flow. In addition, a Block action will cause the source address to be blocked in future network flows.</td>
<td>Security Filters on page 169 Application Filters on page 172</td>
</tr>
</tbody>
</table>
Scan and sweep filters are not affected by restrictions and exceptions in the shared settings for Application Protection filters. When you create exceptions and apply-only settings in the shared settings, they only affect Vulnerability Probing filters.

<table>
<thead>
<tr>
<th>Filter</th>
<th>Location on the SMS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Security Policy</strong></td>
<td>Security Filters on page 169, Application Filters on page 172</td>
</tr>
</tbody>
</table>

Security policy filters act as attack and policy filters. As attack filters, these filters compare packet contents with recognizable header or data content in the attack along with the protocol, service, and the operating system or software the attack affects. These attack filters require deployment knowledge and/or operational policy.

These filters detect traffic that may or may not be malicious that may meet one of the following criteria:

- Different in its format or content from standard business practice.
- Aimed at specific software or operating systems.
- Contrary to your company security policies.

By default, Security Policy filters are disabled. Configuring security policy filters requires knowledge of the installation network configuration. When enabled, these filters may generate false attack alerts depending on your network or application environment. For example, false alerts could be caused by the following:

- Custom or legacy software that uses standard protocols in non-standard ways.
- Attacks on applications or operating systems that you do not have installed.
- Activities that could be benign or malicious depending on where they originate.

⚠️ **Caution:** Scan your network hosts before disabling or creating exceptions to specific attack protection filters. Some operating systems install default services which may be vulnerable to attack. If you disable or add an exception to a filter that protects a service that you do not know about, you may increase your network vulnerability.

**Spyware**
<table>
<thead>
<tr>
<th>Filter</th>
<th>Location on the SMS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spyware is a type of software that transmits information without the user's knowledge or permission. Spyware may be the result of a virus infection or may be installed along with other applications. Spyware often consumes vast resources and can slow systems and, in some cases, cause systems to become unstable or unusable.</td>
<td>Security Filters on page 169</td>
</tr>
<tr>
<td><strong>Virus</strong>&lt;br&gt;A virus is an application or piece of malicious code that can infect other programs. Viruses can embed a copy of itself in programs making them Trojan Horses. When you run these infected programs, the embedded virus also runs and propagates the infection.</td>
<td>Security Filters on page 169</td>
</tr>
<tr>
<td><strong>Vulnerabilities</strong>&lt;br&gt;Attackers generally look for vulnerabilities in a network. Writing malicious code, they try to find the weak points in a network security system to bypass filters and reach data and services. These attackers seek to use intrusion methods against areas such as software back-doors and poorly protected hosts and ports. Vulnerability scanning checks for all potential methods that an attacker could use to infiltrate a network and system.&lt;br&gt;Vulnerabilities filters protect these possible points of entry in a network, detecting and blocking attempted intrusions. These filters protect vulnerable components of a computer system or network by analyzing and blocking traffic seeking these points of entry. The filters constantly scan for possible intrusions points, giving a warning when a vulnerability is found or when malicious attacks occur.</td>
<td>Security Filters on page 169</td>
</tr>
<tr>
<td><strong>Infrastructure Protection Group</strong></td>
<td>Security Filters on page 169</td>
</tr>
<tr>
<td><strong>Network Equipment</strong>&lt;br&gt;Network attacks can broadly or specifically seek access and data to corrupt on a network. Network equipment filters protect networked equipment from attacks that scan and search for hardware. Networked hardware receives requests and from operating systems and services on a network. These filters detect and block the malicious attacks that target equipment accessible through a network, such as printers, modems, routers and integrated phone systems.</td>
<td>Security Filters on page 169</td>
</tr>
</tbody>
</table>
**Traffic Normalization**

Traffic Normalization filters block network traffic when the traffic is considered improper or malformed.

These filters allow you to set alerts to trigger when the system recognizes this traffic. Traffic pattern anomaly filters alert when network traffic varies from normal. Traffic normalization filters enforce valid packet processing within the Threat Suppression Engine. They protect the engine by detecting invalid or abnormal packets. By protecting the engine, the filters scrub the network of possible issues.

As these filters inspect traffic for malformed packets, Recommended Setting for the action set is typically set to Block.

By default, Traffic Normalization filters are set to Block. We do not recommend using a *permit action* on page 123 as it could introduce vulnerabilities with malformed packets.

As these filters manage traffic, you may notice not all filters result in blocked streams. The following filters do not hold blocked data streams:

- 7102: IP fragment invalid. The packet is dropped.
- 7103: IP fragment out of range. The packet is dropped.
- 7104: IP duplicate fragment. The packet is dropped.
- 7105: IP length invalid. The packet is dropped.
- 7121: TCP header length invalid. The packet is dropped.

Traffic Normalization filter names must be unique within a profile. The SMS gives each filter a unique ID, which it uses as a reference in the system.

**Performance Protection Group**

**Instant Messaging**

Instant messaging is a real-time, text-based communication between two or more people using computers that are connected over a network.
Filter

Peer-to-Peer (P2P)
Peer-to-peer protocols are primarily used to share music and video files, and essentially turn a personal computer into a file server, which makes its resources as well as those of its host network available to the peer-to-peer community. Performance Protection filters allow you to shield traffic associated with these kinds of file-sharing protocols.

Note: All peer-to-peer filters are user-activated and must be enabled to block peer-to-peer traffic.

Streaming Media
Streaming media refers to a type of media that is delivered over a computer network. Protocols include:

- **Unicast** — sends a separate copy of the media stream from the client to each client.
- **Multicast** — sends a single copy of the media stream over any given network connection and must be implemented in network routers and servers.

Search
The SMS provides several methods for searching profiles for filters:

- **Global Search** — Performs a search across all listed profiles.
- **Search** — Performs a search within a selected profile.
- **Find** — Performs a keyword search on the displayed page.

Table 46. Search

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global Search</td>
<td>Searches all listed profiles for filters that match search criteria.</td>
<td>Left navigation pane</td>
</tr>
</tbody>
</table>
### Find and view a filter

1. Do one of the following:
   - To find a filter across all listed profiles, select **Profiles > Inspection Profiles > Global Search > Find**.
   - To find a filter within a selected profile, select **Profiles > Inspection Profiles > [Profile Name] > Search > Find**.

2. Enter the name of the filter or keyword, and click **Find**.

   The next entry that matches the criteria is highlighted in the filter list.

### Search profile filters

Search enables you to search by extended criteria, across all filter categories, and includes options for user settings, severity, protocol, platform, modified or added filters, and vulnerability criteria.

1. Do one of the following:
   - For a global search across all listed profiles, select **Profiles > Inspection Profiles > Global Search**.
   - For a standard search within a selected profile, select **Profiles > Inspection Profiles > [Profile Name] > Search**.

2. Click **Filter Criteria** to search for:
Table 47. Filter criteria

<table>
<thead>
<tr>
<th>Select this criteria:</th>
<th>To search for ...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter Specific Info</td>
<td>• <strong>Filter Name</strong> - Filter name or filter number.</td>
</tr>
<tr>
<td></td>
<td>The SMS allows limited special character searching including regular expressions.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Filter Description</strong> - Read-only description provided by the TMC.</td>
</tr>
<tr>
<td>Filter Severity</td>
<td>•  <em>Severity level</em> on page 151</td>
</tr>
<tr>
<td>Filter Type</td>
<td>•  <em>Security filters</em> on page 169</td>
</tr>
<tr>
<td></td>
<td>•  <em>Application filters</em> on page 172</td>
</tr>
<tr>
<td>Suspicious URL Metadata</td>
<td>• <strong>Include</strong> - Filters that include suspicious URL metadata.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Exclude</strong> - Filters that do not include suspicious URL metadata.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The correct DV is required to enable the Suspicious URL Metadata field.</td>
</tr>
<tr>
<td></td>
<td>Activate the DV after you upgrade the SMS. For more information on the correct</td>
</tr>
<tr>
<td></td>
<td>DV version for your product, see the <em>SMS Release Notes</em> on the TMC at</td>
</tr>
<tr>
<td></td>
<td><a href="https://tmc.tippingpoint.com/">https://tmc.tippingpoint.com/</a>*</td>
</tr>
<tr>
<td>User Defined Filters</td>
<td>•  <em>Advanced DDoS filters</em> on page 173</td>
</tr>
<tr>
<td></td>
<td>•  <em>Reputation filters</em> on page 175</td>
</tr>
<tr>
<td></td>
<td>•  <em>Traffic Management filters</em> on page 185</td>
</tr>
<tr>
<td></td>
<td>•  <em>SSL Inspection policies</em> on page 134</td>
</tr>
<tr>
<td></td>
<td>•  <em>SSL servers</em> on page 132</td>
</tr>
<tr>
<td>Control</td>
<td>• <strong>Category</strong> - All filters distributed by the TMC are initially tagged <em>Category</em></td>
</tr>
<tr>
<td></td>
<td>• <strong>Filter</strong> - If a <em>filter has been edited</em> on page 166 to use specific settings,</td>
</tr>
<tr>
<td></td>
<td>select this check box.</td>
</tr>
</tbody>
</table>
### Security Management System User Guide

**Select this criteria:**

<table>
<thead>
<tr>
<th>To search for ...</th>
</tr>
</thead>
</table>

#### State

- **Enabled** - Filters that are *enabled* on page 166.
- **Disabled** - Filters that are disabled.
- **Type Specific** - Depending on device model, the same filter may have different states (for example, a filter may be enabled on a device but disabled on a different device).

#### Filter Category

- **All categories**
- **Specific** *filter categories* on page 152.

3. Click **Source Criteria** to search for:

**Table 48. Source criteria**

<table>
<thead>
<tr>
<th>Select this criteria:</th>
<th>To search for ...</th>
</tr>
</thead>
</table>

#### Filter Released

- **Start dates:**
  - Select **Oldest** to include all filters before the configured End Date in the time range.
  - Select **Date** to enter a date in MM/DD/YYYY format.
  - Select **Date** and click the calendar icon to select a DV or Auxiliary DV package, or a date from the calendar.

- **End dates:**
  - Select **Newest** to include all filters after the Start date in the time range.
  - Select **Date** to enter a date in MM/DD/YYYY format.
  - Select **Date** and click the calendar icon to select a DV or Auxiliary DV package, or a date from the calendar.

**Note:** After upgrading to SMS v4.5.0, you must [activate a new DV](page 194) before you can search for filters by released dates.

#### Filter Last Modified

- **Start dates:**
  - Select **Oldest** to search for the first date the filter was last modified.
Select this criteria:  To search for ...

- Select **Date** to enter a date in MM/DD/YYYY format.
- Select **Date** and click the calendar icon to select a DV or Auxiliary DV package, or a date from the calendar.

End dates:

- Select **Newest** to search for the most recent date the filter was last modified.
- Select **Date** to enter a date in MM/DD/YYYY format.
- Select **Date** and click the calendar icon to select a DV or Auxiliary DV package, or a date from the calendar.

**Note:** After upgrading to SMS v4.5.0, you must *activate a new DV* on page 194 before you can search for filters by last modified dates.

<table>
<thead>
<tr>
<th>Filter Source</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Digital Vaccine (DV) on page 188</td>
<td></td>
</tr>
<tr>
<td>• Auxiliary DV on page 198, and select <strong>Any</strong> or a specific version</td>
<td></td>
</tr>
<tr>
<td>• DV Toolkit on page 201, and select <strong>Any</strong> or a specific version</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Device Support</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Any</td>
<td></td>
</tr>
<tr>
<td>• Supports IPS</td>
<td></td>
</tr>
<tr>
<td>• Supports NGFW</td>
<td></td>
</tr>
<tr>
<td>• Supports Both</td>
<td></td>
</tr>
<tr>
<td>• Does not support IPS</td>
<td></td>
</tr>
<tr>
<td>• Does not support NGFW</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Profile</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>• All profiles</td>
<td></td>
</tr>
<tr>
<td>• Specific profile on page 122</td>
<td></td>
</tr>
</tbody>
</table>

4. Click **Additional Criteria** to search for:
Table 49. Additional criteria

<table>
<thead>
<tr>
<th>Select this criteria:</th>
<th>To search for ...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Actions</td>
<td>• Common action sets including <strong>Permit</strong>, <strong>Rate Limit</strong>, and <strong>Block</strong></td>
</tr>
<tr>
<td>Action Set</td>
<td>• <strong>Any</strong> or select an <em>action set</em> on page 123</td>
</tr>
<tr>
<td>Exceptions</td>
<td>• <strong>Any</strong>, <strong>With Exceptions</strong> and then enter a name and select source IP addresses and destination IP addresses, or <strong>Without Exceptions</strong></td>
</tr>
<tr>
<td>Lock</td>
<td>• <strong>Locked</strong> filters</td>
</tr>
<tr>
<td></td>
<td>• <strong>Unlocked</strong> filters</td>
</tr>
<tr>
<td>Inheritance</td>
<td>• <strong>Use Inherited Settings</strong> filters</td>
</tr>
<tr>
<td></td>
<td>• <strong>Not Using Inherited Settings</strong></td>
</tr>
<tr>
<td></td>
<td>For information on inheritance, see <em>New profiles</em> on page 136.</td>
</tr>
<tr>
<td>Filter Comment</td>
<td>• User-provided comments for the filter</td>
</tr>
</tbody>
</table>

5. Click **Filter Taxonomy Criteria** to search for:

Table 50. Filter taxonomy criteria

<table>
<thead>
<tr>
<th>Select this criteria:</th>
<th>To search for ...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classification</td>
<td>• Application/Protocol Anomaly</td>
</tr>
<tr>
<td></td>
<td>• Distributed Denial of Service (DDoS)</td>
</tr>
<tr>
<td></td>
<td>• IP filters</td>
</tr>
<tr>
<td></td>
<td>• Malicious code</td>
</tr>
<tr>
<td></td>
<td>• Reconnaissance/Suspicious access</td>
</tr>
<tr>
<td></td>
<td>• Security Policy</td>
</tr>
</tbody>
</table>
Select this criteria: | To search for ...
---|---
| • Vulnerability

**Protocol**
• Specific protocols

**Platform**
• Specific platforms

6. Click *Vulnerability Criteria* to search for:

**Table 51. Vulnerability criteria**

<table>
<thead>
<tr>
<th>Select this criteria:</th>
<th>To search for...</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CVE ID</strong></td>
<td>• Unique tracking number used to identify a Common Vulnerabilities and Exposures (CVE)</td>
</tr>
<tr>
<td><strong>Bugtraq ID</strong></td>
<td>• Unique tracking number used to identify a Bugtraq ID</td>
</tr>
<tr>
<td><strong>Vulnerability Scan Database</strong></td>
<td><em>Vulnerability scans</em> on page 227 that have been imported for use on the SMS.</td>
</tr>
<tr>
<td></td>
<td>• CVE in the scan database</td>
</tr>
<tr>
<td></td>
<td>• CVE from all scan files or a specific file</td>
</tr>
<tr>
<td></td>
<td>• Select Any or a vendor</td>
</tr>
<tr>
<td></td>
<td>• <strong>Asset Addr(s)</strong> - One or more IP addresses for an asset. An asset is the network IP address of the host vulnerable to the CVE identified in the vulnerability scan.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Flagged</strong> - All CVEs that are flagged for follow-up.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Not Flagged</strong> - All CVEs that are not flagged.</td>
</tr>
</tbody>
</table>

7. Click **Search**.

**View filter search results**
The Search Results includes the following information.
### Table 52. Filter search results

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>Current filter state; a check mark indicates the filter is enabled and assigned an action set.</td>
</tr>
<tr>
<td>Name</td>
<td>Unique name and number used to identify the filter.</td>
</tr>
<tr>
<td>Control</td>
<td>All filters distributed by the TMC are initially tagged Category. If you edit the filter to use specific settings, Filter displays.</td>
</tr>
<tr>
<td>Action Set</td>
<td><em>Action set</em> on page 123 assigned to the filter. By default, all filters are disabled or assigned a Recommended action set.</td>
</tr>
<tr>
<td>Category</td>
<td>Every filter is assigned to a <em>category</em> on page 152 and cannot be changed.</td>
</tr>
<tr>
<td>Source</td>
<td>Source of the filter and can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <em>Digital Vaccine (DV)</em> on page 188: Downloadable security packages that include filters for protecting your network system. These filters provide new signatures to protect against researched threats to network security.</td>
</tr>
<tr>
<td></td>
<td>• <em>Auxiliary DV</em> on page 198: Specialized filter packages that address specific security needs, such as advanced malware protection or other special-purpose type protection. Updates and distribution of Auxiliary DVs are independent of base DVs.</td>
</tr>
<tr>
<td></td>
<td>• <em>DV Toolkit</em> on page 201: An optional, stand-alone, TippingPoint application that lets you write custom filters for use on TippingPoint devices.</td>
</tr>
<tr>
<td>AFC</td>
<td>Individual filters contain <em>Adaptive Configuration Settings</em> on page 152 that can be enabled or disabled. If AFC is disabled for particular filter, then that filter is never affected by adaptive filtering settings on the device.</td>
</tr>
<tr>
<td>Locked</td>
<td>Indicates if the filter is locked. You cannot edit a locked filter.</td>
</tr>
</tbody>
</table>
### Column Description

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exception</td>
<td>Indicates if the filter contains IP address group <em>exceptions</em> on page 168 for the source or destination.</td>
</tr>
<tr>
<td>Severity</td>
<td><em>Severity</em> on page 151 level assigned to the filter.</td>
</tr>
<tr>
<td>CVE IDs</td>
<td>Unique tracking number used to identify Common Vulnerabilities and Exposures (CVE). CVE IDs are publicly known security vulnerabilities.</td>
</tr>
<tr>
<td>Released</td>
<td>Date the filter was distributed by the TMC.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> You must <em>activate a new DV</em> on page 194 before you view the released date.</td>
</tr>
<tr>
<td>Last Modified</td>
<td>Most recent date the filter was modified by the TMC.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> You must <em>activate a new DV</em> on page 194 before you view the last modified date.</td>
</tr>
<tr>
<td>Filter Disclosed</td>
<td>Date the filter was publicly disclosed, if available.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> You must <em>activate a new DV</em> on page 194 before you view the filter disclosed date.</td>
</tr>
</tbody>
</table>

You can right-click on entries in the filter list and do the following:

- **Find** — Search for a filter using a keyword
- **Edit** — Edit a selected filter
- **Copy Filter Settings** — Copy all settings or selected settings (Action, AFC, or Exception settings)
- **Add Exception** — Create a custom filter exception
- **View Related Events** — Display the related events for the filter in the Events screen
- **Change Lock** — Change lock status
- **ThreatLinQ** — View filter information
Editing filters

You can tune filters to meet the needs of your enterprise. You can modify a filter or add an exception to a filter. You also can alter the system response to an attack filter by editing the action set on page 124, changing how or when contacts are notified, or even disabling the filter.

The following tasks apply to most security and application filters:

- Edit category settings on page 166
- Edit a filter on page 166
- Add a filter exception on page 168
- Remove a filter exception on page 169

Edit category settings

You can enable or disable an entire category of filters. You can also change the action set for an entire group of Security or Application filters on page 152. To edit the category setting for an individual filter, see Edit a filter on page 166.

1. Select Profiles > Inspection Profiles > [Profile Name] > Profile Overview.
2. Click the Category Settings tab, select the entries you want to edit, and click Edit Category Settings.
3. For each category you want to edit, do the following:
   - Select the Locked checkbox to lock the settings.
   - Select the Enabled checkbox to enable the category of filters.
   - Select an Action Set for the filters.
4. Click OK.

Edit a filter

If a filter has inherited settings and the base filter is locked, you cannot edit the filter with inherited settings.

1. Select Profiles > Inspection Profiles, and search for or locate the filter you want to edit.
2. Select a filter from the Search Results, and click Edit.
3. Review the Filter Info for the category, severity, and recommended action. You can also view name of the filter and the name of the profile, and the dates the DV filter was released and last modified.
4. To lock the filter, select the Locked check box.
5. Under Action, do one of the following:
   - Select Use Category Settings to use the recommended action setting for the selected filter.
• Select **Use Filter Specific Settings** to customize the action setting for the selected filter. Select the **Enabled** check box to enable filter specific settings, and select an **Action Set**.

To modify the action set for multiple filters within a category, we recommend **editing the Category Settings** on page 166.

If you modify the action set for filter, go to Profiles > Inspection Profiles > [Profile Name] > Profile Overview > Shared Settings to view this information.

6. Under **General Settings**, do one of the following:

• To apply the global adaptive filter settings for flow control, select **Use Adaptive Configuration Settings**.

• To remove any global adaptive filter settings for this filter, clear **Use Adaptive Configuration Settings**.

• Add comments in the text box as needed.

7. To create a custom filter exception, click **Add** under **Exceptions**. See **Create or edit a filter exception** on page 168.

8. To view the filter description, including a link to ThreatLinQ information on the TMC, select **Filter Details**.

9. To display the associated Common Vulnerabilities and Exposures (CVEs) for the filter, select the **CVE ID**.

   If the filter correlates with a CVE that has been imported as a **vulnerability scan** on page 227, the SMS displays the following vulnerability scan information:

   ◦ Whether the CVE has been flagged for follow-up
   ◦ Date/time the CVE was first mapped to the DV filter
   ◦ Date/time the CVE was last mapped to the DV filter
   ◦ Network assets including the IP addresses and asset groups
   ◦ Comments that have been entered for the CVE

   You can **edit the CVE details** on page 233.

10. To re-distribute the modified filter, click **Distribute**.

11. Click **OK**.

**Edit multiple filters**

When viewing a list of filters, you can select multiple filters to edit.

**Note:** If a filter has inherited settings and the base filter is locked, you cannot edit the filter with inherited settings.
1. Do one of the following:
   • To edit multiple filters across multiple profiles, perform a global search for filters.
   • To edit multiple filters within a selected profile, perform a regular search for filters.

2. Press the Shift or CTRL key while selecting filters, and click Edit.

3. Select Filter Settings, and select or modify options under:
   • Locked - Change locked status for the selected filters.
   • Action - Change Category Setting or use filter specific settings.
   • AFC - Change the filters to use Adaptive Configuration Settings.
   • Comments - Change filter annotations.
   • Exceptions - Add, edit, or remove filter exceptions. See Create or edit a filter exception on page 168.

4. To view the filters that will be changed, select Filters Being Modified.

5. To re-distribute the modified filters, click Distribute.

6. Click OK.

**Create or edit a filter exception**

You can create custom filter exceptions. When you create a filter exception, you exclude the IP address group from being the target of the action set for the selected filters. The filter exception applies only to the selected filter; it does not globally affect all filters.

**Important:** The SMS restricts the number of IP addresses used in filter exceptions, restrictions, and quarantined access for a profile to 65,536. If a profile exceeds this limit, you cannot distribute the profile. This limit promotes better performance for your system. Saving and distributing too many filter changes to a device at one time can cause problems with performance, out-of-memory errors, and fallback mode for High Availability (HA).

1. Select Profiles > Inspection Profiles, and search for or locate the filter you want to edit.

2. Click Add Exception.

3. Enter a Name for the exception.

4. Under Source IP Address, do one of the following:
   • Select Any IP to indicate that traffic flowing from any IP address will not be inspected by this filter.
   • To create an unnamed IP address group, select IP Address and specify an IP address.

After you create the filter exception, go to Admin > Named Resources > IP Address Groups > Show Unnamed Items to view this IP address group.

• To select (or create) a named IP address group, click the Right arrow next to the IP Address field.
From here, you can search for, select, or create a new IP address group. For more information, see
*Named resources* on page 642 and *Create or edit named resource groups* on page 644.
Traffic flowing from the specified source will not be inspected by this filter.

5. Under **Destination IP Address**, do one of the following:
   - Select *Any IP* to indicate that traffic flowing to any IP address will not be inspected by this filter.
   - To create an unnamed IP address group, select *IP Address* and specify an IP address.

   After you create the filter exception, go to **Admin > Named Resources > IP Address Groups > Show Unnamed Items** to view this IP address group.

   - To select (or create) a named IP address group, click the **Right arrow** next to the *IP Address* field.

   From here, you can search for, select, or create a new IP address group. For more information, see
*Named resources* on page 642 and *Create or edit named resource groups* on page 644.
Traffic flowing to the specified destination will not be inspected by this filter.

6. Click **OK**.

**Remove a filter exception**

1. Select **Profiles > Inspection Profiles**, and search for or locate the filter you want to edit.
2. Click **Edit**.
3. Under **Exceptions**, select an exception to delete.
4. Click **Remove**.
5. To remove the exception from the filter, click **Distribute**.
6. Click **OK**.

**Security filters**

Security filters defend against exploits that target applications and operating systems of workstations and servers on a network. Security filters include a variety of attack protection and security policy filters used to detect attacks targeting resources on your network. Malicious attacks may probe your network for vulnerabilities, available ports and hosts, and network accessible applications. Security filters defend your network by providing a device with threat assessment, detection, and management instructions.

These filters block traffic depending on the configured actions for a filter. You can *set these actions to the entire category of filters* on page 166 or *override specific filters* on page 166 to perform a different set of *actions* on page 123.

To view the security filter categories on the SMS, select **Profiles > Inspection Profiles > [Profile Name] > Security Filters**.

Security filters include the following categories:

- *Exploits* on page 152
Security filter exceptions and restrictions

Security filter settings do the following:

- **Restrictions** — Restrict all security filters to function for the listed IP addresses.
- **Exceptions** — Exempt all security filters to not function for the listed IP addresses.

When you add or modify a security filter exception or restriction, the settings apply global changes to the following filter categories:

- **Security Policy** on page 154
- **Network Equipment** on page 155
- **Exploits** on page 152
- **Identity Theft** on page 153
- **Reconnaissance** on page 153
- **Virus** on page 155
- **Spyware** on page 154
- **Vulnerabilities** on page 155
- **Traffic Normalization** on page 156

Create or edit a security filter restriction

1. Select **Profiles** > **Inspection Profiles** > [Profile Name] > **Security Filters**.
2. Click the **Restrictions** tab, and then do one of the following:
• To create a new restriction, click Add.
• To edit an existing restriction, select an exception name, and then click Edit.

3. In the Name field, provide or modify the name for the restriction.

4. In the Source IP Address field, do one of the following:
   • Select Any IP to apply the restriction to all traffic sources.
   • Select IP Address, and provide or select an IP address to apply the restriction to that specific source.

5. In the Destination IP Address field, enter an IP address and do one of the following:
   • Select Any IP to apply the restriction to all traffic destinations.
   • Select IP Address, and specify an IP address to apply the restriction to that specific destination.

6. Select Locked if you want to lock the settings.
   Locking the settings will prevent the filter from being changed and will also lock any profiles that use the profile as a child.

7. Click OK.

Create or edit a security filter exception

1. Select Profiles > Inspection Profiles > [Profile Name] > Security Filters.
2. Select the Exceptions tab and do one of the following:
   • Click Add to create a new restriction.
   • Select an IP address pair name, then click Edit to modify an existing exception.

3. In the Name field, provide or modify the name for the exception.

4. In the Source IP Address field, do one of the following:
   • Select Any IP to apply the exception to all traffic sources.
   • Select IP Address, and specify an IP address to apply the exception to that specific source.

5. In the Destination IP Address field, enter an IP address and do one of the following:
   • Select Any IP to apply the exception to all traffic destinations.
   • Select IP Address, and specify an IP address to apply the exception to that specific destination.

6. Select Locked to lock the settings.

7. Click OK.
Application filters

Application filters allow key applications to have prioritized access to bandwidth. These filters ensure mission critical applications have adequate performance during times of high congestion.

Application filters allow you to manage policy around non-productive or potentially illegal applications. Initially this includes Peer-to-Peer management, where the user may apply block or shape actions across the category or on an individual basis.

These filters block traffic depending on the configured actions for a filter. You can set these actions to the entire category of filters on page 166 or override specific filters on page 166 to perform a different set of actions.

To view the application filter categories on the SMS, select Profiles > Inspection Profiles > [Profile Name] > Application Filters.

Application filters include the following categories:

- **Reconnaissance** on page 153
- **Security Policy** on page 154
- **Instant Messaging** on page 156
- **Peer-to-Peer** on page 157
- **Streaming Media** on page 157

Create or edit application filter restrictions

You can create restrictions for all application filters to function for the listed IP addresses. When you add or modify an application filter restriction, the settings apply global changes to the following filter categories:

- **Instant Messaging** on page 156
- **Streaming Media** on page 157
- **Peer-to-Peer** on page 157

1. Select Profiles > Inspection Profiles > [Profile Name] > Application Filters.
2. Click the Restrictions tab, and then do one of the following:
   - To create a new restriction, click Add.
   - To edit an existing restriction, select an exception name, and then click Edit.
3. In the Restrictions section, click Add.
4. In the Name field, provide or modify the name for the restriction.
5. In the Source IP Address field, do one of the following:
• Select **Any IP** to apply the restriction to all traffic sources.
• Select **IP Address**, and provide or select an IP address to apply the restriction to that specific source.

6. In the Destination IP Address field, enter an IP address and do one of the following:
   • Select **Any IP** to apply the restriction to all traffic destinations.
   • Select **IP Address**, and specify an IP address to apply the restriction to that specific destination.

7. Select **Locked** if you want to lock the settings.

8. Click **OK**.

**Advanced DDoS**

Advanced Distributed Denial of Service (DDoS) filters enable you to create filters for detecting denial of service attacks. When using Advanced DDoS Protection filters, keep in mind the following:

• You must place the device in a Symmetric Network.
• You must disable Asymmetric Mode for the device.
• The device must see both sides of the traffic.

**Create or edit an Advanced DDoS filter**

1. Select **Profiles** > **Inspection Profiles** > [Profile Name] > Advanced DDoS.

2. Do one of the following:
   • Click **New** to create a new Advanced DDoS filter.
   • Select an existing Advanced DDoS filter, and click **Edit**.

3. Select **Filter Parameters** to specify:

**Table 53. Filter parameters**

<table>
<thead>
<tr>
<th>Select this option:</th>
<th>To ...</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Locked</strong></td>
<td>Lock the filter. If a filter has inherited settings and the base filter is locked, the filter with inherited settings cannot be edited.</td>
</tr>
<tr>
<td><strong>Filter Info</strong></td>
<td>Enter a <strong>Name</strong> for the Advanced DDoS filter.</td>
</tr>
<tr>
<td>Select this option:</td>
<td>To ...</td>
</tr>
<tr>
<td>------------------</td>
<td>--------</td>
</tr>
</tbody>
</table>
| **Action**       | Select the action set to perform if an attack against the specified host is detected.  
**Note:** Before you can create a new Advanced DDoS filter, you must have an action set on page 123 that has a block action and does not perform a packet trace. |
| **Network Settings** | Choose the **Direction** to which the filter should be applied, and specify the address of the destination to protect, or click the **Right arrow** to search for, select, or create a named IP address to protect. |
| **Exceptions**   | Create, edit, or remove a list of IP address groups that will be exempt from inspection by this filter.  
Do one of the following:  
• Click **Add** to create a new exception.  
• Select an existing exception, and click **Edit**.  
  a. Enter a **Name**.  
  b. To create an unnamed IP address group, enter the IP address in the **Source IP Address** field.  
  After you create the advanced DDoS filter, go to **Admin > Named Resources > IP Address Groups > Show Unnamed Items** to view this IP address group.  
  c. To create a named IP address group, click the **Right arrow** next to the **Source IP Address** field.  
  From here, you can search for, select, or create a new IP address group. For more information, see **Create or edit named resource groups** on page 644.  
  After you create the advanced DDoS filter, go to **Admin > Named Resources > IP Address Groups** to view this IP address group. |

4. Select **SYN Proxy Settings** to:
Table 54. SYN Proxy settings

<table>
<thead>
<tr>
<th>Select this configuration:</th>
<th>To ...</th>
</tr>
</thead>
<tbody>
<tr>
<td>SYN Proxy</td>
<td>Protect against SYN floods of the system. Typical SYN Flood attacks overwhelm a server with malicious connection requests (TCP SYNs) with spoofed source IP addresses and prevent legitimate clients from accessing the server. The IPS acts as a proxy, synthesizing and sending the SYN/ACK packet back to the originator, waiting for the final ACK packet. After the IPS receives the ACK packet from the originator, the IPS then “replays” the three-step sequence to the receiver. In the event of a distributed attack with random spoofed source addresses, SYN Proxy protection temporarily blocks new connections to the server without interfering with existing connections. This protection can be manually enabled to a DDoS filter settings. Select the <strong>Enabled</strong> check box, and specify the number of SYN requests allowed per second (1 to 10,000) for the <strong>Notification Threshold</strong>.</td>
</tr>
</tbody>
</table>

5. Click **OK**.

**Reputation filters**

A Reputation filter associates an *action set* on page 123 with one or more suspect IP addresses, domains, or URLs in the Reputation Database.

When the profile containing the Reputation filter is distributed to a device, the specified actions are applied to traffic that matches the addresses of tagged entries in the Reputation Database that have been screened using specified tag criteria.

Creating a Reputation filter consists of two steps. In the first step, you define the general settings: the name for the filter, the state, the locked status, the action set, and the type of Reputation Database entries. In the second step, you specify the tag criteria to use when matching entries in the Reputation Database.
When you create a Reputation filter using addresses from the Reputation Database, any tag category associated with the address is included. See Reputation database on page 210.

**Note:** If the tag criteria contains **Does not have this tag**, when you distribute the profile, the SMS sends all entries that do not have this tag category to the device including Reputation DV, geographic, and user-provided entries.

**Note:** After creating Reputation filters, you must distribute the profile to one or more devices in order to fully activate the feature. If you unmanage a device and then after re-managing the device, you must redistribute all the profiles to all the segments for reputation distribution to start working again.

### Edit Reputation settings

Reputation settings apply to all Reputation filters in a profile.

1. Select Profiles > Inspection Profiles > [Profile Name] > Reputation/Geo.
2. Click **Edit Settings**.
3. Select **Locked** to lock the settings for all Reputation filters in the profile.
4. Select a **Filter Matching Address** to specify which address of an incoming packet is used when it matches a Reputation filter.
5. Select a **Lookup Packet Handling** option to specify what the device should do with incoming packets during a Reputation lookup.
6. To apply the filter action to HTTP requests with matching DNS hostnames, select the checkbox under **Reputation Enforcement Options**. This option requires TPS TOS v5.0.0 or later.
7. Click **OK**.

### Create or edit a Reputation filter

1. Select Profiles > Inspection Profiles > [Profile Name] > Reputation/Geo.
2. Do one of the following:
   - Click **New Reputation** to create a new Reputation filter.
   - Select an existing Reputation filter, and click **Edit**.
3. Enter a filter title in the **Name** field, and then select the **Locked** check box if you want to prevent the ability to edit the filter.
4. Select the appropriate block or permit action from the **Action Set** drop-down list, and select the **Enabled** check box to enable the filter. If you clear this check box, the Reputation filter will not be distributed to the device.
5. (Optional) Provide a brief description or comment about the Reputation filter in the **Comments** field.
6. Click **Entry Selection Criteria** and specify the following items:
a. **Entry Criteria** — Select the type of address entries (IPv4, IPv6, DNS Domains, or URLs) from the Reputation Database to include in the filter.

b. **Tag Criteria** — Select the type of tag entries (tagged or untagged) from the Reputation Database to include in the filter and then select the check box next to any tag category you want to include.

   Note: If the tag criteria contains **Does not have this tag**, when you distribute the profile, the SMS sends all entries that do not have this tag category to the device including Reputation DV, geographic, and user-provided entries.

7. Click **OK**.

### Edit a Reputation filter

1. On the Profiles navigation pane, expand **Profiles**, expand **Inspection Profiles**, expand **Default**, and then click **Reputation/Geo**.

   The Reputation Filters and Settings workspace appears.

2. Select a Reputation filter from the table, and then click **Edit**. Alternatively, double-click a filter in the table to open it.

   The Edit Reputation Filter wizard opens.

3. Update any fields as required.

4. Click **OK**.

### Change the precedence of a Reputation or Geographic filter (move up/down)

1. On the Profiles navigation pane, expand **Profiles**, expand **Inspection Profiles**, expand **Default**, and then click **Reputation/Geo**.

   The Reputation Filters and Settings workspace appears.

2. Select a Reputation or Geographic filter from the table, and then click the appropriate button:
   - Click **Move Up** to move the highlighted entry up.
   - Click **Move Down** to move the highlighted entry down.

   **Important:** By default, the Reputation and Geographic filters display in the order in which they were created, and the Reputation engine matches the first filter and applies the selected action.

   **Note:** Creating a Geographic filter for a country—that has a large range of IP addresses and a significant amount of traffic—and selecting the Notify action set can affect the device adversely by the large number of events generated.

   The new order is automatically saved.
Delete a Reputation or Geographic filter

**Important:** Deleting a Reputation or Geographic filter will also remove all data relating to that filter; however, any events that were generated for the filter will still be visible. In circumstances in which you no longer need to deny a country but it is linked to events and reports, it may be better to disable the state of the filter rather than delete it.

1. On the Profiles navigation pane, expand **Profiles**, expand **Inspection Profiles**, expand **Default**, and then click **Reputation/Geo**.
   The Reputation Filters and Settings workspace appears.
2. Select a Reputation or Geographic filter from the table, and then click **Delete**.
   A dialog appears in which you can confirm the deletion.

Create or edit Reputation filter exceptions

1. Select **Profiles > Inspection Profiles > Default > Reputation/Geo**.
2. Click the tab for the reputation filter exceptions (IP, DNS, or URL) that you want to configure.
3. To edit an existing Reputation filter exception, select an exception name, and then click **Edit**.
4. To create a new Reputation filter exception, click **Add**.
5. Configure the exception.

   - For IP exceptions:
     a. (Optional) Select **Locked** if you want to lock the settings.
     b. Type a name for the IP exception in the **Name** field.
     c. In the **Source IP Address** field, do one of the following:
        - Select **Any IP** to apply the restriction to all traffic sources.
        - Select **IP Address**, and provide or select an IP address to apply the restriction to that specific source.
     d. In the **Destination IP Address** field, enter an IP address and do one of the following:
        - Select **Any IP** to apply the restriction to all traffic destinations.
        - Select **IP Address**, and specify an IP address to apply the restriction to that specific destination.

   - For DNS exceptions:
     a. (Optional) Select **Locked** if you want to lock the settings.
     b. Type the name of the domain that you want to exclude from the filter. The domain name must be explicit. Do not use wildcards.
For URL exceptions:

a. (Optional) Select **Locked** if you want to lock the settings.
b. Type the URL that you want to exclude from the filter.

**Note:** A single wildcard string `\*` can be used only at the beginning and end of user-defined URLs entries and exceptions. For example, each of the following wildcard entries successfully matches URL `http://a.com/path/to/resource`:

- **Domain wildcard usage:** `\*/path/to/resource`
- **Path wildcard usage:** `http://a.com/\*`
- **Path wildcard usage:** `http://a.com/path/\*`
- **Path wildcard usage:** `http://a.com/path/to/\*`
- **Both domain and path wildcard usage:** `\*/path/\*`
- **Both domain and path wildcard usage:** `\*/path/to/\*`

6. Click **OK**.

### Create or edit domain name exceptions

1. Go to **Profiles > Inspection Profiles > Default > Reputation/Geo**
2. Click the **Exceptions** tab.
3. To edit an existing domain name exception, select a domain name, and then click **Edit**.
4. To create a new domain name exception, click **Add**.
5. (Optional) Select **Locked** if you want to lock the settings.
6. Type a name for the Reputation domain name in the **Name** field.

**Important:** You must explicitly list each domain name that you want to exclude from the filters. Wildcards, such as an asterisk (`\*`), do not work.

7. Click **OK**.

### Reputation filters table

The Reputation filters table displays the available Reputation and Geographic filters. The filters are in precedence order so as to resolve overlapping criteria.

To access the table, go to **Profiles > Inspection Profiles > [Profile Name] > Reputation/Geo** and select the Reputation Filters and Settings tab.
<table>
<thead>
<tr>
<th>Column</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expand/Collapse</td>
<td>Pertains to a Reputation or Geographic filter. By default, all filters are initially expanded. You can expand or collapse these filters to see more or fewer Criteria information. A plus sign indicates that it can be expanded to show more criteria; a minus sign indicates that it can be collapsed. You can click the column heading to quickly expand or collapse all Reputation or Geographic filters.</td>
</tr>
<tr>
<td>Order</td>
<td>Displays the order number and precedence in which the filter is applied in the Reputation engine. By default, the Reputation and Geographic filters display in the order in which they were created. The Reputation engine matches the first filter, applies the selected action, and does not apply additional filters listed in the Reputation Filters table.</td>
</tr>
<tr>
<td>Name</td>
<td>Displays the name of the Reputation or Geographic filter. You can double-click a filter entry to edit it.</td>
</tr>
<tr>
<td>State</td>
<td>Displays whether a filter is active. A check mark indicates that the filter is activate and can be distributed to a device.</td>
</tr>
<tr>
<td>Locked</td>
<td>Indicates the lock status of a filter. A check mark indicates that the filter is locked and cannot be edited.</td>
</tr>
<tr>
<td>Action</td>
<td>Associated action set that is performed when the filter is triggered. See Action sets on page 123. The SMS displays an icon to indicate the type of action for the selected filter.</td>
</tr>
<tr>
<td>IPv4/IPv6</td>
<td>Indicates the version of the Internet protocol.</td>
</tr>
<tr>
<td>Column</td>
<td>Definition</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>DNS</td>
<td>Indicates whether the filter has a Domain Name System. If the option to apply filter action to HTTP requests with matching DNS hostnames is disabled, DNS requests can only be seen and enforced if the device is between the client and the DNS server.</td>
</tr>
<tr>
<td>URL</td>
<td>Indicates whether the filter matches URLs.</td>
</tr>
<tr>
<td>Untagged/Tagged</td>
<td>Untagged: A checkmark indicates that the Reputation filter will match all entries in the Reputation Database that do not have tags. Tagged: A checkmark indicates that the Reputation filter will match all entries in the Reputation Database that have tags and will filter the entries by the criteria defined for the filter.</td>
</tr>
<tr>
<td>Criteria</td>
<td>Criteria used for the selected filter based on tagged Reputation Database entries. A Geographic filter will display the evaluation (inclusion or exclusion), country icon (if available), and the official name of the selected country, sorted in alphabetical order. If a Geographic filter has an exclusion, Any displays to indicate that every other country in the database is included.</td>
</tr>
</tbody>
</table>

Management tasks

This area supports the following profile management tasks:

- **Search** — Search for a specific profile.
- **Distribute** — Distribute the selected Reputation and/or Geographic filters to one or more devices in your network.
- **Move Up** — Move the selected filter up one row in the Reputation Filters table.
- **Move Down** — Move the selected filter down one row in the Reputation Filters table.
- **New Reputation** — Create a new Reputation filter.
- **New Geographic** — Create a new Geographic filter.
- **Edit** — Edit a selected Reputation or Geographic filter.
• **Delete** — Remove the selected Reputation or Geographic filter. A dialog appears in which you can confirm the deletion. In circumstances in which you no longer need to deny a country but it is linked to events and reports, it may be better to disable the state of the filter rather than delete it.

**Reputation settings**

Reputation settings apply to all reputation filters in a profile.

- The Filter Matching Address setting specifies which address of an incoming packet is used when testing for a filter match.
- The Lookup Packet Handling setting specifies what the device should do with packets that arrive during a reputation lookup.

**Geographic filters**

These filters detect and manage traffic based on a computer’s IP address/hostname within a geographic region or country. These filters enable you to perform actions based on the countries that you allow or deny in a filter. IP address can be tied to real-world geographic regions or countries, and identifying a client’s geographic location may provide clues about the user’s intentions. The SMS supports real-time geolocation analysis through the integration of the free MaxMind GeoLite City binary database.

**Note:** If you have a paid MaxMind subscription, you can import the database file. See Geo Locator database on page 652.

A Geographic filter is similar to a Reputation filter in that it associates an action set, and when the profile containing the Geographic filter is distributed to a device, the specified actions are applied to traffic that matches the included and excluded countries.

Creating a Geographic filter consists of two steps. In the first step, you define the general settings: the name for the filter, the state, the locked status, and the action set that specifies whether to allow or deny traffic based on the geographic region. In the second step, you search for, select, and evaluate the country criteria as an **inclusion** or **exclusion**. Once you distribute the filter, you will can view events and generate reports based on this filter.

**Note:** After creating Geographic filters, you must distribute the profile to one or more devices in order to fully activate the feature. If you unmanage a device and then after re-managing the device, you must redistribute all the profiles to all the segments for geographic distribution to start working again.

**Important:** A country can only be assigned to one Geographic filter at a time. For example, if you create a filter and allow Japan, you cannot search for and select Japan in a different Geographic filter until you remove it from the first filter.

**Any country**

Every time you create a new Geographic filter, the SMS automatically includes *Any* country, which allows you to quickly include all countries in the database without having to search for and select one or more
Inclusions and exclusions

You can include one or more countries in a Geographic filter. In this way, you can track visits from a region that is spread across multiple countries. For example, the sales region known as APLA (Asia Pacific and Latin America) includes the following countries: Argentina, Australia, Brazil, China, Hong Kong, India, Indonesia, Japan, Mexico, New Zealand, Korea, and Taiwan. To track this region, you can create a filter, include all of the countries, and then select an action set. The SMS displays a green check mark icon for each country that is included in a Geographic filter.

In addition, if you want to exclude one or more countries in a Geographic filter, you can search for, select, and exclude a country. The SMS displays a red strikethrough icon for each country that is excluded in a Geographic filter.

You can also edit an existing Geographic filter to exclude a previously included country and vice versa.

Important: An inclusion or an exclusion does not necessarily indicate that traffic for the selected country is allowed or denied. The action set for the filter determines the action assigned to the country.

Create or edit a Geographic filter

1. Select Profiles > Inspection Profiles > [Profile Name] > Reputation/Geo.
2. Do one of the following:
   - Click New Geographic to create a new geographic filter.
   - Select an existing geographic filter, and click Edit.
3. Enter a filter title in the Name field, and then select the Locked check box if you want to prevent the ability to edit the filter.
4. Select the appropriate block or permit action from the Action Set drop-down list, and select the Enabled check box to enable the filter. If you clear this check box, the Geographic filter will not be distributed to the device.
5. (Optional) Provide a brief description or comment about the Geographic filter in the Comments field.
6. Click the + icon (located to the right of the Country list). Alternatively, right-click in the Country list, and then select Add Country.
   The Choose Countries dialog opens, and lists all available countries, sorted in alphabetical order. The SMS also displays the country flag icon, if available
7. Enter the official name of the country in the Search field. As you type, the SMS automatically narrows the list of countries. Alternatively, use the scroll bar to browse through the list of all available countries.

Note: You cannot enter an abbreviation or alternative name for a country. For example, you cannot enter “US” or “America” for “United States.”
8. Select one or more countries. Hold the **SHIFT** key to select multiple sequential countries in the list; hold the **CTRL** key to select two or more non-sequential countries in the list.

9. Select an evaluation:
   - Select **Inclusions** to include (allow) the selected countries in the filter.
   - Select **Exclusions** to exclude (deny) the selected countries in the filter.

   **Note:** You cannot include some countries and exclude others in the same filter. When you exclude or deny a country, the SMS automatically includes every other country available in the database, as shown by a green check mark and *Any*.

10. Click **OK**.

   **Important:** An *inclusion* or an *exclusion* does not necessarily indicate that traffic for the selected country is allowed or denied. The action set for the filter determines the action assigned to the country.

   **Note:** Creating a Geographic filter for a country—that has a large range of IP addresses and a significant amount of traffic—and selecting the Notify action set can affect the device adversely by the large number of events generated.

   The selected countries display in the Country list. Included counties display a green checkmark icon; excluded counties display a red strikethrough icon.

11. Click **OK**.

   The Geographic filter is added to the Reputation Filters table.

### Edit a Geographic filter

1. On the Profiles navigation pane, expand **Profiles**, expand **Inspection Profiles**, expand **Default**, and then click **Reputation/Geo**.

   The Reputation Filters and Settings workspace appears.

2. Select a Geographic filter from the table, and then click **Edit**. Alternatively, double-click a filter in the table to open it.

   The Edit Geographic Filter dialog opens.

3. Update any fields as required.

4. (Optional) To add a country, click the + icon (located to the right of the Country list). Alternatively, right-click in the County list, and then select **Add Country**.

   **Important:** A country can only be assigned to one Geographic filter at a time. For example, if you create a filter and allow Japan, you cannot search for and select Japan in a different Geographic filter until you remove it from the first filter. If you search for Japan, it will not display in the Choose Countries list.
5. (Optional) To remove a country, select a country, and then click the **-** icon (located to the right of the Country list). Alternatively, right-click the country, and then select **Remove Selected Countries**.

6. (Optional) To include a country, right-click a country, and then select **Include Countries**.

7. (Optional) To exclude a country, right-click a country, and then select **Exclude Countries**.

   **Note:** You cannot include some countries and exclude others in the same filter. When you exclude or deny a country, the SMS automatically includes every other country available in the database, as shown by a green check mark and *Any*.

8. Click **OK**.

**Traffic Management filters**

Traffic Management filters react to traffic based on a limited set of parameters including the source IP address, destination IP address, port, protocol, or other defined values. For example, you might define the following Traffic Management filters for your web servers in a lab that denies access to external users:

- Block traffic if the source is on an external subnet that arrives through port 80 and is destined for the IP address of your web server.
- Block traffic if the source is your web server, the source port is 80, and the destination is any external subnet.

These filters detect issues in bandwidth usage. Because the SMS does not include these filters, you must create them.

**Note:** Traffic Management filters differ from other traffic-shaping filters, such as *Traffic Normalization filters* on page 156, which are Infrastructure Protection filters that enforce valid packet processing within the Threat Suppression Engine. They protect the engine by detecting invalid or abnormal packets. By protecting the engine, the filters scrub the network of possible issues.

**Maximum filter limits**

The SMS enforces the maximum number of Traffic Management filters that can be distributed to a device based on device capacity. The SMS groups devices into three categories (low-end, medium-end, and high-end) with an assigned maximum to each category for enforcement purposes.

SMS takes into consideration the expanded Traffic Management filters as well as what the device has into account. If the number of Traffic Management filters for a device exceeds the limit, the SMS displays a message.

Traffic Management filter limits include:

- **Low-end device limit:** 5,000 filters
  - Low-end devices include *S-Series devices* on page 406.
- **Medium-end device limit:** 8,000 filters

- High-end device limit: 12,000 filters

  High-end devices include *2200T* on page 401 and *TX-Series devices* on page 401.

**Create or edit a Traffic Management filter**

1. Select *Profiles > Inspection Profiles > [Profile Name] > Traffic Management*.
2. Do one of the following:
   - Click *New* to create a new Traffic Management filter.
   - Select an existing Traffic Management filter, and click *Edit*.
3. Enter a *Name* for the filter. Traffic Management filter names must be unique within a profile. The SMS gives each filter a unique ID, which it uses as a reference in the system.
4. Select *Locked* to lock the filter.
5. Select an *Action* to specify the actions taken with a packet after it triggers a rule. As Traffic Management filters inspect traffic for malformed packets, the recommended setting for the action set is typically set to Block. We do not recommend using a Permit action, as this action could introduce vulnerabilities with malformed packets.

**Table 56. Traffic Management filter actions**

<table>
<thead>
<tr>
<th>Select this option:</th>
<th>To ...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>Turn on filter-specific settings. Clear the check box to turn off the action.</td>
</tr>
<tr>
<td>Block</td>
<td>Discard a packet.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The SMS blocks, but does not log, traffic that matches this filter. Use caution when selecting this action as it might cause a network outage, if not correctly defined.</td>
</tr>
<tr>
<td>Allow</td>
<td>Allow a packet to reach its intended destination.</td>
</tr>
<tr>
<td>Trust</td>
<td>Allow a packet to flow though (traffic is not inspected by the profile).</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Selecting this action might introduce vulnerabilities in your network.</td>
</tr>
</tbody>
</table>
Select this option: | To ...
---|---
**Rate Limit** | Limit traffic to a defined speed. The SMS does not log any Traffic Management filter rules when a packet hits a filter.

6. (Optional) In the General Settings area, enter comments.

7. Configure the network settings:

**Table 57. Traffic Management filter network settings**

| Select this option: | To ...
---|---
**Direction** | Specify the direction from the following.
- Port A to Port B
- Port B to Port A
- Create filters for both directions

**Protocol** | Specify the protocol and the protocol dependent parameters from the following.
- IP/IPv6. (Optional) select **Apply Only to IP Fragments** and then enter an IP address for the fragment.
- TCP/TCPv6, and then specify source and destination ports.
- UDP/UDPv6, and then specify source and destination ports.
- ICMP/ICMPv6, and then specify ICMP settings (type and code).

**Source Address** | • Any
• Any IPv6
• Value

**Named Resources**
If you select **Value**, you can select or create an unnamed or named IP address group.
- Enter the IP address in the **Source Address** field to create an unnamed IP address group.
Select this option: | To ...
---|---
• Click the **Right arrow** next to the **Source Address** field to select or create a named IP address group. For more information, see *Create or edit named resource groups* on page 644.

**Destination Address**
• Any
• Any IPv6
• Value

**Named Resources**
If you select **Value**, you can select or create an unnamed or named IP address group.
• Enter the IP address in the **Dest Address** field to create an unnamed IP address group.
• Click the **Right arrow** next to the **Dest Address** field to select or create a named IP address group. For more information, see *Create or edit named resource groups* on page 644.

The SMS uses cross multiplication when distributing Traffic Management filters to pair the source and destination addresses. For example, a single Traffic Management filter that has 10 addresses in its source group and 10 addresses in its destination group will produce 100 Traffic Management Filters upon distribution.

**Note:** Sending too many Traffic Management filters to the device can exceed the device maximum. For more information, see *Maximum filter limits* on page 185. To prevent this, ensure that the source or destination addresses has a value of **Any/Any IPv6**. For example, if you select the **IPv6** protocol, select **Any IPv6** for the source or destination addresses.

8. To re-distribute the modified filter, click **Distribute**.

9. Click **OK**.

**Digital Vaccines**
Digital Vaccines (DV) are downloadable security packages that include filters for protecting your network system. These filters provide new signatures to protect against researched threats to network security. The
Threat Management Center (TMC) researches, creates, and distributes these filter packages. You can visit the Threat Management Center website at: https://tmc.tippingpoint.com/TMC/.

Go to Profiles > Digital Vaccines to download filter packages and distribute them to your devices. You can configure the SMS to automatically check for, download, and distribute filter updates to your managed devices. You can also set up the SMS to send you email notification of automatic Digital Vaccine downloads and distribution. To receive these messages by e-mail, add your contact information to the Network Information.

**Note:** If you do not want to activate a Digital Vaccine when downloading it, clear that option when prompted to download a new DV.

### DV Inventory tab

The DV Inventory tab has the following features:

- **Active DV** — Provides version information about the active Digital Vaccine package.
- **Auto DV Activation:**
  - Automatic Download — Downloads new Digital Vaccine packages as they become available on TMC.
  - Automatic Activate — Automatically activates the downloaded package in the SMS.
  - Automatic Distribute — Distributes the downloaded package to all available devices.
  - DV Notification Pop-ups — Displays a notification popup when a DV is available. The DV Notification Pop-ups option is only available when auto download is disabled. Additionally, this option only affects the current user.

**Note:** An auto-downloaded Digital Vaccine will not activate if its major version is different than the major version of the currently active Digital Vaccine.

- **DV Inventory** — Lists the Digital Vaccine packages that have been downloaded and are available for distribution
- **Distribution Progress** — Provides information on distribution status of a Digital Vaccine package for a device

#### Table 58. DV Inventory

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Column</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Active</td>
<td>Active status of the Digital Vaccine package. You can download many packages that can be activated based on your system needs.</td>
</tr>
<tr>
<td>vTPS DV</td>
<td>A check mark indicates that the Digital Vaccine package is only available for virtual TPS (vTPS) devices.</td>
</tr>
<tr>
<td>Released</td>
<td>Date and time the Digital Vaccine package was released.</td>
</tr>
<tr>
<td>Downloaded</td>
<td>Date and time the Digital Vaccine package was downloaded from the TMC.</td>
</tr>
<tr>
<td>Size</td>
<td>File size of the Digital Vaccine package.</td>
</tr>
<tr>
<td>Devices</td>
<td>Number of devices that have received the distributed Digital Vaccine package. If the number is zero (0), the package has not been distributed.</td>
</tr>
</tbody>
</table>

**Digital Vaccine version information**

TippingPoint releases an updated Digital Vaccine every week. The Digital Vaccine is packaged separately for different TOS versions, as shown in the following table.

**Table 59. Digital Vaccine version information**

<table>
<thead>
<tr>
<th>A Digital Vaccine that begins with</th>
<th>Applies to</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.5</td>
<td>Devices running TOS v2.5.2 to TOS v3.1x.</td>
</tr>
<tr>
<td>3.2</td>
<td>Devices running TOS v3.2.0 or later, such as IPS and TPS devices.</td>
</tr>
<tr>
<td>4.0</td>
<td>vTPS devices only.</td>
</tr>
</tbody>
</table>

We recommend that you download the same Digital Vaccine for all of your managed devices. For example, if the weekly Digital Vaccine is #DV8771, and you manage a vTPS and a 440T TPS, after you download the DVs, the DV Inventory should include the following versions:

- 3.2.0.8771 for the 440T device
• 4.0.0.8771 for the vTPS

If the Digital Vaccine version does not match, click **Download from TMC** and review the list of available Digital Vaccines.

**Download and manage Digital Vaccine packages**

1. Download or import the latest filters from the TMC in the form of Digital Vaccine packages. The **Profiles > Digital Vaccines** screen displays the list of packages installed and activated on your system. To obtain the latest package from the TMC, click **Download**. If you have the package saved locally, click **Import**.

2. Edit and customize the filters. You may need to enable certain filters according to the filter pillar type.

3. Distribute the profile to the device(s) or associated segment group.

   As you make changes and additions, the SMS adds the changes to the profile. The profile includes all filter changes and recent additions of the Digital Vaccine package.

   Right-clicking an entry in the DV Inventory tab displays the following options in a drop-down menu:
   
   • **Import** — Import a Digital Vaccine package from a file.
   • **Download from TMC** — Download the latest Digital Vaccine package from the TMC.
   • **Distribute** — Distribute the Digital Vaccine package to the devices.
   • **Activate** — Make the selected package the currently used package.
   • **Details** — View the details of the package.
   • **Delete** — Remove the package file from the system.

Through the **Profiles > Digital Vaccines** screen and navigation pane, you can manage Digital Vaccine packages. When you update the filters of a system, you can download or import the packages. To import a package, you must have a Digital Vaccine package file. You can receive this file through the Threat Management Center website at: [https://tmc.tippingpoint.com/TMC/](https://tmc.tippingpoint.com/TMC/).

The package file can download directly from the Threat Management Center on the SMS. See **Auto-download and distribute a DV, virtual DV, or Auxiliary DV** on page 192.

**Note:** When you cannot access the TMC using a secure communication system, you can download the package file to your computer and import it using the SMS client. HTTP and telnet are examples of unsecure communication services. HTTPS and SSH are examples of secure communication services.

**Scheduled Distributions tab**

From the Scheduled Distributions tab, you can:

• **Distribute a DV, virtual DV, or Auxiliary DV package** on page 197

• **Stop distribution of a DV, virtual DV, or Auxiliary DV** on page 197
• Create a new scheduled distribution on page 197
• Edit a scheduled distribution on page 198

Importing DV packages

When you import a Digital Vaccine package, the SMS accesses for available updates. If a new package is available, the SMS may prompt you to download and install the update. Packages are downloaded and added to the DV list for activation as you need.

You can also configure the automatic update feature to have the SMS check and download updates periodically. When a Digital Vaccine is automatically downloaded, it is also activated. However, the DV has no impact on current profiles until the DV is distributed.

You can perform the following tasks:
• Auto-download and distribute a DV, virtual DV, or Auxiliary DV on page 192
• Import a DV, virtual DV, or Auxiliary DV package on page 193
• Download a DV, virtual DV, or Auxiliary DV package on page 193

Auto-download and distribute a DV, virtual DV, or Auxiliary DV

1. On the Profiles navigation pane, do one of the following:
   • Click Digital Vaccines to open the DV Inventory screen.
   • Click Auxiliary DV to open the Auto Auxiliary DV Activation screen.

2. On the Auto DV Activation or Auto Auxiliary DV section, click Edit.

3. On the Edit Auto DV Settings dialog, select from the following options:
   • Automatic Download — If enabled, the SMS downloads new Digital Vaccine packages as they become available on TMC.
   • Automatic Activation — If enabled, the SMS automatically activates the downloaded package in the SMS. An auto-downloaded Digital Vaccine does not activate if its major version is different than the major version of the currently active Digital Vaccine.
   • Automatic Distribution — If enabled, the SMS distributes the downloaded package to all available devices.
   • DV Notification Popups — If enabled, the SMS displays a notification popup when a DV is available. This option is only available when auto download is disabled and only affects the current user.

4. Click OK.
Import a DV, virtual DV, or Auxiliary DV package

1. In a web browser, open https://tmc.tippingpoint.com/TMC/.
   
   If you have not already done so, create a TMC account using your Customer ID and Serial Number.

2. From the top menu, select Releases > Digital Vaccines > Digital Vaccines.
   
   The page lists all available complete packages that are available. The most recent version is at the top of the list.

3. Click the More Info button next to the most recent package.

   
   The File Download dialog opens.

5. Click Save.

   Note: To avoid unexpected behavior on the SMS, do not change the name of this file.

6. On the Profiles navigation pane, do one of the following:
   - Click Digital Vaccines to open the DV Inventory screen.
   - Click Auxiliary DV to display the Auto Auxiliary DV Activation screen.

7. On the DV Inventory section or the Auxiliary DV Inventory, click Import.

8. Select the DV package, and then click OK.
   
   The file imports and displays in the DV Inventory section.

Download a DV, virtual DV, or Auxiliary DV package

1. On the Profiles navigation pane, do one of the following:
   - Click Digital Vaccines to display the DV Inventory screen.
   - Click Auxiliary DV to display the Auto Auxiliary DV Activation screen.

2. On the DV Inventory or the Auxiliary DV Inventory section, click Download from TMC or Download.

3. Select a version to download.

4. Select the options to activate and/or distribute the package after downloading.

5. Click Download.

   The package downloads to the system and displays in the DV Inventory. You can now make this package active if desired, as well as view details, distribute, and remove the package.
Managing DV packages

After importing these packages, you can activate, delete, and view the information for the packages.

Activate a DV, virtual DV, or Auxiliary DV package

**Note:** You must activate a new DV before you can search for filters in a DV package on page 195 or view the released, last modified, or filter disclosed dates in the Search Results on page 163 or filter details on page 151.

1. Select **Profiles**, and do one of the following:
   - Click **Digital Vaccines** to display the DV Inventory screen.
   - Click **Auxiliary DV** to display the Auto Auxiliary DV Activation screen.
2. On the DV Inventory or the Auxiliary DV Inventory section, select a package, and then click **Activate**.
   The package displays as active in the DV Inventory section.

View details of a DV, virtual DV, or Auxiliary DV package

1. On the Profiles navigation pane, do one of the following:
   - Click **Digital Vaccines** to display the DV Inventory screen.
   - Click **Auxiliary DV** to display the Auto Auxiliary DV Activation screen.
   The Details screen provides information on the file size, release date, and download date. A table lists the DV inventory according to distributions to devices.
2. On the DV Inventory or the Auxiliary DV Inventory section, select a package, and then click **Details**.
   The Release Notes tab provides the documentation for the DV package. The Deployments tab provides information about the deployment mode. You can perform a distribution and activation for the DV package from this screen.

Delete a DV, virtual DV, or Auxiliary DV package

1. On the Profiles navigation pane, do one of the following:
   - Click **Digital Vaccines** to display the DV Inventory screen.
   - Click **Auxiliary DV** to display the Auto Auxiliary DV Activation screen.
2. In the DV Inventory or the Auxiliary DV Inventory section, select the package(s) you want to delete.
   **Note:** You cannot delete active packages. If you attempt to delete an active package, an error message displays.
3. Click **Delete**.
Search filters in a DV package

To view and search filters in a DV package, use the global search feature or search a selected profile in which
the filter package is applied. For additional information, see Search on page 157 and Search profile filters
on page 158.

1. Do one of the following:
   • For a global search across all listed profiles, select Profiles > Inspection Profiles > Global Search.
   • For a standard search within a selected profile, select Profiles > Inspection Profiles > [Profile
     Name] > Search.

2. Click Source Criteria to search for:

Table 60. Source criteria

<table>
<thead>
<tr>
<th>Select this criteria:</th>
<th>To search for ...</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Filter Released</strong></td>
<td>Start dates:</td>
</tr>
<tr>
<td></td>
<td>• Select <strong>Oldest</strong> to include all filters before the configured End Date in the time range.</td>
</tr>
<tr>
<td></td>
<td>• Select <strong>Date</strong> to enter a date in MM/DD/YYYY format.</td>
</tr>
<tr>
<td></td>
<td>• Select <strong>Date</strong> and click the calendar icon to select a DV or Auxiliary DV package, or a date from the calendar.</td>
</tr>
<tr>
<td></td>
<td>End dates:</td>
</tr>
<tr>
<td></td>
<td>• Select <strong>Newest</strong> to include all filters after the Start date in the time range.</td>
</tr>
<tr>
<td></td>
<td>• Select <strong>Date</strong> to enter a date in MM/DD/YYYY format.</td>
</tr>
<tr>
<td></td>
<td>• Select <strong>Date</strong> and click the calendar icon to select a DV or Auxiliary DV package, or a date from the calendar.</td>
</tr>
<tr>
<td><strong>Note:</strong> After you upgrade to this SMS version, you must <strong>activate a new DV</strong> on page 194 before you can search for filters by released dates.</td>
<td></td>
</tr>
<tr>
<td><strong>Filter Last Modified</strong></td>
<td>Start dates:</td>
</tr>
<tr>
<td></td>
<td>• Select <strong>Oldest</strong> to search for the first date the filter was last modified.</td>
</tr>
<tr>
<td></td>
<td>• Select <strong>Date</strong> to enter a date in MM/DD/YYYY format.</td>
</tr>
</tbody>
</table>
Select this criteria: | To search for ... |
---|---|
| | • Select **Date** and click the calendar icon to select a DV or Auxiliary DV package, or a date from the calendar. |
| **End dates:** | • Select **Newest** to search for the most recent date the filter was last modified. |
| | • Select **Date** to enter a date in MM/DD/YYYY format. |
| | • Select **Date** and click the calendar icon to select a DV or Auxiliary DV package, or a date from the calendar. |

**Note:** After you upgrade to this SMS version, you must *activate a new DV* on page 194 before you can search for filters by last modified dates.

**Filter Source**
- **Digital Vaccine (DV)** on page 188
- **Auxiliary DV** on page 198, and select **Any** or a specific version
- **DV Toolkit** on page 201, and select **Any** or a specific version

3. Click **Search**.

### Distributing DV packages overview

When you distribute a Digital Vaccine package, you update the filter settings for a device. A package may include modifications including new filters, modified filters, and removed filters.

You can set up the system to automatically distribute the package on the **Profiles > Digital Vaccines** screen. The screen enables you to manage all distributions through the Distribution Progress section of the screen. You can enact and cancel a distribution from the screen.

### Scheduled distributions

When you schedule a distribution you have the following options:

- **One-time distribution** — Runs once at the schedule time using the DV package selected.
- **Recurring distribution** — Runs at the times and days specified and distributes the latest DV package available on the SMS to the selected devices if you have an older version of the DV.

Devices that have a TOS prior to 2.5 will only receive a new DV package if there is a newer 2.2 DV available on the SMS. Similarly, devices with TOS of 2.5 and above will only receive a new DV package if there is a newer 2.5 DV available on the SMS. The recurring scheduled distribution updates devices that have older
DV versions, regardless of whether a recent TMC download occurred. The criteria is only that the device is in the list of devices to distribute and that it has an older DV.

For information about how you can schedule distributions to a stack of devices, see Security policy configuration on page 526.

**Distribute a DV, virtual DV, or Auxiliary DV package**

1. On the Profiles navigation pane, do one of the following:
   - Click Digital Vaccines to display the DV Inventory screen.
   - Click Auxiliary DV to display the Auto Auxiliary DV Activation screen.
2. On the DV Inventory or the Auxiliary DV Inventory section, select a package.
3. Click Distribute.
4. On the distribution dialog, select the device or devices you want to receive the distribution.

   The package distributes. As it runs, an entry displays with updating status in the Distribution Progress section.

   For information about how you can distribute package updates to a stack of devices, see Security policy configuration on page 526.

**Stop distribution of a DV, virtual DV, or Auxiliary DV**

1. On the Profiles navigation pane, do one of the following:
   - Click Digital Vaccines to display the DV Inventory screen.
   - Click Auxiliary DV to display the Auto Auxiliary DV Activation screen.
2. On the Distribution Progress section, select a distribution in progress.

**Create a new scheduled distribution**

1. On the Profiles navigation pane, click Scheduled Distributions.
2. On the DV Distribution Schedule area, click New.
3. Complete the information for each screen and click Next to continue.
   - To return to a previous screen, click Previous. After entering information on the final screen, click Finish to save your entries.
4. On the General Settings > Schedule section, select a one time or recurring schedule.
   - If you select a recurring schedule, complete the scheduled distribution time.
5. On the General Settings > Schedule section, select which package to distribute or the <Latest Available>. 
6. Click **Next**, and then choose which device or devices will receive the distribution package.

7. If you want the distribution to be a high priority, select the **High Priority** check box next to the appropriate devices.

8. Click **Finish**.

**Edit a scheduled distribution**

1. On the Profiles navigation pane, click **Scheduled Distributions**.

2. Select an existing scheduled distribution from the List pane, and click **Edit**.

3. Make desired changes, and click **OK**.

**Auxiliary DVs**

Auxiliary DVs are specialized filter packages that addresses specific security needs. Auxiliary DVs augment the protection provided by the base DV. Update and distribution of an Auxiliary DV package is independent of your base DV.

Auxiliary DV packages are activated when distributed to the device and deactivated when they are uninstalled from the device.

The SMS can support and manage one or more Auxiliary Digital Vaccine types for IPS devices that support this feature.

**Note:** The SMS does not manage multiple base DVs on the device. When a new base DV is installed, the old base DV is deleted.

For more information on obtaining TippingPoint Auxiliary DVs, contact your TippingPoint representative.

**ThreatDV**

Threat Digital Vaccine (ThreatDV) is a type of Auxiliary DV that includes advanced malware protection. Like the regular Digital Vaccines, ThreatDV is delivered to the TMC on a periodic schedule and can be automatically or manually downloaded to the SMS for distribution to your security devices that support this Auxiliary DV type.

**Note:** TOS 3.7 or later versions are required on an IPS device for ThreatDV support.

The SMS displays the ThreatDV packages in the Auxiliary DV screen of the Profiles section. You can monitor and manage the installation and activation of the ThreatDV package versions and monitor distribution progress in the same way that you manage other filter packages.

Anti-malware ThreatDV filters fall into the same categories used for regular Digital Vaccine malware filters, and display accordingly when the filters are viewed for an inspection profile.

For more information about obtaining TippingPoint Auxiliary DVs, contact your TippingPoint representative.
## Auxiliary DV screen

The Auxiliary DVs screen includes the following information:

- **Auto Auxiliary DV Activation** — Provides the option to edit the SMS settings for auto download, activate, distribution, and notification pop-ups of Digital Vaccine packages. See *Auto-download and distribute a DV, virtual DV, or Auxiliary DV* on page 192.

- **Auxiliary DV Inventory** — Lists the packages that have been downloaded and are available for distribution.

- **Distribution Progress** — Provides information on distribution status of an Auxiliary DV package for a device.

### Table 61. Auxiliary DV inventory

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category</td>
<td>User-created label</td>
</tr>
<tr>
<td>Version</td>
<td>The version of the Auxiliary DV</td>
</tr>
<tr>
<td>Active Status</td>
<td>The active status of the Auxiliary DV. You can import multiple Auxiliary DVs that can be activated based on your system needs.</td>
</tr>
<tr>
<td>Released</td>
<td>Date and time the Auxiliary DV was released by TippingPoint</td>
</tr>
<tr>
<td>Downloaded</td>
<td>Date and time the Auxiliary DV was downloaded from the TMC</td>
</tr>
<tr>
<td>Size</td>
<td>File size of the Auxiliary DV</td>
</tr>
<tr>
<td>Description</td>
<td>Brief description of the Auxiliary DV</td>
</tr>
<tr>
<td>Devices</td>
<td>Number of devices that have received the distributed Auxiliary DV. If the number is zero (0), the ADV has not been distributed.</td>
</tr>
</tbody>
</table>
Table 62. Auxiliary DV distribution progress

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device</td>
<td>Number of devices receiving the distributed Auxiliary DV. Expand to see the name of each target device.</td>
</tr>
<tr>
<td>Package</td>
<td>Version of the Auxiliary Digital Vaccine package being distributed</td>
</tr>
<tr>
<td>Start Time</td>
<td>Date and time the distribution began</td>
</tr>
<tr>
<td>End Time</td>
<td>Date and time the distribution ended</td>
</tr>
<tr>
<td>Status</td>
<td>Status of the distribution</td>
</tr>
<tr>
<td>Progress</td>
<td>Progress of the distribution expressed in a percentage value</td>
</tr>
</tbody>
</table>

**Auxiliary Digital Vaccine tasks**

Through the **Profiles (Auxiliary DVs)** screen and navigation pane, you can manage Auxiliary DV packages. When you update the filters of a system, you can download or import the packages. An Auxiliary DV can be downloaded and activated automatically or manually. After you activate an Auxiliary DV package, you must distribute it in a profile to a device.

**Import Auxiliary DV packages**

When you import an Auxiliary Digital Vaccine package, such as ThreatDV, the SMS accesses TMC and verifies that you have this value-added feature. If a package is available, the SMS prompts you to download and install the package. Packages are downloaded and added to the Auxiliary DV list for activation as you need.

You can also configure the automatic update feature to have the SMS Client check and download updates periodically. When an Auxiliary Digital Vaccine is automatically downloaded, it is also activated. However, the Auxiliary DV has no impact on current profiles until the Auxiliary DV is distributed.

**Manage Auxiliary DV packages**

After you import a package, you can activate, delete and view the information for the package.
Uninstall an Auxiliary DV

**Note:** Uninstalling the Auxiliary DV uninstalls filters associated with the Auxiliary DV package. The enabled filters in the associated profile are NOT removed. The associated profile MUST be distributed to completely uninstall the Auxiliary DV filters for any device. See *Distribute profiles* on page 142.

1. On the Profiles navigation pane, click **Auxiliary DVs**.
2. On the Auxiliary DV Inventory section, select an entry.
3. Click **Uninstall**.

   The package uninstalls filters associated with the selected Auxiliary DV package. When you distribute profiles, the uninstalled Auxiliary DV is removed from the devices.

Distribute Auxiliary DV packages

When you distribute an Auxiliary DV package, you update the filter settings for a device. A package may include modifications including new filters, modified filters, and removed filters.

To set up the system to automatically distribute the package, see *Auto-download and distribute a DV, virtual DV, or Auxiliary DV* on page 192.

The screen enables you to manage all distributions through the Distribution Progress section of the screen. From this screen you select a specific distribution entry can perform any of the following actions:

- Details — Display details about the Auxiliary DV including number and names of devices.
- Stop Distribution — Stops the select Auxiliary DV distribution.
- Clear Obsolete — Clears an old or unwanted distribution listing.

**Note:** Auxiliary DV filters MUST be distributed to work. Activating the Auxiliary DV package enables the package for distribution and does NOT enable the filters in the Auxiliary DV package.

Clear an obsolete distribution listing for Auxiliary DVs

1. On the Profiles navigation pane, click **Auxiliary DV**.
2. On the Distribution Progress section, click **Clear Obsolete** to remove old entries.

Digital Vaccine Toolkit Packages

Digital Vaccine Toolkit is a TippingPoint application that lets you write custom filters for use on devices and the SMS. Custom filters are saved into package files, imported into the SMS, activated, and then distributed to devices.

When you activate a DV Toolkit package, a new SMS filter number is created. When you distribute the package, the filter number is synchronized across:
• **SMS Profiles** (search results and filter details)

• **SMS Reports.** However, if an existing or saved report has a DV Toolkit filter number (generated in a previous SMS release), the report still displays that number, not the new filter number.

• **SMS Events.** However, if an event listing has a DV Toolkit filter number from a previous SMS release, the event still displays that number, not the new filter number.

• **Device LSM** (Filter Overrides) and **CLI** (show filter and the show np rule commands)

• **DV Toolkit application.** When you export a DV Toolkit package from the SMS and import it on the DV Toolkit application, the package retains the filter number assigned to it by the SMS.

**Note:** The SMS only preserves filter numbers when the DV Toolkit package is exported and imported back on to the same SMS. The SMS might not preserve the filter numbers if the DV Toolkit package is imported into a different SMS.

**Original filter numbers assigned from the DV Toolkit application are included on the SMS**

The SMS saves the filter number that was originally created from the DV Toolkit application. You can view this filter number on the SMS in the Search Results.

**View DV Toolkit filter numbers on the device LSM**

When you view the filter overrides on the device LSM, the SMS-assigned filter number display on the filter name. However, you will not be able to view the original filter number that was created from the DV Toolkit application.

**View DV Toolkit filter numbers on the device CLI**

Use the show filter and the show np rule commands to view the SMS-assigned filter number. When entering these commands on the device CLI, do not to include `C` with the filter number.

You cannot view the original filter number that was created from the DV Toolkit application on the device CLI.

**Associate DV Toolkit packages with devices and profiles in the SMS**

Associating the filters in DV Toolkit packages with devices and profiles on the SMS involves these steps.

1. **Create a DV Toolkit package** on page 203.
2. **Import a DV Toolkit package** on page 204.
3. **Activate a DV Toolkit package** on page 205.
4. **Create an inspection profile** on page 138 (or edit an existing profile). Using this profile, you can **review filters from the active DV Toolkit packages and enable filter settings** on page 205.
5. **Distribute a DV Toolkit package to the device** on page 207.
6. **Distribute a profile to the device** on page 142.

### Create DV Toolkit packages

Use the DV Toolkit application to create and save custom filters to a package file. For instructions on creating DV Toolkit packages, see the *Digital Vaccine Toolkit and Converter User Guide* available on the TMC at [https://tmc.tippingpoint.com/TMC/](https://tmc.tippingpoint.com/TMC/).

### Limit access to DV Toolkit packages

You can use role-based access control for DV Toolkit packages. Access control lets you independently customize access rights and restrictions for each user based on role and group settings. As a result, you can set up DV Toolkit packages that only a certain group of users can see. Multiple users can have separate, active DV Toolkit packages running on the same SMS.

To limit access to DV Toolkit packages, select **Admin > Authentication and Authorization** and then:

- Create (or edit) a role and set capabilities for DV Toolkit Management (**Create Role** > **Capabilities** > **Profiles** > **DV Toolkit management**). See *Managing user roles* on page 558.
- Create (or edit) a group for each role and set which DV Toolkit packages the group can access (**Create Group** > **DV Toolkit Packages**). See *Managing user groups* on page 560.
- Create (or edit) a user and assign the group to the user (**Create User** > **Group Membership**).

### DV Toolkit Packages screen

The DV Toolkit Packages screen includes the following information:

- DV Toolkit Inventory — Lists the DV Toolkit packages that have been imported and are available for distribution.
- Distribution Progress — Provides information on distribution status of a DV Toolkit package for a device.

#### DV Toolkit Inventory

The following table describes the columns in the DV Toolkit Inventory table.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Package</td>
<td>Name of the DV Toolkit package.</td>
</tr>
<tr>
<td>Version</td>
<td>Version of the DV Toolkit package.</td>
</tr>
</tbody>
</table>
## Import a DV Toolkit package

When importing DV Toolkit packages, keep in mind:

- You must have a DV Toolkit package file. You can create this file using the DV Toolkit application.

- If you do not provide a name for the properties when you create the package it in the DV Toolkit application, the package name displays "untitled" in the SMS after you import it. It's a best practice to use a distinct name for the properties when you create the DV Toolkit package file. Within the DV Toolkit application, select **File > Properties** to change the name of the properties for the package.

- You can activate a new DV Toolkit package, or you can replace a currently active package (the SMS keeps the filter overrides for the previously active package).

1. Select **Profiles > DV Toolkit Packages**.
2. Click **Import**.
3. Click **Browse** to browse to and select a DV Toolkit package file.
4. To automatically activate the package and replace an existing (active) package, do the following:
   a. Select the **Activate the imported DV Toolkit package** check box.
   b. Click **OK**.
   c. Do any of the following:
      - To activate the new DV Toolkit package, click **Activate**. (The DV Toolkit package will be activated as a new package and will not be associated with existing filter overrides in any other package).
      - To replace an existing, active package, select the **Overwrite a currently active DV Toolkit with the activating DV Toolkit** check box, select a DV Toolkit package from the list of active packages, and...
then click **Overwrite**. (The DV Toolkit package will replace the selected package and the SMS will keep the filter overrides for the previously active package).

5. Click **OK**.

The package displays in the DV Toolkit Inventory table and the DV Toolkit Packages navigation pane. If the package is active, a green check mark displays under the Active column, and (active) displays after the package name in the DV Toolkit Packages navigation pane.

### Activate a DV Toolkit package

There are three ways to activate a DV Toolkit package.

- *When you import the DV Toolkit package* on page 204
- From the DV Toolkit Inventory
- From the DV Toolkit Details

When activating DV Toolkit packages, keep in mind:

- You can have multiple, active DV Toolkit packages on the SMS.
- After you activate a DV Toolkit package, you can search for (or create) an Inspection profile to review the filters in the DV Toolkit package. You can select one or more filters and edit the filter settings. By default, all filters in the DV Toolkit package are not enabled and have no recommended action set.
- You cannot delete an active DV Toolkit package. To delete a package, you must first deactivate it.

1. Do any of the following:
   - Select **Profiles > DV Toolkit Packages** and select a package from the DV Toolkit Inventory table.
   - Click **Profiles**, expand **DV Toolkit Packages** in the navigation pane, and then select a package.

2. Click **Activate**.

### Search for DV Toolkit filters

When searching for DV Toolkit filters, keep in mind:

- After you activate a DV Toolkit package, you can search for (or create) an Inspection profile to review the filters in the DV Toolkit package. You can select one or more filters and edit the filter settings. By default, all filters in the DV Toolkit package are not enabled and have no recommended action set.
- After you activate a DV Toolkit package, the SMS assigns a new filter number. You can view this filter number in the Search Results and the Filter Settings.
- The SMS also saves the filter number that was created from the DV Toolkit application. You can view this filter number in the Search Results.
• You can only search across the active DV Toolkit packages that you have access to. Access control lets you independently customize access rights and restrictions for each user based on role and group settings. See Limit access to DV Toolkit packages on page 203.

1. Select Profiles > Inspection Profiles and select an existing Inspection Profile. Alternatively, you can create a new profile. See Create a new profile on page 138.

2. To search for the filters in a DV Toolkit package, do any of the following:
   • Click Global Search to search across all listed Inspection Profiles for a DV Toolkit package.
   • Expand the name of a profile, and then click Search to perform a search within a selected profile. See Search on page 157.

3. Expand the Source Criteria panel, select the DV Toolkit check box, and then do the following:
   • Select an active DV Toolkit package from the drop-down list.
   • Select ANY to search across all active DV Toolkit packages.

4. Click Search.

   Based on the source criteria, the filters display in the search results.

5. To edit a filter, do any of the following:

<table>
<thead>
<tr>
<th>Select a filter</th>
<th>Edit filter settings - Actions</th>
</tr>
</thead>
</table>
| To enable one filter in a DV Toolkit package, double-click a filter name from the search results. | • Select Use Filter Specific Settings.  
• Select the Enabled check box.  
• Select an action from the Action Set drop-down list. |
| To enable more than one filter in a DV Toolkit package, select one or more filters from the search results, and then click Edit. | • Select Change filters to use the settings below.  
• Select Use Filter Specific Settings.  
• Select the Enabled check box.  
• Select an action from the Action Set drop-down list |
View DV Toolkit filter numbers in the Search Results

After you activate a DV Toolkit package, you can view the original DV Toolkit filter number in the Search Results. To view the DV Toolkit filter numbers in the Search Results, you must first set the visibility as the DV Toolkit Filter # column is hidden by default.

1. Select Profiles > Inspection Profiles > Search.
2. Right-click on the Search Results, and then select Table Properties.
3. Locate the DV Toolkit Filter # column name, and then select Visible.
4. Click OK.

Distribute a DV Toolkit package to the device

When distributing DV Toolkit packages to the device, keep in mind:

- An active DV Toolkit package enables the package for distribution; it does not enable the filters in the DV Toolkit package. You must distribute the package and the Inspection Profile to the device to enable the filters within the DV Toolkit package. When you distribute a DV Toolkit package, you update the filter settings for the device. A package may include modifications, such as new filters, modified filters, and removed filters.

- After you distribute a DV Toolkit package to the device, you can review the name of the package in the SMS on the Device Summary screen, the Device Configuration Summary screen, and the Device Configuration wizard.

- The SMS merges multiple DV Toolkit packages into a single package as the device only supports one DV Toolkit package.

**Important:** To properly maintain your security policy, perform a one-time DV Toolkit package reinstallation and profile redistribution. When you reinstall the DV Toolkit package, the SMS reassigns filter numbers to previously distributed DV Toolkit filters. When you distribute the profile back to the device, the SMS synchronizes the filter number with the device.

1. Do any of the following:
   - Select Profiles > DV Toolkit Packages and select an active package from the DV Toolkit Inventory table.
   - Select Profiles, expand DV Toolkit Packages in the navigation pane, and then select an (active) package.
2. Click Distribute.
3. Do any of the following:
   - Click the All Devices check box to distribute the package to all of your managed devices.
   - Expand All Devices, and then select one or more devices.
Select a device to be aware of the impact of the DV Toolkit package. Use the icons to see if a package will be added, removed, or replaced on the selected device.

- (Optional) Click the High Priority check box to designate the DV Toolkit package distribution as high priority. High priority updates will run before low priority updates.

4. Click **OK**.

**View DV Toolkit details**

The DV Toolkit Details screen includes the following information:

- **DV Toolkit Details** — Provides information about the imported DV Toolkit package.
- **Device DV Toolkit Inventory** — Lists the name of the devices that have received the distributed package. You can distribute the DV Toolkit package to more than one device at a time.

Do any of the following:

- Select **Profiles > DV Toolkit Packages**, select a package from the DV Toolkit Inventory table, and then click **Details**.
- Select **Profiles**, expand **DV Toolkit Packages** in the navigation pane, and then select a package.

**Remove DV Toolkit packages from the device and the SMS**

Removing DV Toolkit packages from the device and the SMS involves these steps.

1. **Deactivate a DV Toolkit package on the SMS** on page 208.
2. Redistribute the profiles that have filter overrides from the DV Toolkit package to the device(s).
3. **Uninstall a DV Toolkit package from the device** on page 209.
4. **Delete a DV Toolkit package from the SMS** on page 210.

**Note:** If you deactivated or deleted a DV Toolkit package from the SMS that you want to uninstall from the device, you must re-import the package and then uninstall it from the device.

**Deactivate a DV Toolkit package on the SMS**

When deactivating DV Toolkit packages on the SMS, keep in mind:

- You can only deactivate packages that are active. You must deactivate a package before you can delete it.
- The package is still available on the device. To remove a package from the device, you must uninstall it. See **Uninstall a DV Toolkit package from the device** on page 209.
- When you deactivate a package, the SMS:
  - Removes all existing profile filter overrides in the package.
- Removes the name of the package from the Inspection Profile search and global search (Source Criteria panel).

- Keeps the name of the package in the DV Toolkit Inventory table, DV Toolkit packages navigation pane, and the configuration and summary areas (Device Summary screen, Device Configuration Summary, and Device Configuration wizard). You must distribute the active DV Toolkit packages to the device to remove the package from the configuration and summary areas. You must delete the package to remove it from the inventory table and navigation pane.

1. Do any of the following:
   
   - Select **Profiles** > **DV Toolkit Packages** and select an active package from the DV Toolkit Inventory table.
   
   - Select **Profiles**, expand **DV Toolkit Packages** in the navigation pane, and then select an (active) package.

2. Click **Deactivate**.

### Uninstall a DV Toolkit package from the device

When uninstalling DV Toolkit packages to the device, keep in mind:

- You can only uninstall packages that have been distributed to the device.

- When you uninstall a package, the SMS:
  
  - Removes the package from the device. However, if the device has other active packages, these packages will be distributed to the device, and a new package will be created. To remove a package from the SMS, you must deactivate it. See *Deactivate a DV Toolkit package on the SMS* on page 208.
  
  - Removes the name of the package from the Device Summary screen, the Device Configuration Summary screen, and the Device Configuration wizard.
  
  - Keeps all existing profile filter overrides in the uninstalled package.
  
  - Keeps the name of the package in the DV Toolkit Inventory table, the DV Toolkit packages navigation pane, and the Inspection Profile search and global search (Source Criteria panel).

1. Select **Profiles** > **DV Toolkit Packages**.

2. Select a package that has been distributed to a device from the DV Toolkit Inventory table.

3. Click **Uninstall**.

4. Do any of the following:
   
   - Click the **All Devices** check box to uninstall the package from all of your managed devices.
   
   - Expand **All Devices**, and then select one or more devices.

   Select a device to be aware of the impact of the DV Toolkit package. Use the icons to see if a package will be added, removed, or replaced on the selected device.
• (Optional) Click the **High Priority** check box to designate the DV Toolkit package distribution as high priority. High priority updates will run before low priority updates.

5. Click **OK**.

   The package distributes to the selected device.

**Delete a DV Toolkit package from the SMS**

When deleting DV Toolkit packages from the SMS, keep in mind:

- You can only delete packages that are inactive. See *Deactivate a DV Toolkit package on the SMS* on page 208
- If the package was distributed to the device, it will still be available on the device. To remove the package from the device, you must uninstall it.

1. Select **Profiles > DV Toolkit Packages**.
2. Select an inactive package from the DV Toolkit Inventory table, and then click **Delete**.

**Reputation database**

The TippingPoint Reputation Database is a collection of IP addresses within a geographic region or country, DNS names, and URLs on an SMS that represent potential risks to network security. Entries can be user-provided, provided from the ThreatDV Feed, or both. There is no limit to the number of entries a user can provide. Entries in the Reputation Database can be tagged or untagged. A tagged entry consists of an IP address, a DNS address, or a URL, plus a reputation tag category and associated values. A tag category can be created manually or by ThreatDV. Tag categories created by the reputation service are read-only and may not be modified.

Entries can also be imported from a CSV file and must follow specific import Reputation rules. Untagged entries contain only an IP address, a DNS address, or a URL, and function as a user-defined list of sites to block.

**Note:** The SMS ignores any invalid entries imported from a CSV file. All IP, DNS, and URL tagged entries must be valid and correctly formatted before the SMS can apply the tag category values.

Reputation entries in the Reputation Database are used to create Reputation filters that target specific security needs of your network. See *Reputation filters* on page 175.

**Reputation database interface**

The Reputation database interface includes a tabbed screen that displays Summary, Activity, and Tag Categories tabs. Each tab provides information about Reputation database activity.
Summary tab

The Summary tab provides a summary of the number of entries in the database and the status of the database synchronization progress.

Database summary

The Database Summary area lists the number of entries contained in the Reputation Database. Each entry in the database contains an IP address, a domain name, or a URL, and may have one or more associated tag categories with specified values. A Reputation Database entry must contain an IP address, a domain name, or a URL, but does not have to be associated with a tag.

Activity tab

The Activity tab provides information about Reputation Database activity including:

- Sync Progress — Information about the synchronization of the Reputation Database on the SMS to one or more target devices.
- Tasks — Information about Reputation Database tasks such as adding, editing or importing entries.

Sync progress

Changes to the Reputation Database are automatically synchronized to devices which have reputation filters active. A complete (Full) database synchronization is performed when reputation filters are distributed to a device. After the reputation filters are distributed and the full synchronization is performed, subsequent synchronizations contain only changed (Delta) entries. A full synchronization is only needed for recovery purposes. The Reputation Database updates the list of Reputation entries to be included on the device. Entries are selected according to the criteria provided in any active Reputation filters existing on the device.

This area provides the following information about a Reputation Database package:

Table 64. Sync progress

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device</td>
<td>Number and name of one or more target devices.</td>
</tr>
<tr>
<td>Package</td>
<td>Type of synchronization, such as Full or Delta.</td>
</tr>
<tr>
<td>Distributed</td>
<td>Date and time of last successful synchronization.</td>
</tr>
<tr>
<td>Column</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Status</td>
<td>Status of the synchronization, such as Complete (Success).</td>
</tr>
<tr>
<td>Progress</td>
<td>Current progress of the synchronization.</td>
</tr>
</tbody>
</table>

**Tasks**

The tasks listed in this area include changes to the Reputation Database such as adding, editing or importing entries to the Reputation Database on the SMS. For status information about synchronizing the database with target devices, see the Sync Progress area of this tab.

This area provides the following information about Reputation Database tasks:

**Table 65. Tasks**

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Type of task.</td>
</tr>
<tr>
<td>Status</td>
<td>Status of task, such as Complete or In Progress.</td>
</tr>
<tr>
<td>Time Queued</td>
<td>Date and time when the task was placed in the queue.</td>
</tr>
<tr>
<td>Time Started/Completed</td>
<td>Date and time when the task started/completed.</td>
</tr>
</tbody>
</table>

View Reputation database details for distribution to device targets

1. On the Profiles navigation pane, click **Reputation Database**.
2. Click the **Activity** tab.
3. Select a device on the Sync Progress pane, and then click **Details**. The Sync to Device dialog provides information:
   - Status Details — Summary information about the Reputation Database Synchronization/Distribution.
   - Target Details — Information about target devices associated with the Reputation Database Synchronization/Distribution.
4. Click **Close**.

**Perform a full synchronization of the Reputation database**

Changes to the Reputation Database are automatically synchronized to devices which have reputation filters active. A full database synchronization is only needed for recovery purposes. To perform a full Reputation Database synchronization to the selected devices:

1. On the Profiles navigation pane, click **Reputation Database**.
2. On the **Edit** menu, click **Full Sync**.

**Stop a synchronization of the Reputation database**

1. On the Profiles navigation pane, click **Reputation Database**.
2. Click the **Activity** tab.
3. Select a device on the Sync Progress pane, and then click **Stop Sync**.

**Clear obsolete distribution entries**

1. On the Profiles navigation pane, click **Reputation Database**.
2. Click the **Activity** tab.
3. Select a device on the Sync Progress pane, and then click **Clear Obsolete**.

**Tag Categories tab**

The Tag Categories tab provides information on tag categories that define the types of tags that may be used to tag reputation database entries. A tag category can be created manually, by ThreatDV, or be predefined on the SMS. Tag categories can be imported or exported as a group in .xml format.

**Note:** To prevent duplicate definitions when importing profiles from another SMS or when managing a device that was managed by another SMS, export the Reputation Tag Categories from one SMS to the other. As a result, all SMS devices will recognize these Tag Categories as identical and will not treat them as different Tag Categories. You can then import or export Tag Categories many times between all SMS devices without resulting in duplicate definitions because each SMS will recognize previously imported or exported Tag Categories and will not duplicate them.

**Table 66. Reputation database tag categories**

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A unique name for the tag category.</td>
</tr>
<tr>
<td>Type</td>
<td>Type of data that the tag category contains:</td>
</tr>
<tr>
<td>Column</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>User Defined</td>
<td>An indication if a tag category was created by the user and not a subscription service.</td>
</tr>
<tr>
<td>Description</td>
<td>A brief description (up to 255 characters) indicating how the tag category is to be used.</td>
</tr>
</tbody>
</table>

**Table 67. Reputation database tag categories**

<table>
<thead>
<tr>
<th>Descriptive name</th>
<th>Type</th>
<th>Settings</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Comment</td>
<td>Text</td>
<td>Up to 255 characters</td>
<td></td>
</tr>
<tr>
<td>Country</td>
<td>List</td>
<td>A list of values, such as:</td>
<td>Defined values should be a subset of the descriptive name.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• China</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• France</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Mexico</td>
<td></td>
</tr>
<tr>
<td>Last Seen</td>
<td>Date</td>
<td>Date and time input format</td>
<td>For Input Format options, see help embedded in the Create/Edit Tag Category dialog.</td>
</tr>
<tr>
<td>Approved</td>
<td>Yes/No</td>
<td>Pre-defined values of:</td>
<td>Similar to the List category, this category has two pre-defined values, Yes or No.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Yes</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• No</td>
<td></td>
</tr>
</tbody>
</table>
Predefined tag categories

The SMS incorporates predefined tag categories from Deep Discovery (DD) devices. The advanced threat intelligence provided in these categories keeps the Reputation Database updated and enables robust reputation filters for enhanced protection of your system.

You can either configure your DD device to send this data automatically to the SMS (as a tag entry), or you can use the SMS to manually add or import the entries. To configure this integration from your DD device, refer to the documentation on the Trend Micro documentation site. To add these entries manually, you must define the tag categories listed in the following table so that the specific data you need can be mapped to the SMS.

**Important:** Only users with SuperUser permissions should manually add the predefined tag categories. For more information on account settings, see Authentication and authorization on page 542.

The SMS automatically includes the following predefined tag categories.

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Settings</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trend Micro Detection Category</td>
<td>List</td>
<td>Pre-defined values of:</td>
<td>Specifies which category the detection falls under.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Suspicious Object</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• C&amp;C Callback Address</td>
<td></td>
</tr>
<tr>
<td>Trend Micro Publisher</td>
<td>Text</td>
<td>Up to 255 characters</td>
<td>Can be used to identify the Trend Micro product name that discovered the threat.</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Settings</td>
<td>Notes</td>
</tr>
<tr>
<td>-----------------------</td>
<td>------</td>
<td>------------------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>Trend Micro Severity</td>
<td>List</td>
<td>Pre-defined values of:</td>
<td>Identifies the threat severity.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• High</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Medium</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Low</td>
<td></td>
</tr>
<tr>
<td>Trend Micro Source</td>
<td>Text</td>
<td>Up to 255 characters</td>
<td>Can be used to identify the configured host name of the Trend Micro device that discovered the threat.</td>
</tr>
</tbody>
</table>

**Import all tag categories**

1. On the Profiles navigation pane, click **Reputation Database**.
2. Click the **Tag Categories** tab.
3. Click **Import**.
4. Enter the name of the file to import or browse to its location.
5. Click **Next** to upload the file.

**Export all tag categories**

1. On the Profiles navigation pane, click **Reputation Database**.
2. Click the **Tag Categories** tab.
3. Click **Export**.
4. Enter the name of the file to save and browse to the area where you want to save the file.
5. Click **Save**.

**Add or edit a Reputation tag category**

1. On the Profiles navigation pane, click **Reputation Database**.
2. Click the **Tag Categories** tab.
3. To create a new tag category, click **Add**.
4. To edit an existing tag, select a tag from the table, and then click **Edit**, or right-click the selected tag entry, and then click **Edit**.
5. On the General area, complete the following information:
• Name — a unique name that identifies the tag category.

• Type — type of data (Text, List, Date, Yes/No, Number Range) that the tag category contains. Tag category types cannot be edited.

• Description — a brief description (up to 255 characters) indicating how the tag category is to be used.

6. In the Settings area, enter the appropriate information for the type of tag category you selected.

7. Click OK.

**Delete a Reputation tag category**

**Important:** Deleting a Reputation Tag category or LIST tag category value from a LIST tag category results in removal of that tag category or LIST tag category value from any Reputation entry or Reputation filter that uses those items. Before deleting any of these items, create an SMS backup. See Restore the SMS database on page 590.

1. On the Profiles navigation pane, click Reputation Database.

2. Click the Tag Categories tab.

3. Select a tag category from the inventory, and then click Delete.

**ThreatDV entries**

ThreatDV is a subscription-based service that identifies and delivers suspect IP, DNS, and URL addresses to subscribers. The addresses are tagged with reputation, geographic, and other identifiers for ready and easy security policy creation and management.

ThreatDV provides the addresses and tags multiple times a day in the same manner as standard Digital Vaccines. You can choose to download addresses into the Reputation database automatically or manually.

The ThreatDV IP/DNS Reputation Feed pane provides a summary of the IP/DNS Reputation Feed, including:

• License status — License status indicator and information for managed devices.

• Automatic DV download — Enabled/disabled status.

• Last DV installed — Date and time the last DV was installed.

• DV version — Version number of the DV.

• DV type — Type of DV.

• IPv4 — Number of entries with IPv4 addresses.

• IPv6 — Number of entries with IPv6 addresses.

• DNS — Number of entries with domain names.
• URL — Number of entries with web addresses.
• Total — Total of entries.

The ThreatDV URL Reputation Feed pane provides similar information for the URL Reputation Feed.

**Import a ThreatDV package**

**Note:** ThreatDV is a subscription-based service.

1. In a Web browser, open [https://tmc.tippingpoint.com/TMC/](https://tmc.tippingpoint.com/TMC/).

   If you have not already done so, create a TMC account using your Customer ID and Serial Number.

2. From the top menu, select **Releases > ThreatDV > SMS Full Reputation Feed**.

   The page lists all packages that are available. If you have a current ThreatDV subscription, reputation packages are included in the list. The most recent version is at the top of the list.

3. In the Download File page, click the **Download** button.

   After a few seconds, the File Download dialog box is displayed.

4. Click **Save**.

   The Save As dialog box displays. Navigate to the location where you want to save the file, and click the **Save** button. The file will be saved to the location you specified.

   **Note:** To avoid unexpected behavior on the SMS, do not change the name of this file.

5. In the SMS, on the Profiles navigation pane:

   • Click **Digital Vaccines** to display the DV Inventory screen.

   • Click **Auxiliary DV** to display the Auto Auxiliary DV Activation screen.

6. On the DV Inventory or Auxiliary DV Inventory section, click **Import**.

7. Locate and select the file to import. Click **OK** to begin import.

**Reset a ThreatDV**

**Important:** Reset DV deletes ALL Reputation DV entries in the Reputation Database and CANNOT be undone. ThreatDV tag categories are NOT deleted.

1. On the Profiles navigation pane, expand **Reputation Database**, and then click **ThreatDV Entries**.

2. To reset the DV for IP/DNS entries, click **Reset DV** in the ThreatDV IP/DNS Reputation Feed pane at the top. To reset the DV for URL entries, click **Reset DV** in the ThreatDV URL Reputation Feed pane at the bottom.

3. Verify that you want to delete ALL Reputation DV entries in the Reputation Database, and then click **OK**.
User entries

The SMS supports an unlimited number of user-provided entries to the Reputation Database. Reputation entries represent IP addresses, domain names, or URLs that are known to be malicious or that are otherwise listed for specific handling by reputation filters. Address entries in the Reputation Database can be tagged or untagged. Untagged entries contain only an address and function as a user-defined list of sites to block. A CIDR counts as a single entry.

The time it takes before users begin to see their imported entries appear in the SMS interface depends on a number of factors:

- The number of user entries being added.
- The number of user entries that already exist.
- The congestion of the reputation processing queue.

In a typical scenario—a few hundred entries contained in the file import, less than 100K user entries already on the system, and an empty reputation processing queue—entries can begin to appear in the SMS interface in as little as a minute's time. However, processing time increases along with the number of user entries and the number of tasks staged in the processing queue, which could include profile distributions and full Reputation DV feeds. In fact, entries cannot be imported until previously existing tasks in the queue have been completed.

When an address is added to the database, you can associate one or more tag categories. For existing address entries, you can add or remove one or more associated tag categories. When you associate a tag category with an address, you must also specify one or more of the possible values for that tag category. Reputation entries are used to create filters. See Reputation filters on page 175.

Import entries into the Reputation database

You can create a file that contains the information you want to add to the Reputation Database. For IP and DNS entries, the import file must be in comma-separated value (CSV) format with each line made up of one or more fields separated by commas. The file can contain addresses only or addresses and one or more associated tags. For URL entries, the import file must be delimited by a pipe (|) instead of commas, and entries can be URLs only or URLs with one or more associated tags. There is no limit to the number of entries you can add to the file that you import. See Reputation import rules on page 691.

Import user-provided entries to the Reputation database from a file

1. Before you create your import file, refer to Reputation import rules on page 691.
2. On the Profiles navigation pane, expand Reputation Database, and then click User Entries.
3. Click Import.
4. Specify the path of the file you would like to import, or click Browse and select the file.
5. Click Next to upload the file.
6. On the Import Reputation Entries dialog, select the types of entries in the import file: IPv4, IPv6, DNS names, or URLs, and then click Next.

7. Specify the tags to use with the imported entries.
   - Import tags from file — Indicates that tags in the import file should be applied to imported entries.
   - Specify tags to apply to all imported entries — Select this option to display a screen from which you can choose the tags, and their values, to apply to imported entries.
   - Import tags from file and specify tags to apply to all imported entries — Select this option to apply both tags from the import file and tags you select from the next screen to imported entries. Conflicts are handled according the setting of the User-specified tags override tags from import file option.
   - User-specified tags override tags from import file — This option is available only when the Import tags from file and specify tags to apply to all imported entries option is selected. This item specifies how to handle tags in the file and tags you specify on the next screen that have the same name. If this option is selected, tags you select on the next screen will take precedence over tags from the import file. If this option is not selected, tags from the file will take precedence over tags you specify on the next screen.

8. Click Next.

9. Review the summary information about the import.
   - If correct, click Finish.
   - If incorrect, click Previous and make any needed changes.

Adding user-provided entries to the Reputation database

You can manually add address and URL entries in the Reputation database. When you add entries, you have the option to add addresses and URL entries only or add addresses and URL entries with tag categories and values. A CIDR counts as a single entry. Entries with tags provide more options for tracking and blocking suspicious traffic. See Reputation filters on page 175.

Add a user-provided entry (addresses and URLs only) to the Reputation Database

1. On the Profiles navigation pane, expand Reputation Database, and then click User Entries.
2. Click Add.
3. Select the type of address and enter the corresponding information:
   - IP Address
   - DNS Domain For DNS, you can select Exact Match for the domain name
   - URLs
4. Click OK.
Add an address, URL, tag category, or tag value to the Reputation database

1. On the Profiles navigation pane, expand **Reputation Database**, and then click **User Entries**.
2. Click **Add**.
3. Add Address information. Select the type of address and enter the corresponding information:
   - IP Address
   - DNS Domain. For DNS, you can select **Exact Match** for the domain name
   - URL
4. Add one or more tags with specific value. For each tag:
   a. Select the tag.
   b. Add the value for selected tag.
5. Click **OK**.

Exporting user-provided Reputation entries

You can export user-provided Reputation entries to a file. For IP and DNS entries, the file must be in comma-separated value (CSV) format with each line made up of one or more fields separated by commas. For URL entries, the file must be delimited by a pipe (|) instead of commas. You can export entries to capture the state of the Reputation database and then quickly restore it at a later time.

Export a user-provided entry from the Reputation Database

1. On the Profiles navigation pane, expand **Reputation Database**, and then click **User Entries**.
2. Click **Export**.
3. Click **Browse** to select the location where the file will be exported to.
4. Click **Next** and then select the type of entry to export:
   - IPv4
   - IPv6
   - DNS names
   - URL
5. Click **Finish**.

Geographic entries

For information on import information and Lookup services for the Geo Locator database, see **Geo Locator database** on page 652.
Reputation database search

The Search Entries screen provides a convenient area to search for entries in the Reputation Database using user-defined filter criteria to build a search query. The search criteria are specified by including tag categories and values for the various tag categories. By default, all tag categories known to the SMS are displayed as columns in the result table.

Search criteria

When building a search query, you can use the following criteria:

- **Entry criteria** — Search criteria based on the type of address entry in the Reputation database.
- **Tag criteria** — Search criteria based on the tags in the Reputation database. This area lists the available tag categories in the Reputation database that can be included in the search.

Table 69. Reputation database search criteria

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>Select this option if the entry represents an IP address or block of IP addresses. The specified address may be either IPv4 or IPv6. If the value represents a block of IP addresses, the value should end with a “/” followed by a prefix length.</td>
</tr>
<tr>
<td>DNS Domain</td>
<td>Select this option if the entry represents a DNS name. If this option is selected, DNS lookup requests for the specified entry are dropped by the IPS.</td>
</tr>
<tr>
<td>URL</td>
<td>Select this option if the entry represents a URL. The URL must be less than 4K in length. A single wildcard string * (backslash and asterisk) is supported. URL categories, such as Travel, are not supported. <strong>Note</strong>: Selecting this option searches for <em>user-defined</em> URL entries only. To look up entries and scores in the ThreatDV URL Reputation Feed, select ThreatDV URL Lookup in the navigation pane.</td>
</tr>
</tbody>
</table>
Table 70. Reputation database search criteria

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Include Untagged Entries</td>
<td>Includes addresses that do not have tags associated with them.</td>
</tr>
<tr>
<td>Include Tagged Entries</td>
<td>Includes addresses that have tags associated with them.</td>
</tr>
<tr>
<td>Include Rep DV Entries</td>
<td>Includes Reputation Digital Vaccine entries, an optional subscription-based service. These entries are displayed in a separate column on the search results table.</td>
</tr>
<tr>
<td>Include User Entries</td>
<td>Includes user entries. These entries are displayed in a separate column on the search results table.</td>
</tr>
<tr>
<td>Include Geographic</td>
<td>Includes Geographic information based on a computer’s IP address/hostname within a geographic region or country. These entries are displayed in the Address and Geo Filter Country columns on the search results table.</td>
</tr>
</tbody>
</table>

See Tag Categories tab on page 213.

Search results

The Search table lists the results of your customized search. User-Created Reputation entries can be included in a Reputation or a Geographic filter. When you add a new entry to the Reputation Database, the listing is automatically added to the results table.

Search for entries in the Reputation database

1. Review the information in Search criteria on page 222.
2. On the Profiles navigation pane, expand Reputation Database, and then click Search.
3. For Entry Criteria to include in the search, select from the following and enter the associated entry:
   - IP Address — An IP address or block of IP addresses
   - DNS Domain — A DNS name To search for an exact DNS match, select the Exact Match check box
   - URL — Any URL less than 4K in length
4. For **Tag Criteria** to include in the search, use the check box next to the name of the tag category to include it in the search criteria. Use the expanded view to add specific tag search criteria.

5. Select one or more tag categories to include in the search.

   When you select a tag, the default criteria is “Tag is present and has a value.”

6. To select other criteria, expand the entry and select desired criteria. See *Reputation database interface* on page 210.

7. Click **Search**.

   The results display in the results table in the bottom of the screen.

**Edit bulk (all searched database entries)**

1. Search the database using the appropriate criteria to find desired user-provided entries. See *Search for entries in the Reputation database* on page 223.

2. Click **Edit Bulk** to change all the user-provided entries that match the current search criteria.

3. The Edit Reputation Entry dialog displays.

   The Query Expression indicates the current search criteria used for the screened entries.

4. You can add or remove one or more tags to the entries.

   • To remove a tag, deselect the category.
   • To add a tag, select the tag category and add a specific value.

5. To create a new tag category, click **Add Tag Category**.

6. To change or modify values for an existing tag, click **Different Values** next to the name of the tag and enter the new value.

   **Important:** When you select Edit Bulk, all user provided entries that match the current search criteria are edited. The operation can NOT be undone.

7. Click **OK**.

**Delete bulk (all searched database entries)**

1. Search the database using the appropriate criteria to find desired user-provided entries. See *Search for entries in the Reputation database* on page 223.

2. Click **Delete Bulk** to delete all the user-provided entries that match the current search criteria.

   **Important:** When you select Delete Bulk, all user provided entries that match the current search criteria are deleted. The operation can NOT be undone.

3. To confirm that you want to delete all matching user-provided entries, click **Yes** in the **Delete All User Reputation Entries** dialog.
Edit a user provided entry in the Reputation database

**Note:** The Address, URL, and DNS Domain fields cannot be edited.

1. Search the database using the appropriate criteria to find desired user provided entries. See *Search for entries in the Reputation database* on page 223.

2. Select an entry from the table and click **Edit**.

   The Edit Reputation Entry dialog displays.

3. You can add or remove one or more tags to the entries.
   - To remove a tag, deselect the category.
   - To add a tag, select the tag category and add a specific value.

4. To create a new tag category, click **Add Tag Category**.

5. Click **OK**.

Edit multiple user-provided entries in the Reputation database

1. Search the database using the appropriate criteria to find desired user-provided entries. See *Search for entries in the Reputation database* on page 223.

2. To select multiple entries, do one of the following:
   - Hold down the **SHIFT** key, and then select desired range of user-provided entries.
   - Hold down the **CTRL** key, and then select specific user-provided entries.

3. Select one or more listings from the Reputation Entries area.

4. You can add or remove one or more tags to the entries.
   - To remove a tag, deselect the category.
   - To add a tag, select the tag category and add a specific value.

5. To create a new tag category, click **Add Tag Category**.

6. Click **OK**.

**ThreatDV URL Lookup**

From the **Reputation Database > ThreatDV URL Lookup** page, you can query the ThreatDV URL Reputation Feed to see if a specific URL is in the database.

After you specify the URL that you want to look up and click **Search**, the results table lists any matching entry in the database along with its Reputation score.
A wildcard string (\*) cannot be used as a query string. For example, the following use of the wildcard string is not permitted:

http://mywebsite.com/path/to/resource?\*

As a workaround, you can use the wildcard string earlier in the path:

http://mywebsite.com/path/to/\*

Scheduled distributions

The SMS provides the flexibility to schedule a profile distribution to meet the specific needs of your network. For example, you may want to schedule profile distributions during off-peak times, take advantage of a maintenance window, or address specific traffic patterns.

Create a new profile distribution

1. On the Profiles navigation pane, click Scheduled Distributions.
2. Click New.
3. Complete the information for each screen and click Next to continue.
   - To return to a previous screen, click Previous. After entering information on the final screen, click Finish to save your entries.
4. On the General Settings screen:
   a. Enter a name for the schedule and the scheduled time or recurring schedule you want to use.
   b. Select the profile you want to distribute.
   c. Click Next.
5. On the Segment Groups screen:
   a. Select a segment or segments groups as targets for the profile schedule.
   b. Select High Priority if you want the profile delivered at a high priority. See Distribute profiles on page 142 for more information on priority distributions.
   c. Click Finish.

View a profile schedule

1. On the Profiles navigation pane, select Scheduled Distributions.
2. To view details for any scheduled profile distribution, double-click an individual scheduled profile.

Edit a profile schedule

1. On the Profiles navigation pane, click Scheduled Distributions.
2. Click **Edit**.
3. Make any needed changes.

**Vulnerability Scans (eVR)**

Enterprise Vulnerability Remediation (eVR) enhances visibility into your network by allowing you to pull in data from third-party vulnerability management vendors, match publicly known Common Vulnerabilities and Exposures (CVEs) to DV filters, and take immediate action on your security policy by tuning your IPS enforcement security policy to protect against the known vulnerabilities in your network, all within the SMS.

Custom converters are available for Qualys®, Rapid7 Nexpose®, and Tenable™ Nessus®.

**Table 71. Vulnerability Scans (eVR) tasks**

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Import vulnerability scans (eVR) on page 228</strong></td>
<td>Import a vulnerability scan. After you pull in the vulnerability information, you can add comments on page 229 and show CVEs for a selected vulnerability scan on page 229.</td>
</tr>
<tr>
<td><strong>Search vulnerability scans for CVEs on page 230</strong></td>
<td>Search for CVEs imported on the SMS vulnerability scan database. You can review the vulnerabilities identified in your network on page 231, sorted by CVE, and which assets are impacted by these vulnerabilities.</td>
</tr>
<tr>
<td><strong>Profile tuning on page 234</strong></td>
<td>Assess true vulnerabilities and restrict access to assets.</td>
</tr>
<tr>
<td><strong>View CVE details on page 233</strong></td>
<td>View CVE details on page 233, flag CVEs for follow-up, and track changes to your security policy.</td>
</tr>
<tr>
<td><strong>Delete vulnerability scans on page 235</strong></td>
<td>Remove a vulnerability scan from the SMS.</td>
</tr>
</tbody>
</table>

**Note:** When you perform a backup restore on the SMS, if the backup version does not match the current SMS version, the vulnerability scan (eVR) converters are not restored. The vulnerability scan (eVR) converters are only restored during a backup if the backup version and the current version of the SMS are the same.
Enable sharing CVE coverage gaps with the TMC

Select Edit > Preferences > Security > Enable sharing CVE coverage gaps to help TippingPoint improve DV coverage to enable the SMS to send CVE IDs that are included within a scan file but are not yet identified within a DV filter to the TMC. For more information, see TMC Information Share on page 41.

Import vulnerability scans (eVR)

1. Run a vulnerability assessment report (vulnerability scan) using supported vulnerability management products from Qualys, Rapid7, and Tenable.
2. Export the result of the vulnerability scan to a supported file format for use on the SMS.
3. Select Profiles > Vulnerability Scans (eVR).
4. Click Import.
5. Click Browse and select a vulnerability scan.
6. Depending on the vulnerability management tool used to run the scan, select the appropriate converter:
   - Select Native if the vulnerability scan is an SMS-Standard CSV file.
   - Select Custom, and select the respective vulnerability management product: Qualys-CSV, Nessus, or Nexpose.

   To successfully import or convert a vulnerability scan, review the Vulnerability scan (eVR) specifications on page 228.

   The Converter Properties displays the converter version, the export format of the vulnerability scan (for example, CSV or XML), and the name of vulnerability management vendor.
7. (Optional) Enter comments about when the scan was imported.
8. Click OK.

   The SMS converts the file and imports the data from the vulnerability scan. The SMS also displays the conversion results and the number of import errors. You can download the Conversion Information File. If the SMS detected any errors while converting or importing the vulnerability scan, you can download the Conversion Error File.
9. Click OK.

   Note: You can also import vulnerability scan data using the Vulnerability Scans (eVR) API. For more information, see the Security Management System Web API Guide.

Vulnerability scan (eVR) specifications

Vulnerability scans must be in a native, comma-separated value (CSV) format before they can be used on the SMS. If you use a supported vulnerability management product from Qualys, Rapid7, or Tenable, the SMS can automatically convert those vulnerability scan results into native format.
**CSV file specifications**

Note the following CSV file specifications (and sequence) before you import a vulnerability scan:

- The first line in the CSV file must be the column headers for each of the columns.
- Each row after the header must contain the same number of columns that are in the header.
- Each column must be delimited with a comma.
- The value within each column must be wrapped in double quotes; however, embedded double quotes are not permitted ("This is "invalid" data").
- Each row in a CSV file must be less than 65536 bytes.

**Vulnerability scan specifications**

The minimum data required for a vulnerability scan is:

- **IP Address** - (host IP addresses) The maximum number of host IP address and vulnerability combinations that you can import on the SMS is 10 million. When the SMS reaches the maximum limit, it displays an error message, and you must delete vulnerability scans before you can import a new scan on page 228.
- **CVE IDs** - CVE must be in the format CVE-YYYY-NNNN where YYYY is a 4 digit year and NNNN is a sequence number.
- **Severity** - Vulnerabilities are assigned a severity levels to define the urgency associated with remediating each vulnerability. Rankings are based on a variety of industry standards including CVE.

**Comment on a vulnerability scan**

You can comment on a vulnerability scan. For example, you can add notes about when a scan was imported, or you can track all remediation changes in subsequent scans.

You can also comment on a CVE on page 233.

1. Select Profiles > Vulnerability Scans (eVR).
2. Select a vulnerability scan, and click Comments.
3. Enter Comments.
4. Click OK.

**Show CVEs for a selected vulnerability scan**

After you import a vulnerability scan, you can view the CVEs.

1. Select Profiles > Vulnerability Scans (eVR).
2. Select a vulnerability scan, and click Show CVEs to view the CVE Search Results on page 231.
Search vulnerability scans for CVEs

1. Select Profiles > Vulnerability Scans (eVR) > CVE Search.
2. Click Scan Criteria to search for:

<table>
<thead>
<tr>
<th>Select this criteria:</th>
<th>To search for ...</th>
</tr>
</thead>
</table>
| **Scans**              | • Select **All** to perform a global search through all imported vulnerability scans.  
                         | • Select the check box next to the vulnerability scan for a specific file. |
| **Scan Vendor**        | • Select **Any** to search for a supported vendor. |
| **Scan Time**          | Start and end dates for when the vulnerability scan was generated.  
                         | **Start time:**  
                         | • Select **Start Time** to enter a date in MM/DD/YY HH:MM format.  
                         | • Select **Start Time**, click the calendar icon to select a date/time from the calendar, and click **OK**.  
                         | **End time:**  
                         | • Select **End Time** to enter a date in MM/DD/YY HH:MM format.  
                         | • Select **End Time**, click the calendar icon to select a date/time from the calendar, and click **OK**. |
| **Import Time**        | Start and end dates for when the vulnerability scan was imported on the SMS.  
                         | **Start time:**  
                         | • Select **Start Time** to enter a date in MM/DD/YY HH:MM format.  
                         | • Select **Start Time**, click the calendar icon to select a date/time from the calendar, and click **OK**.  
                         | **End time:**  
                         | • Select **End Time** to enter a date in MM/DD/YY HH:MM format. |
3. Click **CVE Criteria** to search for:

<table>
<thead>
<tr>
<th>Select this criteria:</th>
<th>To search for ...</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CVE Details</strong></td>
<td>• Unique tracking number used to identify a Common Vulnerabilities and Exposures (CVE).</td>
</tr>
</tbody>
</table>
| **Discovered Time**   | Start and end dates for when the CVE vulnerability was discovered.  
Start time:  
• Select **Start Time** to enter a date in MM/DD/YY HH:MM format.  
• Select **Start Time**, click the calendar icon to select a date/time from the calendar, and click **OK**.  
End time:  
• Select **End Time** to enter a date in MM/DD/YY HH:MM format.  
• Select **End Time**, click the calendar icon to select a date/time from the calendar, and click **OK**. |
| **Assets**            | • One or more IP addresses for an asset. An asset is the network IP address of the host vulnerable to the CVE identified in the vulnerability scan. |
| **Flagged Status**    | • **Flagged** - All CVEs that are flagged for follow-up.  
• **Not Flagged** - All CVEs that are not flagged. |

4. Click **Search**.

**View CVE search results**

The CVE Search Results displays the following information:
### Table 72. CVE search results

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE</td>
<td>Unique tracking number used to identify Common Vulnerabilities and Exposures (CVE). CVEs are publicly known security vulnerabilities.</td>
</tr>
<tr>
<td>Filters</td>
<td>Unique name and number used to identify the security filters on page 169 or application filters on page 172 that are associated with a CVE.</td>
</tr>
<tr>
<td></td>
<td>If there is more than one filter associated for a CVE, the SMS displays the number of filters in parentheses. Click the + symbol next to the CVE to view all of the filter names.</td>
</tr>
<tr>
<td>Not Protected Profiles</td>
<td>List of profiles on page 135 on the SMS that are not currently protected from a CVE.</td>
</tr>
<tr>
<td></td>
<td>If there is more than one profile that is not protected from a CVE, the SMS displays the number of profiles in parentheses. Click the + symbol next to the CVE to view all of the profiles that are not protected.</td>
</tr>
<tr>
<td></td>
<td>Note: Ignored profiles do not display in this list. See View CVE details on page 233 to ignore or show profiles for the CVE.</td>
</tr>
<tr>
<td>Protected Profiles</td>
<td>List of profiles on page 135 on the SMS that are currently protected from a CVE.</td>
</tr>
<tr>
<td></td>
<td>If there is more than one profile that is protected from a CVE, the SMS displays the number of profiles in parentheses. Click the + symbol next to the CVE to view all of the protected profiles.</td>
</tr>
<tr>
<td></td>
<td>Note: Ignored profiles do not display in this list. See View CVE details on page 233 to ignore or show profiles for the CVE.</td>
</tr>
<tr>
<td>Assets</td>
<td>Network assets discovered in a vulnerability scan. Assets include IP addresses of the host vulnerable to the CVE and the Asset Group.</td>
</tr>
<tr>
<td></td>
<td>If there is more than one asset associated for a CVE, the SMS displays the number of assets in parentheses. Click the + symbol next to the CVE to view all of the assets.</td>
</tr>
<tr>
<td>Flagged</td>
<td>Indicates if the CVE has been flagged for follow-up.</td>
</tr>
</tbody>
</table>
You can right-click on entries in the CVE search results and do the following:

- **Find/Filter** — Search for a filter using a keyword
- **Details** — View or edit CVE details
- **Set Flagged**— Quickly change the flagged status for one or more CVEs

### View CVE details

A vulnerability scan captures vulnerability information in your network at a single point in time. After you import the scan on the SMS, you can view CVE details for every CVE identified within the vulnerability scan.

1. Select **Profiles > Vulnerability Scans (eVR) > CVE Search**.
2. Select a CVE from the **CVE Search Results** on page 231 and click **Details**. Alternatively, you can double-click a CVE in the CVE Search Results.
3. Click **Details** to:
   - Access the URL link to the CVE database.
   - **Flag** the CVE for follow-up. You can quickly search for flagged CVEs on page 230 on the SMS.
   - Add or edit comments for the CVE. You can also add comments to the vulnerability scan on page 229.
4. Click **Ignored Profiles** to view a list of profiles, and do the following:
   - Select a profile, and click **Ignore** to hide the profile from the list of **Not Protected Profiles** and **Protected Profiles**. See **View CVE search results** on page 231.
   - Select a profile, and click **Show** to display the profile on the list of **Not Protected Profiles** and **Protected Profiles**. See **View CVE search results** on page 231.
5. Click **Filters** to view a list of active DV filters that correlate with the CVE.
6. Click **Assets** to view a list of network assets, such as the host IP addresses and the asset groups vulnerable to the CVE, as identified in the vulnerability scan.
7. Click **OK**.
Profile tuning

Profile tuning enables you make the right decision on how to remediate a vulnerability. Remediation might involve updating an asset, scheduling a change window to execute a patch, or turning the Digital Vaccine filter on in absence of an update from the software vendor.

1. Select Profiles > Vulnerability Scans (eVR) > Profile Tuning.

   The SMS displays a list of available profiles on page 135 including the version and the dates the profile was last modified and distributed.

2. Select a profile, and click Next.

   The SMS correlates the CVEs provided through a scan to the CVEs of DV filters, and lists all filters that are currently Not Protected and Permit Traffic.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Unique name and number used to identify a filter.</td>
</tr>
<tr>
<td>Action Set</td>
<td>Current action set on page 123 assigned to a filter and are set to disabled by default.</td>
</tr>
<tr>
<td>Category</td>
<td>Every DV filter is assigned to a category on page 152 and cannot be changed.</td>
</tr>
<tr>
<td>Source</td>
<td>All CVEs that match a filter.</td>
</tr>
<tr>
<td>Severity</td>
<td>Severity on page 151 level assigned to a filter, which helps you prioritize the vulnerabilities found.</td>
</tr>
</tbody>
</table>

3. Review the list of Not Protected/Permitting Filters.

   To remediate these vulnerabilities, TippingPoint recommends that you apply a blocking action set (Block, Block + Notify, or Block + Notify + Trace) to every filter.

   However, in some cases, you may need to override the recommended action for individual filters due to specific network requirements, or in cases where the recommended settings for a filter interact poorly with your network. After a filter is customized, it is not affected by the global category settings that specify the filter State and Action.

   • To use the recommended policy: Select one or more filters, select a blocking action set from the Change these filters to drop-down list, and click Apply to Selected.
• To override the recommended policy: Select a filter, and select an action set from the **Pending Action Set** drop-down list.

If you ignore an action set for a filter, select **Show Ignored Filters** to show or hide these filters.

Click **Next**.

The SMS lists all of the CVEs that are included in a vulnerability scan, but that do not match the CVEs of a DV filter.

4. Review the list of **Vulnerabilities with no Protection**, and do one of the following:
   • Enter comments for the selected CVE.
   • **View CVE Details** on page 233.

Click **Next**.

The SMS lists all of the modified filters including the pending action set changes.

5. Review the list of **Modified Filters**, and do one of the following:
   • Enter the same comments for all of the modified filters within the profile.
   • Click **Launch distribution wizard when finished** to immediately **distribute the profile** on page 142.
   • Click **Finish** to save the updates to your security policy without distributing the profile.

### Delete vulnerability scans

When you delete a vulnerability scan, you delete all data including CVEs, matching DV filters, and assets, such as the host IP addresses and the asset groups.

1. Select **Profiles > Vulnerability Scans (eVR)**.
2. Select one or more vulnerability scans, and click **Delete**.

### Firewall profiles

Firewall rules are created to permit or block network traffic between subnets connect to the firewall. Rules can match network zones, IP addresses, users, services, applications and time-of-day. Appropriate policies are applied to the different types of traffic. Typically, policies allow internal networks access to external resources while blocking external access to sensitive internal networks.

Tipping Point Next Generation Firewall (NGFW) enhances the traditional use of firewall rule sets by supporting application and user awareness. New application awareness classifications can be applied on top of existing stateless rules to control a subset of additional applications that have been identified.
An application firewall controls applications on the network by inspecting the traffic and determining the application by the packet contents unlike a stateless firewall that simply uses the information in the packet headers.

A firewall rule consists of three basic units:

- **Rule criteria** — Values specified for various traffic classifiers to determine if traffic matches a rule. For example, 123.43.12.156 might be a criteria value specified for the Source IP Address traffic classifier.

- **Action sets** — Specifies what the system should do when traffic matches a rule.

- **Inspection profiles** — An inspection profile performs additional evaluation of traffic that is permitted by a firewall rule. Two inspection profiles can be specified on a rule:
  - Security — Performs deep packet inspection based on the filter settings in the selected profile.
  - Reputation — Compares IP addresses to the reputation entries in the selected profile.

For more information on NGFW policy and firewall rules, see the *Tipping Point Next Generation Firewall Concepts and Deployment Guide*.

**Important:** When you start managing a firewall device, the default action set is Block. This action set does not include notifications. Blocked traffic will not appear as an event or send notifications so you may not realize that traffic is being blocked.

## Security zones (Firewall only)

Security zones allow you to group interfaces from one or more devices to make it easier to define policy. Groups of interfaces are assigned to zones with inspection policy applied to traffic moving between the zones. This allows for both flexibility and granularity when creating Inspection policies.

Each device has an included security zone of this-device. It isn’t visible in the list of security zones but does appear as an option when choosing security zones when creating rules. The this-device zone applies to traffic that has a source or destination for that particular device itself, such as IPv6 neighbor traffic and DHCP requests. It is included by default in the any zone, but when the any zone is not in use, this-device must be specified if traffic is meant to communicate with the device.

### Create or edit a security zone

1. Select **Profiles > Shared Settings > Security Zones**.
2. Do one of the following:
   - Click **New** to create a new security zone.
   - Select an existing security zone, and click **Edit**.
3. Enter a **Name** for the security zone.
4. Enter a **Description** for the security zone.
5. Select **Application Visibility** to monitor applications passing through the zone.

   **Note:** This forces additional inspection of the traffic as it passes through the device and could affect performance.

6. Click **Add** to add interfaces to the zone. Select the interface(s), and click **OK**.
7. To remove interfaces, select the interface in the Member Interfaces list, and click **Remove**.
8. Click **OK**.

**Schedules (Firewall only)**

You can create and manage schedules to specify when to include or exclude traffic. Each schedule consists of a name and up to four intervals. An interval is defined by days and start and end times. If a schedule contains multiple intervals, click the plus (+) sign next to the name to show the schedule intervals.

**Note:** You cannot delete a schedule if it is used by one or more firewall rules, whether or not the rule has been distributed.

If a schedule contains multiple intervals, click the plus (+) sign next to the name to show the schedule intervals.

You can click **Collapse All** or **Expand All** to collapse or expand all the schedules in the list.

**Tip:** On the Schedules screen, the right-click menu provides a shortcut to create a new schedule, edit or delete an existing schedule, or to add or edit a time interval for a schedule.

**Create or edit a schedule**

1. Select **Profiles > Shared Settings > Schedules**.
2. Click **Schedules**.
3. Do one of the following:
   - Click **New** to create a new schedule.
   - Select an existing schedule, and click **Edit**.
4. Enter a **Name** for the schedule.
5. Select the days and specify start and end times to define the interval.

   **Note:** Note that 12:00 AM is midnight and 12:00 PM is noon. The start time and end time must occur in the same day (a valid time interval never has a start time before midnight and an end time after midnight).

6. Click **OK**.
Service groups (Firewall only)

Service groups allow you to group services together, similar to application groups, in a single element to make policy management easier.

Create or edit a service group

1. Select Profiles > Shared Settings > Service Groups.
2. Do one of the following:
   - Click New to create a new service group.
   - Select an existing service group, and click Edit.
3. Enter a Name for the service group.
4. Enter a Description of the group.
5. To include a service to a group, either select a single service from the list and clicking the single arrow button to move it to the Member Services list or by clicking the double arrows to move all of the services to the Member Services list.
   
   You can remove services from the Member Services list by selecting the service and clicking the single arrow back. Clicking the double Arrow will move all of the services out of the Member Services list.
6. Click OK.

Application groups (Firewall only)

Application groups allow you to create groups of applications using query criteria or by selecting applications individually so the groups can be used in other policy settings. You can easily select groups based on the following categories:

- Application or Application Category
- Protocol and Protocol OSI Layer
- Function and Transactions
- Application Class and Vendor

Note: By default, when an entire application is checked, all its transactions that match the criteria are included. From the <Transaction> drop-down menu, you can specify any transactions of a selected application function that you want to exclude (in other words, the profile reflects the entire application function criteria minus the transactions marked is not).

Create or edit an application group

1. Select Profiles > Shared Settings > Application Groups.
2. Do one of the following:
   - Click **New** to create a new application group.
   - Select an existing application group, and click **Edit**.

3. Enter a **Name** for the application group.

4. Enter a **Description** for the application group.

5. Either select single applications from the alphabetical list by clicking the box next to the application name or set up the group based on one of the criteria groups.

To select applications based on the criteria groups, select a criteria group. Select the appropriate criteria then verify in the list of applications that the appropriate applications have been selected. You can deselect any of the applications that have been automatically selected based on criteria.

**Note:** An application group function that has all transactions marked **is not** can still match traffic. This is possible when other sub-application criteria, which are included in the digital vaccine and are unrelated to transactions, match traffic. The Transaction field of any generated logs remains empty.

6. Click **OK**.

Keep in mind the following protocol when defining your search criteria:

- If your criteria has more than one entry specified, every application that matches any entry will be included. For example, if the entries “Social Media” and “Gaming” are both specified in the criteria, then all social networking applications and all game applications will match and be included in the profile.

- If multiple criteria are specified, applications must match each criteria type. For example, if you specify both the “Social Media” category and the “Post comment” transaction, all applications in the “Social Media” category that have “Post comment” transactions will match.

- For control filters at the sub-application or transaction level, enable only the subset of the application that matches the transaction criteria.

- The final selection of application groups reflects applications that match the positive criteria (includes) and with all applications that match the negative criteria (excludes) removed. If the positive criteria returns no matches, all applications that are not excluded by negative criteria will be considered by the profile.

**Manage firewall profiles**

When you first start managing a firewall device, the SMS does not have any information about the device profiles or rules for that device. If it is a new device, we recommend that you start managing it using rules and profiles in the SMS. If you have created or modified profiles on the firewall, you will need to import them into the SMS. You can use this profile as a base for other profiles that can be distributed to other devices.
Basic profile management tasks include creating, editing, and distributing profiles. Each profile contains a set of filters that you can modify with custom settings, including action sets, exceptions, and selected notification contacts. The SMS supports individual and multi-filter edits.

When you create a new profile, the system builds a profile based on the currently activated Digital Vaccine settings. You can then manage the profile and filters.

Firewall profiles allow you to manage groups of settings, such as NAT rules, captive portal settings, and firewall rules. They also include security and reputation inspection profiles. It is important to have inspection profiles configured before configuring firewall profiles or use the default inspection profiles to get started. You can edit them later as you update the inspection profiles.

**Note:** When you edit filters through the Events screen, the system accesses the last profile distributed to the device. The profile must be distributed to the device before those changes take effect.

### Table 73. Firewall profile management tasks

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Import</td>
<td>Imports the policy from a device and saves it as a new profile.</td>
</tr>
<tr>
<td>New</td>
<td>Creates a new profile.</td>
</tr>
<tr>
<td>Distribute</td>
<td>Distributes a profile or profiles to IPS devices in your network.</td>
</tr>
<tr>
<td>Delete</td>
<td>Removes a profile.</td>
</tr>
</tbody>
</table>

**Import a firewall profile**

1. Click **Devices** on the main menu, and then click **All Devices**.
2. Right-click a device in the Inventory pane, select **Edit**, and then click **Import Policy**.
3. Enter a unique name for the policy.
4. Click **Next**.

   The policy is added to the Firewall Profiles (<Profiles > Profiles > Firewall Profiles>).

**Create a new profile**

1. On the Profiles navigation pane, expand **Profiles**, and then click **Firewall Profiles**.
2. Click **New**.
3. Enter the following information for the profile:
a. **Name** — unique name for the profile.
b. **Description** — a brief description for the profile.

4. Select a security profile from the drop down menu to apply to unclassified traffic or create a new profile by clicking the ellipses button and following the steps in *Create a new profile* on page 138.

5. Select a reputation profile from the drop down menu to apply to unclassified traffic or create a new profile by clicking the ellipses button and following the steps in *Create a new profile* on page 138.

6. Click **OK**.

7. Configure Captive Portal, Firewall, and NAT rules as necessary:
   - See *Firewall rules* on page 242 for setting basic firewall rules.
   - See *Captive portal rules* on page 245 for information on setting captive portal rules.
   - See *NAT rules* on page 247 for information on setting NAT rules.

### Create a snapshot of a firewall profile version

Create a snapshot to save the current settings so that you can activate it at a later time.

1. On the Profiles navigation pane, expand **Profiles**, and then click **Firewall Profiles**.
2. Select a profile, and then click **Snapshot**.

   **Note:** If you delete a profile, you will lose all snapshots associated with the profile. Profile snapshots are saved as part of the profile data and will be deleted along with the other data.

   A snapshot of the current version of the profile is created.

3. Click the **Versions** tab.

   The new entry displays in the All Versions table.

### Activate a firewall profile version

1. On the Profiles navigation pane, expand **Profiles**, and then click **Firewall Profiles**.
2. Select a profile, click the **Versions** tab, and then select the profile version to activate.
3. Click **Activate**.

### Delete a firewall profile

**Important:** Deleting a profile will also delete all data relating to that profile, including all profile snapshots. However, any events that were generated will still be visible.

1. On the Profiles navigation pane, expand **Profiles**, and then click **Firewall Profiles**.
2. On Inventory pane, select a profile, and then click **Delete**.
Firewall rules

The Firewall Rules pane allows you to set inclusion and exclusion criteria based on security zones, IP addresses, services, schedules, applications and users. You can also specify what profiles are use to inspect any traffic that is permitted through the firewall.

The second section of the Create Firewall Rule (Setting) wizard includes Traffic Classifier sections where you will specify the criteria used to match network traffic. Each criteria can be matched as either an included or excluded value. You cannot have the same criteria specified twice in the same list and some classifiers have restrictions on the combinations of values that can be excluded and excluded.

Firewall rules are evaluated in the order indicated in Profiles > Firewall Profiles > Rule Name >Firewall Rules. Only the first matching rule is applied. To change the order of the rules, select the appropriate rule, then click Move Up or Move Down at the bottom of the pane.

Many of the criteria used in this section are created in the Shared Settings section of the Profiles view. The process of adding items is similar in all sections of the Profiles view.

Add items to firewall rules

The following steps explain how to add and remove items in a wizard or dialog box.

1. Click the + symbol to open the dialog.
2. Select the item from the list or search for the item by name.
3. Select whether to include or exclude the item.
4. Click OK.
5. Repeat until all of the items have been included or excluded. To remove items in the list, select the item and click the - symbol.
6. Context menus provide actions to quickly change selected items from “include” to “exclude” or vice versa.

Create firewall rules

1. On the Profiles navigation pane, expand Profiles, and then click Firewall Profiles.
2. Expand a firewall profile, and then click Firewall.
3. Click New to create a new firewall rule, or select an existing rule, and then click Edit.
4. On the General section:
   a. Enter a unique ID for the rule.
   b. Select Rule Enabled to inspect and evaluate traffic based on the rule. You may have rules for troubleshooting that you do not want normally enabled. It is in the list of rules but traffic will not be evaluated based on the rule. Other rules you will want to enable for regular use.
c. The Position field is a read-only field indicating the location of rule in the list of rules. You can change the order of the rules by moving the rules up and down on the Firewall Rules inventory screen.

5. On the Action and Inspection section you will specify the action taken when a rule matches network traffic and how traffic that is permitted through the firewall will be inspected by the inspection device. From the Action Set drop down menu, choose one of the following:

• Block — Stops all packets from this connection.
• Permit — Allows the traffic to flow with optional inspection by IPS.
• Trust — Always allow traffic to flow without further inspection by the firewall or IPS.
• Notify — An additional action that can be added to Block or Permit to generate an event when a rule matches network traffic.
• Trace — An additional action that can be added to Block or Permit to save the packets that were inspected to determine the rule matched.

When you choose one of the Permit actions, specify how the traffic should be inspected by the inspection device. Choose a security and/or reputation profile from the list of inspection profiles.

6. On the Install on Targets section, select which devices to include or exclude from the rule.

The device may be included in the profile distribution but if it is excluded here, the rule will not apply to the device. If you specify one or more devices to include, those devices must also be selected in the distribution dialog when you distribute the profile. See Add items to firewall rules on page 242.

7. On the Sources > Security Zone section, the source security zone is the security zone from which a packet originates.

Security zones are an aggregation of selected interfaces from one or more firewall devices. You may have several security zones included but a security zone may only be excluded when the only include criteria is “any”.

8. On the Sources > IP Addresses section, the source IP address is the value in the source address field of a packet’s header.

Source IP addresses could be host addresses, CIDRs, or ranges with both IPv4 and IPv6 supported. When adding IP addresses, do not overlap included IP addresses with other included IP addresses. It is the same with excluded IP addresses with no overlap allowed. Source IP addresses could be host addresses, CIDRs, or ranges with both IPv4 and IPv6 supported. When adding IP addresses, do not overlap included IP addresses with other included IP addresses. It is the same with excluded IP addresses with no overlap allowed.

9. On the Destinations > Security Zones section, the destination security zone is the one that includes the interface that the packet will leave the firewall.
Security zones are an aggregation of selected interfaces from one or more firewall devices. You may have several security zones included but a security zone may only be excluded when the only include criteria is “any”.

10. On the Destinations > IP Addresses section, the destination IP address is the value in the destination address field of a packet’s header. Destination IP addresses could be host addresses, CIDRs, or ranges with both IPv4 and IPv6 supported. When adding IP addresses, do not overlap included IP addresses with other included IP addresses. It is the same with excluded IP addresses with no overlap allowed.

11. On the Other Criteria > Services section, specify which services or service groups that will be matched against when examining the network packet headers. A service is a collection of one or more TCP/UDP ports, IP protocols, and ICMP types and codes. A service group is a collection of one or more services. Services may be included or excluded in any combination.

12. On the Other Criteria > Schedules section, select one or more schedules to specify when the rule will be evaluated. For example, you may want to block certain types of traffic in off hours to reserve bandwidth for faster backups.

13. On the Other Criteria > Users section, you will select the users to add to the rule criteria list. You can select individual users based on login names or user groups. Use the radio buttons to narrow the search results by authentication method:
   a. LDAP — This will show only LDAP users and groups that are currently used in one or more rules. Click the + symbol to browse for users on an LDAP server or to create a new LDAP user.
   b. RADIUS — This will show only RADIUS users that are already defined on a RADIUS server and currently used in one or more rules. Click the + symbol to create a new RADIUS user.
   c. Local — This will show only individual or group accounts that are already defined on one or more firewall device and are currently used in one or more rules. Click the + symbol to browse for users on firewall devices or to create a new local user.

   **Note:** Adding and deleting users to the rule will add and delete references to those accounts managed elsewhere. The actual user accounts are managed in an Active Directory, RADIUS, or LDAP server and not in SMS.

14. On the Other Criteria > Applications section, select applications or applications groups to include or exclude from the rule. An application group is a set of criteria that matches one or more applications in the Digital Vaccine. For example, you may want to include all messenger applications in a blocking rule. Selecting a messenger group gives you the advantage of not having to constantly keep adding new messenger applications. When new applications are developed that fit the category, they will automatically be added to the Digital Vaccine settings in the future. There are several constraints regarding applications as rule criteria.

   • Only a single application group may be specified. It must be evaluated as an include criteria.
   
   • If an application group is specified in the rule criteria list, no applications may be added to the same list.
   
   • Includes and excludes are specified in the definition of the application group itself.
• If individual applications are specified in the rule criteria list, application groups will not be available for selection. Additional individual applications may be selected and added to the rule criteria list.

• Individual applications are always added to the rule criteria list as includes criteria. They may be changed to excludes with the rule criteria list context menu item.

• Individual applications in the rule criteria list must all be includes or all be excludes.

15. Once you have entered all of the rule criteria, select Comments from the wizard’s navigation pane. Enter a general description for new rules. For revisions, you can enter comments on the revisions.

16. When you have completed configuring the rule, click **OK**.

## Captive portal rules

Captive portals allow administrators to restrict access to sections of the network until users are validated via password, LDAP, or other authentication method. Captive portals typically force a client to display an authentication page before accessing the internet in order to require users to accept an acceptable use policy before accessing the internet, provide payment, or to allow users access to only a subset of your network.

You can find captive portals at hotels where they will allow you to access your room bill or the hotel services but not access to the internet without either signing in with a special code or paying a fee. Some businesses with free Wi-Fi will use captive portals to require you to sign an acceptable use policy before allowing access to the internet.

**Note:** Click **Distribute** to distribute the entire profile to the devices.

## Create a captive portal rule

1. On the Profiles navigation pane, expand **Profiles**, and then click **Firewall Profiles**.
2. Expand the appropriate firewall profile, and then click **Captive Portal**.
3. Click **New** to create a new captive portal rule or select an existing rule, and then click **Edit**.

   The Create Captive Port Rule dialog opens.

4. On the General section, enter a unique ID and a description of the rule.
5. On the Install on Targets section, select which devices to include or exclude from the rule. The device may be included in the profile distribution but if it is excluded here, the rule will not apply to the device. If you specify one or more devices to include, those devices must also be selected in the distribution dialog when you distribute the profile. To select devices to include or exclude:
   a. Click the + symbol to open the Choose Install on Targets dialog.
   b. Select the device from the list or search for the device by name.
   c. Select whether to include the device or exclude the device.
   d. Click **OK**.
e. Repeat until all of the devices have been included or excluded. To remove devices in the list, select the device and click the - symbol.

6. On the Sources section, click the + symbol to add security zones or source IP addresses to be include or excluded from the rule.

**Note:** Security zones are defined in **Shared Settings > Security Zones.** Each device has an included security zone of this-device. It isn’t visible in the list of security zones but does appear as an option when choosing security zones when creating rules. The this-device zone applies to traffic that has a source or destination for that particular device itself, such as IPv6 neighbor traffic and DHCP requests. It is included by default in the any zone, but when the any zone is not in use, this-device must be specified if traffic is meant to communicate with the device.

7. On the Destinations section, click the + symbol to add destination IP addresses to be include or excluded from the rule.

8. Click **OK.**

**Special captive portal rules to allow blocked users to log out**

If a blocked user attempts to log into a captive portal, the user will not be permitted to perform any actions, including logging out. Create the following firewall rules to allow users to log out of the captive portal. On the device, you need to configure the users: allowuser and blockuser.

**Rule: allow_users**

- Action set: Permit + Notify
- Included users: allowuser

**Rule: port_logout**

- Action set: Permit + Notify
- Included services: TCP port 8443

**Rule: block_users**

- Action set: Block + Notify
- Included users: blockuser

**Rule: port_login**

- Action set: Permit + Notify
- Included services: TCP port 80
NAT rules

If your network uses Network Address Translation (NAT), you will need to configure Source and Destination NATs rules for the firewall.

Source NAT rules change the source address in the IP header of network packets by specifying the type of translation to perform and the criteria that determines which packets are translated.

Destination NAT rules change the destination address in the IP header of network packets with the option to change the destination ports by specifying the type of translation to perform and the criteria that determines which packets are translated.

Create source NAT rules

1. On the Profile navigation pane, expand Profiles, and then click Firewall Profiles.
2. Expand a firewall profile, and then click NAT.
3. Select the Source NAT tab, and then click New to create a new rule or select an existing rule and click Edit.

   The Create Source NAT Rule wizard opens.

4. On the General section, create a unique ID for the NAT rule and a description.
5. On the Translation section, specify the translation to perform on traffic that matches the settings in the lower section of the screen. Available options include:
   - IP Address of Egress Interface — When selected, packets that match the criteria specified will have their source address replaced by the address of the interface through which the packets leave the firewall.
   - Host IP Address — When selected, you will specify a single, fixed IP address in the field to use as the source address for all packets that match the criteria specified. The address must be a valid IPv4 address.
   - Addresses from Subnet or Range — When this options is selected, addresses from a specified pool of addresses are used in a round-robin fashion to replace the source IP address for packets that match the criteria specified. The value of this field may be a Classless Inter-Domain Routing (CIDR) or a range of IPv4 IP addresses.

6. On the Install on Targets section, select which devices to include or exclude from the rule. The device may be included in the profile distribution but if it is excluded here, the rule will not apply to the device. If you specify one or more devices to include, those devices must also be selected in the distribution dialog when you distribute the profile. To select devices to include or exclude, see Add items to firewall rules on page 242.
   a. Click the + symbol to open the Choose Install on Targets dialog.
   b. Select the device from the list or search for the device by name.
c. Select whether to include the device or exclude the device.

d. Click **OK**.

e. Repeat until all of the devices have been included or excluded. To remove devices in the list, select the device and click the - symbol.

7. On the Source IP Addresses section, specify the IPv4 IP addresses that will be in the source address field of a packet’s header. This may be host addresses, CIDRs, or ranges. You can include or exclude the addresses in various combinations but there can be no overlap between included addresses or excluded addresses. See *Add items to firewall rules* on page 242.

8. On the **Destinations > Security Zones** section, specify the security zone which contains the interface through which the packet will leave the firewall. Security zones are an aggregation of selected interfaces from one or more firewall devices. You may include several destination security zones but you can only exclude a security zone when the only include criteria is “any”. See *Add items to firewall rules* on page 242.

9. On the **Destinations > IP Addresses** section, specify the value for the destination address field in the packet’s header. The IP addresses may be IPv4 host addresses, CIDRs, or ranges. You can include or exclude the addresses in various combinations but there can be no overlap between included addresses or excluded addresses. See *Add items to firewall rules* on page 242.

10. When you have finished configuring the Source NAT Rule, click **OK**.

### Create destination NAT rules

1. On the Profiles navigation pane, expand **Profiles**, and then click **Firewall Profiles**.

2. Expand a firewall profile, and then click **NAT**.

3. Select the **Destination NAT** tab, and then click **New** to create a new rule or select an existing rule and click **Edit**. The Create Destination NAT Rule wizard opens.

4. On the General section, create a unique **ID** for the NAT rule and a **description**.

5. On the Translation section, specify the translation to perform on traffic that matches the settings in the lower section of the screen. Your options are:

   - **Host IP Address** — When selected, you will specify a single, fixed IP address in the field to use as the destination address for all packets that match the criteria specified. The address must be a valid IPv4 address.

   - **Addresses from Subnet or Range** — When this options is selected, addresses from a specified pool of addresses are used in a round-robin fashion to replace the destination IP address for packets that match the criteria specified. The value of this field may be a Classless Inter-Domain Routing (CIDR) or a range of IPv4 IP addresses.

   - **Enable Port Translation** — When this option is selected, the destination port values in the TCP/UDP header will be translated for packets that match the criteria specified.

   - **Protocol** — Select TCP to translate matching TCP packets or UDP to translate matching UDP packets.
• Original Port Start/End — Specify the lower and upper ends of the range of port values to translate.

• Translated Port Start/End — The start is the lower end of the range of port values to use when replacing port values in matching packets. The upper end is calculated for you to ensure the original port range and the translated port range are the same size. Port values are translated based on their position in the original and translated ranges (i.e. the first value in the original range is translated to the first value in the translated range for matching packets and the second value in the original range is translated to the second value in the translated range for matching packets). All port values must be in the range 0-65535 inclusive.

6. On the Install on Targets section, select which devices to include or exclude from the rule.

The device may be included in the profile distribution but if it is excluded here, the rule will not apply to the device. If you specify one or more devices to include, those devices must also be selected in the distribution dialog when you distribute the profile. To select devices to include or exclude, see Add items to firewall rules on page 242.

7. On the Sources > Security Zones section, specify the security zone which contains the interface through which the packet entered the firewall.

Security zones are an aggregation of selected interfaces from one or more firewall devices. You may include several destination security zones but you can only exclude a security zone when the only include criteria is “any”.

8. On the Sources > IP Addresses section, section the IPv4 IP addresses in the source address field of a packet’s header.

This may be host addresses, CIDRs, or ranges. You can include or exclude the addresses in various combinations but there can be no overlap between included addresses or excluded addresses.

9. On the Destinations > IP Addresses section, specify the value for the destination address field in the packet’s header.

The IP addresses may be IPv4 host addresses, CIDRs, or ranges. You can include or exclude the addresses in various combinations but there can be no overlap between included addresses or excluded addresses.

10. When you have finished configuring the Destination NAT Rule, click OK.

**Distribute firewall profiles**

You can distribute firewall and Inspection profiles to your firewall devices.

Distributing a firewall profile updates the filter settings for a device according to the profile being distributed.

**Distribute profiles to firewall devices**

1. On the Profiles navigation pane, expand Profiles, and then click Firewall Profiles.
2. Select a firewall profile, and then click **Distribute**.

3. Select either all devices or individual devices in the Target pane.

4. For a high priority distribution, select the **High Priority** check box. See *Distribute profiles* on page 142.

5. Click **OK**.

![Caution:](image)

When you enter a significant number of changes to filters within a profile, the period of time required for distributing the profile increases. If you unsuccessfully distribute profiles due to time-out, contact a TippingPoint technical support representative to assist in extending the time-out setting for your profile distribution needs.

**Cancel a distribution in progress**

1. On the Profiles navigation pane, expand **Profiles**, and then click **Inspection Profiles**.

2. Select a profile in the Distribution Progress pane.

3. To view distribution progress, click **Details**, or right-click and select **Details**.

4. Click **Stop Distribution**.

![Note:](image)

A profile distribution can only be cancelled before it enters the installing state. After a device begins installing the package, the distribution cannot be cancelled. If the cancel button is grayed out, the distribution cannot be cancelled.
Responder

Responder features provide security mitigation to block infected or malicious traffic, inform you of possible threats, and place the host into remediation. Responder policies monitor all traffic according to devices, and use filters to enact another layer of protection. Filters include action sets with options to automatically redirect users and halt trigger traffic flows.

The Responder options described in this chapter define how to create actions and policies that perform expanded Responder actions beyond filter action sets. Triggered policies can make an entry to the event log, send email notification regarding the issue, send an SNMP trap, and add entries to the Reputation Database. You can also create switch-level policies and integrate with system management tools. The SMS also provides manual actions for adding hosts to the Active Responder queue.

**Note:** When SuperUser or Admin User access or authority is specified, the user must have the respective SuperUser or Admin capabilities. For more information, see Authentication and authorization on page 542.

The Responder workspace provides a centralized environment for managing security response actions, policies, switches, and response history. To open the Responder workspace, click **Responder** on the SMS toolbar.

Before you begin

Responder controls involve the use of policies, action sets, and filters that identify and possibly react to security violations. As such, you must fully implement an action before it can take effect. To use Responder, you must first:

• Manage the device. See **Devices** on page 282.

• Define actions. See **Responder actions** on page 254.

• Create an Active Responder policy to control how to trigger a response by setting initiation and timeout rules, selecting specific IP addresses, configuring a threshold period, executing and prioritizing responder actions, and selecting a device, if the policy contains an IPS action. See **Policies** on page 262.

• Create a Profile Action Set to control the flow (permit, block, quarantine, rate limit, or trust) and to determine which notification types a filter hit will send (management console, SMS response, remote syslog, email, and SNMP) for the active responder policy. See Create or edit an action set on page 124.

• Select Profile Security and Application Filters to use that particular flow of traffic for the Action Set.

In addition to the overview listed above, the SMS client defines the full implementation requirements for each action to ensure that your Responder policies are set up securely. All implementation requirements are located on the Implementation screen on the Response Action wizard.
Limitations

To ensure your continued success, note the following limitations when using Active Responder:

- **Actions**: The SMS can support a maximum of 250 actions per minute.
- **Response History**: There must be less than 20,000 active responses at any given time. The SMS does not have a limit on the number of closed responses.

Responder configuration

Responder has a number of configurable settings. You can configure triggers for a response, set thresholds, supply the SMS with the URL where hosts that trigger responder policies can be redirected, control the criteria by which a host action is closed, and so on. When a response is triggered, the SMS uses an Active Responder policy to manage affected hosts and halted traffic streams. Each policy requires a set of actions and settings configured to respond to malicious traffic by using switches in the network topology.

Responder is a policy-based service that reacts to triggers and performs a set of actions. You configure and enable Responder policies in the SMS that determine how the service reacts and what actions it takes. A policy can be triggered in several ways: thresholding, manually, Web service, or escalation of an IPS Quarantine action. You can configure policies to include or exclude sets of IP addresses. A policy incorporates a dependency capability that allows actions in the list to execute conditionally, based on the success or failure of other actions.

You configure Responder by creating active responder policies, specifying or creating responder actions, configuring network equipment that will participate in the active responder system, and configuring server options. In general, you configure Active Responder on the following screens in the Responder workspace:

- **Actions**
- **Policies**
- **Network Devices**
- **RADIUSWeb**
- **IP Correlation**

Response action scripts

One way to customize actions is to use the SMS Active Responder script manager to import actions. The SMS Script Manager provides an easy way to import, export, and delete action and device scripts. The script manager saves scripts in XML format. The following scripts can be managed with the SMS: Active Responder Action Script and Active Responder Device Script.
Import an active responder action script

1. On the Responder navigation pane, click Actions.
2. On the Response Actions screen, click Import.

   The Choose File dialog displays.
3. Browse to and select a file. The file type defaults to Quarantine Action Package, which includes both XML and QDP file formats.
4. Click Save.

   **Note:** If a previous version of the script exists, a warning dialog indicates that this action will overwrite an existing script file. If there is a problem during the import process, an error dialog displays and the action script is not imported.

Export an active responder action script

1. On the Responder navigation pane, click Actions.

   The Save File dialog displays.
3. Navigate to where you want to save the script and select Quarantine Action Package for the File type.

   The Script Manager saves the script as an XML file.
4. Click Save.

Delete an active responder action script

1. On the Responder navigation pane, click Actions.
3. Click Delete.

Managing manual response policies

The SMS supports manually responding to hosts through the Active Response screen. When you manually respond to a host, the SMS enacts the Manual Response policy on the traffic flow.

When you edit and enhance a Manual Response, you do the following:

1. Add policy actions. See *Working with the Responder (Response History)* on page 277.
2. Edit the Manual Response policy. See *Edit the default response policy* on page 265.
3. After modifying the policy, you can begin to manually respond to hosts. You need the IP address and any information regarding the devices you may want to specifically act upon. See *Initiate a manual response* on page 266.

You can perform a manual response by right-clicking IP addresses in generated event lists through the Events screen. You can also use the **File > Create Manual Response** menu option through the Active Response screen. If you have manually responded to Hosts, they also display in the Response History screen.

**Managing responder through an external/third-party interface**

For information about using an external or third-party interface to manage Responder, see the *Active Response* area in the *TippingPoint SMS External Interface Guide* that is available from the TippingPoint Threat Management Center (TMC) at [https://tmc.tippingpoint.com](https://tmc.tippingpoint.com), or from the Documentation section of the SMS client Web page.

**Responder actions**

When host traffic triggers an Active Responder policy, the SMS performs the response actions associated with the response policy.

The SMS client provides nine pre-defined action types that you can use to create response actions for Active Responder policies; each is described in detail below. The SMS provides hidden default actions (IPS Quarantine and Switch Disconnect) that can be readily implemented in a response policy, and add flexibility to specific filters. You can also import scripts that define response actions. See *Response action scripts* on page 252.

**Important:** The SMS defines the full implementation requirements for each action to ensure that your Responder policies are set up securely. To review the specific requirements for a particular action, click **Implementation** on the Response Action wizard, if available.

**Notification actions**

The SMS enables you to specify a notification action that is enacted when a response policy is triggered. These notifications are initiated by the SMS when enabled in a policy that is enabled in an action set. You can implement one or more of these notification actions in a policy.

- **Syslog** — Sends an event to a syslog server when the response policy is triggered.
- **Email** — Sends an email to specified recipients when the policy is triggered.
- **Web** — Sends a Web request. Performs an HTTP GET on a URL.
- **SNMP Trap** — Enacts an SNMP Trap for the host traffic when the policy is triggered.
These notification actions apply to Active Responder policy notification, as opposed to IPS Profiles notifications settings that specify how SMS notification of filter events is handled.

**Reputation entry (blacklist) actions**

The SMS provides an action that automatically enters offending IP addresses into the Reputation Database. This action enables you to blacklist IP addresses identified by the Active Responder service. This action has the following characteristics:

- The Reputation Database entry will only be used by profiles that have a Reputation Filter defined with matching tag category values and has been distributed to one or more devices.

- You can specify tagged or untagged entries.

- Tag values you can assign are any tag category currently defined in the Reputation Database as well as user-defined tags created in the Add Tag Category editor. Note that any changes to the tag definitions in the database can invalidate an action.

- Entries can be aggregated and added to the database every 60 minutes (recommended).

- You can control the total number of entries that can be added to the database by this action.

- Tag categories defined in Reputation Entry actions can conflict with Reputation filters that match the tag categories and have defined exceptions that can pre-empt triggering of the Reputation Entry action.

Add this action to a policy and add the policy to an action set enabled for SMS Response.

**IPS Quarantine actions**

The SMS provides a hard-coded IPS Quarantine action. This action performs traffic management as well as reradiates Web requests to be block actions or redirected to a Web page detailing issues they may have regarding their system. You can also add accessible Web sites allowed to the host while blocking all other access, such as to a virus detection company or software update Web site.

The default IPS Quarantine action is set to block all traffic from hosts identified for quarantine, but you can modify these settings. For example, you may want to redirect suspect Web requests to a specified Web server. Incorporating this action in a policy with notification actions can provide an effective defense.

When the SMS has an IPS escalation policy with the IPS Quarantine action, it sends the unquarantine command to ALL managed devices, including the originator.

IPS Quarantine Response (Hidden) Action describes how the IPS behaves when the SMS adds an IP to its list of responded to IP addresses. You can edit this action to better meet the needs of your environment.

The IPS Quarantine action configured on an IPS device provides a first layer of defense. Using the SMS Quarantine response action provides greater flexibility in targeting quarantine behavior. Before you set up this action, you must configure a Profile action set for Active Responder. Create or edit an action set on page 124.
Switch actions

The SMS includes a default Switch Disconnect action that is designed to work with Active Responder policies that apply to switches. This action works dynamically based on IP correlation. You can edit the name for this action, but cannot make any other changes. Specific instructions are required to implement this action.

Other actions are also available that are designed to enact on switches or other network devices that have been defined in the Network Devices screen in Responder. Use these actions to effect remediation by directing targeted hosts to network devices or systems for remediation. The switch actions include the following:

- **Switch Disconnect** — Instructs the switch to momentarily disable the port, which causes the host to reauthenticate. On reauthentication, access is rejected by the RADIUS server. SMS also includes a default Switch Disconnect action that is designed to work with Active Responder policies that apply to switches and works dynamically based on IP correlation. You can edit the name for this action, but you cannot make any other changes.

- **NMS Trap** — Integration with a network management system (NMS) to use an NMS Trap for a response action. An NMS Trap action sends out an SNMP Trap to an NMS (Network Management System) as well as performing other Response actions. NMS-type programs include: 3Com Transcend, 3Com Enterprise Management Suite, 3Com Network Supervisor, OpenNMS, Unicenter, OpenView, SunNet Manager, Traffic Director, eHealth, VitalSuite, and nGenius. Most functions of NMS Trap will require access to switches and the associated IP correlation functions.

- **Move Quarantine Host onto a VLAN** — Moves a host triggered for a response action onto a VLAN.

Switch policies can use all of the other available action types including the default actions and other switch actions.

Creating or editing response actions

The SMS enables you to create actions based response action types (SMS-defined and imported actions). In addition, you can edit or delete an existing action.

Create or edit a response action

1. On the Responder navigation pane, click **Actions**.
2. On the Response Actions screen, do one of the following:
   - To create a new response action, click **New**.
   - To edit an existing response action, select a response from the Response Actions list, and then click **Edit**. The Response Action wizard opens.
3. On the Action Name and Type screen, provide the following information:
• Action Name — Specify or edit the name for the action. This should be a name that is meaningful in describing the purpose of the action.

• Action Type — Select a type from the Action Type drop-down list, if enabled.

Note: When you edit an existing action, you cannot modify the selected action type. Remember that you cannot edit a Switch Disconnect action; you can only change the name of this default action.

4. Click Next or select the next item from the wizard navigation menu and begin entering the values required for the action; each action type is described below.

5. (Optional) To test a connection, click Test.

6. (Optional) Read the Implementation instructions. The implementation instructions describe what is required to use the action.

7. Click Finish to create the new action, or click OK if editing an existing action.

Email response action

This action specifies recipients to which the SMS sends email notifications when a response is triggered.

Note: Before you set up an Email action, the system SMTP Server must be configured under the Admin > Server Properties > Network section of the SMS. The system reply-to and from fields will be used if none are configured in this Email action. For more information about the SMTP Server, see Server properties on page 590.

1. Review the Create or edit a response action on page 256.

2. Select Email from the Action Type drop-down list.

3. Click Email Settings (or click Next), and then do the following:
   a. From — Enter the email address where the notifying email originates (generally an SMS-specific email alias).
   b. Reply To — Enter the email address where replies are to be sent.
   c. To — Click the Add button, and then enter the email address or addresses where syslog email notices will be sent.
   d. To enter multiple email addresses, separate entries with a comma.
   e. User Text — Enter the email message in the field.

   Important: To implement this action, it must be listed in the Actions section of one or more Active Responder policies. See Policies on page 262.

Move quarantined host onto a VLAN response action

This action specifies the VLAN that should be used to quarantine suspect hosts.

1. Review the Create or edit a response action on page 256.

2. Select Move Quarantined Host onto a VLAN from the Action Type drop-down list.
3. Click **VLAN Name** (or click **Next**), and then do the following:
   a. **VLAN Name** — Specify the name of the VLAN. This should be a name that is meaningful in describing the network equipment that recognizes names. The actual interpretation of the name is configured on each device.
   b. **VLAN ID** — Numeric tag, assumed to be 802.1Q compatible, that has a max value of 4095.

**NMS trap response action**

This action specifies a network management system to use for quarantine enforcement at the switch-level.

1. Review the *Create or edit a response action* on page 256.
2. Select **NMS Trap** from the Action Type drop-down list.
3. Click **NMS Trap Destination and Settings** (or click **Next**), and then do the following:
   a. **NMS IP address** — Specify the IP address of the NMS system.
   b. **Destination Port** — Type a Destination Port (any value from 1-65535) or accept the default port (162).
4. Click **SNMP Settings** (or click **Next**), and then do the following:
   a. **SNMP Version** — Select the version of the SNMP agent to use for the traps (version 2 or 3).
   b. **Test OID** — Specifies the object identifier (OID) used for the trap.
   c. **Community-based Security Model** — If using SNMPv2, specify the community string (for example: “public”) to use when sending trap messages.
   d. **User-based Security Model** — If using SNMPv3, specify the user name and the authentication method and information required in your security model.
5. Click **Primary Action Settings** (or click **Next**), and then do the following:
   a. **Primary Action type** — Select RADIUS Reauthentication (default), VLAN isolation, or disable port to specify the action to be invoked.
   b. **NAM rule** — Specify the NAM rule if required by the NMS.
   c. **Active Directory Group** — Specify the active directory group to use for lookup.
   d. **Quarantine VLAN** — Specify the quarantine VLAN address.
   e. **Perform VLAN check** — Checks for VLAN preconditions before attempting this action.
   f. **Drop Port Link** — Drops the port link for 10 seconds if this action is successful. In some configurations, such as 802.1x with an XP client, this will cause a DHCP lease renewal.

**Note:** This is the criteria that will be used to enact the SMS response action or will be attempted first if secondary and final settings are configured for the action.

6. (Optional) Click **Secondary Action Settings** (or click **Next**) to specify the secondary action settings.
   These options are the same as those described for primary action settings.
7. (Optional) Click **Final Action Settings** (or click **Next**) to specify the final action to attempt should the first two actions fail.

The options are the same as those described for primary and secondary options.

**Important:** To implement this action, it must be added to the **Actions** section of an Active Responder policy that is added to an action set enabled for SMS Response.

**Reputation entry response action**

This action specifies an entry that will automatically be added to the Reputation database when targeted.

1. Review the **Create or edit a response action** on page 256.
2. Select **Reputation Entry** from the Action Type drop-down list.
3. Click **Reputation Entry** (or click **Next**), and then do the following:
   a. Aggregate Entry Creation – Select this check box to specify that reputation entry requests are to be aggregated and saved to the database every 60 minutes. To specify that the new reputation entries will be added immediately, clear this check box.
   b. Maximum Reputation Entries – Enter the maximum number (1-2000000) of reputation entries allowed to be created by this action based on the capacity of your Reputation database.
   c. Tag Values – Specify the tags and tag values that will apply to the reputation entries created by this action by selecting the check box of those tags you want to apply.
4. (Optional) Click **Add Tag Category** to add a tag category that you define for the entries. For information about adding tag categories, see **Reputation database** on page 210.

**SNMP trap response action**

This action enables you to use SNMP trap notification for Active Responder events. Sends an SNMP Trap to an SNMP agent (SNMP version 2 or 3).

1. Review the **Create or edit a response action** on page 256.
2. Select **SNMPTrap** from the Action Type drop-down list.
3. Click **Trap Destination** (or click **Next**), and then do the following:
   a. Specify the trap destination Host and Port settings.
   b. If you want the SMS to send a trap when the action is closed, select that option. Otherwise, clear the **Send trap on close** check box.
4. Click **SNMP Settings** (or click **Next**), and then do the following:
   a. **Note:** The fields in the Authentication group are only available for SNMP v3.
      a. SNMP Version — Version of SNMP to use when sending this trap.
b. Community — Group to which the destination host belongs. Value is only valid for SNMP v2.

c. Engine ID — Numeric ID that identifies this trap.

d. User Name — User login name to use for authentication. Defaults to private for a v3 trap. Value is only used for SNMP v3.

e. Authentication Protocol — Protocol to use for authentication. This value is only valid for SNMP v3.

f. Authentication Key — User login password to use for authentication. Value is only valid for SNMP v3.

g. Privacy Protocol — Protocol to use for data protection. Value is only valid for SNMP v3.

h. Privacy Key — Password to use for encrypting the trap. If no value is specified, the trap is not be encrypted. Value is only valid for SNMP v3.

**Important:** To implement this action, it must be added to the Actions section of an Active Responder policy that is added to an action set enabled for SMS Response.

### Syslog response action

This action enables you to specify a Syslog server where Active Responder will send events when a response is triggered.

**Note:** Before you set up a Syslog action, a UDP Syslog agent must be running on the Syslog destination IP and port configured for this action.

1. Review the Create or edit a response action on page 256.
2. Select Syslog from the Action Type drop-down list.
3. Click Syslog Settings (or click Next), and then do the following:
   - IP Address of Server (UDP) — IP address of the syslog server.
   - Port — Listening port on the syslog server (0-65535). The default setting is 514.
   - Facility — Choose the syslog facility that applies.

**Important:** To implement this action, it must be added to an Active Responder policy. See Policies on page 262.

### Web response action

Use this action to elicit a Web server response.

1. Review the Create or edit a response action on page 256.
2. Select Web from the Action Type drop-down list.
3. Click Host Configuration (or click Next), and enter the following information to specify the destination for the HTTP/HTTPS message:

**Note:** If a server is not specified, then the URL must be fully specified (for example, http://xyzzy.com/page).
IP Address of Server — IP address of the server running the HTTP/HTTPS service.

- Port — TCP port on which the service is listening.
- Protocol — protocol used for communicating with the server.
- URL — page to GET.

Host Authentication section

- For Host Authentication, select the **Use Authentication** check box.
- Select Authentication Type (Basic or Digest).
- Enter Username.
- Enter Password.

4. Click **Proxy Settings** (or click **Next**), and provide the following information, if using a proxy service for the Web server:

Proxy Host Settings section

- To use Proxy, select the **Use Proxy Host** check box.
- Enter the name or address of the Proxy Host.
- Enter **Proxy Port** number.

Host Authentication section

- For Host Authentication, select the **Use Authentication** check box.
- Enter the Username to use for login authentication on the proxy host.
- Enter Password.

**Important:** To implement this action, it must be listed in the **Actions** section of one or more Active Responder policies and added to an action set that is enabled for SMS Response. For more information, see **Policies** on page 262. An HTTP Server must be running on the HTTP destination IP and port configured for this action.

### IPS quarantine response action

This action is the SMS default response action for IPS Quarantine. You can edit this action to specify how traffic will be handled.

1. On the Responder navigation pane, click **Actions**.
2. On the Response Actions screen, select **IPS Quarantine** on the Response Actions table.
3. Click **Quarantine Settings**, and then do the following:
Web Requests — Select one of the following actions: Block, Redirect to a Web server (an address is required), or Display quarantine Web page.

Other Traffic — Select one of the following actions: Block or Permit.

To allow quarantined hosts to access specific sites, click Quarantine Exceptions, and then do one of the following:

- Click New to create a new listing.
- Select an existing listing, and then click Edit.

The Quarantined Access dialog opens.

On the Quarantined Access Dialog, do the following:

- Name — Specify or edit the name for the quarantined host. This should be a name that is meaningful in describing the purpose of the quarantined action.
- Destination — Type the IP Address in the field.
- Click OK.

**Important:** To implement this action, add it to a policy that specifies the values that trigger the response action.

### Delete a response action

1. On the Response Actions screen, select a response from the Response Actions list, and then click Delete.
2. In the Delete Action dialog, click Yes to confirm.

## Policies

An active responder policy defines the detection of a security event and the SMS response. Each policy may include the following:

- Segments from multiple managed devices
- One of each type of action you created
- IPS Quarantine action

The system provides a default response policy. This policy enacts when you manually respond to a host and the status is listed in the Response History table. For more information, see *Working with the Responder (Response History)* on page 277.

The method of configuring an active responder policy on an IPS segment is based on a response action set. You create an action set with the SMS action equal to the Active Responder policy and then assign filters with the action set. Then you can distribute to the IPS segments or segment group where you want to enforce SMS Active Responder.
Policy setup options

The following policy setup options are available when setting up or editing an active responder policy:

- **Policy initiation** on page 263
- **Policy remediation communication (timeout)** on page 263
- **Inclusions and exclusions** on page 183
- **IP correlation and thresholding** on page 264
- **Actions** on page 264
- **IPS destinations** on page 264

Policy initiation

An active responder policy controls the security response state of a host. A policy defines a number of actions that occur during a response. These actions can potentially interact with a variety of networking equipment, including an NMS and ingress switches, to enforce a response. A policy also handles reversing these actions when a response is closed. Active responder can be initiated by the following mechanisms:

- By correlating the event stream from a subset of managed IPS devices, and responding when threshold criteria are met.
- Manually, by choosing **File > Create Manual Response** and entering an IP address to be acted on.
- Via a Web service call from an external NMS (Network Management System).
- By escalating an IPS Quarantine – which is local to that IPS – to a potentially network-wide SMS response.

### Note: SMS Policies that escalate the IPS Quarantine should be limited to one SMS active responder policy.

If there is already a host in SMS active responder and that host shares the same identity with an incoming IPS Quarantine escalation, the SMS does NOT escalate the IPS Quarantine into a new response event.

Policy remediation communication (timeout)

The response typically is ended when response actions are complete or the suspect host has had time for remediation to complete. This act must be communicated to the SMS using the same set of mechanisms that are used to initiate a response manually, by an external NMS, or other means. Optionally, a timeout can be configured to automatically close a response when a certain amount of time has passed since the last response request for a given end-station.

Inclusions and exclusions

An Active Responder policy also contains a list of hosts/networks with the following classifications:
• Allow Active Responder — Specifies the IP address ranges and subnets that are to be eligible for Active Response.

• Never Respond — Specifies the IP address ranges and subnets that will never trigger a response.

Typically it makes sense to include IP addresses internal to your organization in the Allow List, with critical servers listed in the Never list.

**Note:** You can specify a multicast subnet or range in the inclusions and exclusions lists; however, you cannot specify a single multicast host.

**IP correlation and thresholding**

The SMS examines IPS alert logs from all managed IPS devices and correlates them using the attacker's IP address. Hit counts are qualified and accumulated within a sliding time window (the Threshold Period). A response is automatically initiated when the accumulated hit count exceeds a threshold. Qualified Filter Hits are simply IPS events that meet these criteria:

• The attacking IP addresses are eligible for a response per the Inclusions and Exclusions lists.

• The attack was seen on one of the selected IPS Segments.

• The Filter that matched is one of the selected IPS Filters for this Policy.

**Note:** The IPS Profiles installed on any selected segments must have NOTIFY turned on for the selected Filters in order for Alerts to be seen by the SMS.

**Actions**

When an end-station is acted on using this Policy, zero or more actions are executed to effect the response. The Policy itself lists configured actions, and incorporates a dependency capability that allows actions in the list to execute conditionally, based on the success or failure of earlier listed actions. For more information, see *Responder actions* on page 254.

**IPS destinations**

The SMS provides the option to distribute IPS actions to selected IPS devices. If an Active Responder policy contains an IPS action, you can select whether you want all the IPS devices or individual IPS devices to receive the Active Responder policy.

**Default response policy**

The default response policy is based on a special IPS action set. Every IPS contains this special hidden response action set and it is managed by the SMS Active Responder application. This action set describes how the IPS behaves when the SMS adds an IP to its list of targeted IP addresses. You can make changes to the default response policy or create a new IPS quarantine with additional configuration options. See *Edit the default response policy* on page 265 and *New response policies* on page 267.
Edit the default response policy

Use this task to modify the criteria defined in the policy and more finely-tune the default response.

1. On the Responder navigation pane, click Policies.

2. On the Policies screen, select the Default Response entry from the Active Responder Policies list, and then click Edit.

   The Active Response Policy wizard opens.

3. On the Initiation and Timeout screen, do the following:
   a. Specify the mechanism to use to initiate the policy. See Policy initiation on page 263.
   b. To set a timeout option, select Enable Automatic Timeout and enter a time in minutes, hours, or days.

   **Note:** Enabling automatic timeout automatically ends the continued application of Response Actions after the prescribed time limit even if remediation has not occurred.

4. Click Inclusions and Exclusions.

5. On the Inclusions and Exclusions screen, specify the hosts/networks to Allow Active Response or Never Respond.

   See Inclusions and exclusions on page 263. Click the arrow next to a field to add an existing Named Resource or to create a new Named Resource.

6. If it is enabled, select Correlation and Thresholding, and provide settings in the Automatic Response Configuration and Qualified Filter Hit Notifications sections.

   **Note:** The Correlation and Thresholding screen is available only if you select Enable Policy on the Initiation and Timeout screen.

7. Select Actions, and then provide the following:
   a. Priority — The order in which the actions are to be performed.
   b. Action — Name assigned to the action that you created. See Responder actions on page 254.
   c. Condition — Trigger for running the action. This option is set when a new action is added to the Response Policy and can be changed by editing a select action through this screen.
   d. Dependency — What other action must take place for this action to be triggered.

8. Click Add to add a Response Action, or select an existing action entry, and then click Edit.

   The Response Action dialog displays.

9. In the Response Action dialog, do the following:
   a. Select an Action from the drop-down menu, or click New to create a new Response Action.
   b. Select an option under Conditional Execution. The selections available in the Action drop-down menu are Response Actions from the Active Response (Actions) area.
When add an action, you can create dependencies by doing the following:

• In the Action drop-down, select an action to add.
• Under Conditional Execution, select either Only on success of or Only on failure of.
• In the drop-down list, select the action to connect for dependency.

For example, if you add an action called Email Admin with an action type of Email. You have an existing action called Switch Down (Switch Disconnect type). For Email Admin, if you specify Only on success of Switch Down, then when the switch goes down, the email action would send a message informing the network administrator.

10. On the Actions screen, review the listed actions. To change the priority of a selected action, use the up and down arrows to change the location of the selected action in the list.

11. In the IPS Destinations screen, select which devices will receive the Response Policy.

• To distribute to all IPS devices, select the All Devices check box.
• To distribute to selected IPS devices, expand the All Devices entry, and then select one or more IPS devices.

12. Click OK.

Manual response

You can manually respond to a targeted host by specifying the IP address of the host and the policy that you want to trigger for that host. When you Initiate a manual response on page 266, if the Response policy includes an IPS action, you can select one or more devices to which to apply the response.

Initiate a manual response

1. On the Responder workspace, click File, and then click Create Manual Response.

   The Create Manual Response dialog displays.

2. Enter an IP Address of a host for which to trigger a response.

3. Select a Policy Name from the drop-down list.

   The SMS enacts this policy against the targeted host.

4. (Optional) Select the Enable Automatic Timeout check box, and specify the number of minutes the system will enforce the policy action or actions.

   Setting this option automatically ends the application of Response actions after the prescribed time limit even if remediation has not occurred.

5. Select All devices or individual devices if the policy you want to apply contains an IPS action.

6. Click OK.
New response policies

New response policies provide more configuration options than the default response policy and allow you to finely tune your response. Responder supports multiple action sets that can be added to a response policy. See *Actions* on page 264.

You can initiate multiple IPS Quarantine actions from the SMS. For new response policies, you must set up a profile action set with IPS quarantine defined before you set up the response policy. See *Create or edit an action set* on page 124.

Create or edit a new response policy

1. On the Responder navigation pane, click **Policies**.
2. On the Active Response Policies screen, click **New**, or select an existing policy from the **Active Response Policies** list, and then click **Edit**.
3. In the **Active Response Policy** wizard, specify the following on the **Initiation and Timeout** screen:
   a. Specify a **Policy Name**.
   b. Specify the mechanism to use to initiate the policy. For more information, see *Policy initiation* on page 263.
   c. If you want to set the timeout option, select the **Enable Automatic Timeout** check box and enter the number of minutes, hours, or days. Setting this option automatically closes the response action for an end-station after the prescribed time limit even if remediation has not occurred.
   d. Click **Next**, or select **Inclusions and Exclusions** from the wizard navigation tree.
4. On the **Inclusions and Exclusions** screen, specify the hosts or networks to **Allow Active Response** or **Never Respond**.
   See *Inclusions and exclusions* on page 263. Click the arrow next to a field to add an existing **Named Resource** or to create a new **Named Resource**.
5. Click **Next**, or select **Correlation and Thresholding** from wizard navigation pane.
6. For Correlation and Thresholding, enter settings for the following:
   **Automatic Response Configuration**:
   - **Qualified filter hits** — The number of hits to enact the policy.
   - **Threshold period** — The period of time in seconds or minutes for the hit count threshold.
   - **Quiet period** — The Quiet Period begins when automatic response action is initiated. A new Threshold Period won't begin until the Quiet Period is over.
   **Qualified Filter Hit Notifications**:
   - Select **Send Syslog Notification** to send a message to the syslog. Enter a server and select a port and facility for the syslog.
• Select **Send SNMP Trap Notification** to send a message to the SNMP trap. Enter a destination and select a port.

7. Select **Actions** from the wizard navigation pane.

8. The **Actions** screen list the actions that are associated with the policy and the following information:
   - **Priority** — The order in which the actions are to be performed.
   - **Action** — Name assigned to the action that you created. See *Creating or editing response actions* on page 256.
   - **Condition** — Trigger for running the action. This option is set when a new action is added to the Active Responder policy and can be changed by editing a select action through this screen.
   - **Dependency** — What other action must take place for this action to be triggered.

9. In the **Actions** screen, click **Add** to add a new Response action or select an existing action entry, and then click **Edit**.

   **Note:** The SMS supports multiple IPS action sets. You must set up a Profile action set with IPS Quarantine defined before you set up an Active Responder policy. See *Create or edit an action set* on page 124.

   The Response Action screen displays.

10. Select an action to add from the drop down menu. You created these actions in the **Actions** screen for Active Response. When adding additional actions, you can create dependencies between the actions:
   a. Select an action to add.
   b. Select an option: success on or failure on.
   c. Select the action to connect for dependency.

   For example, the added action called Email Admin (email type) could have a dependency on the previously added action of Switch Down (switch disconnect type). In this situation, when the switch went down, the email action would send a message informing the network administrator.

11. Click **OK** to return to the setup wizard.

12. On the **Actions** screen, review the listed actions. If you want to change the priority of a selected action, use the up and down arrows to change the location of the selected action in the list.

13. Click **Next**.

14. In the **IPS Destinations** screen, you can select which devices will receive the Active Responder policy.

   • To send an IPS action to all devices with qualified hits, select **Send IPS Action only to the device which triggered the threshold**.

   • To send the IPS action to one or more devices, select the **Select Devices**, and then select one or more devices.
When you configure a IPS Quarantine action for a stack, propagate the policy to the stack so that any stack member that inspects the traffic can also quarantine the traffic when necessary.

15. On the Active Response Policy setup wizard, click **Finish** to save your settings.

**Delete a new response policy**

1. On the **Active Response (Responder)** navigation pane, click **Policies**.
2. In the **Active Response Policies** screen, select the policy you want to delete, and then click **Delete**.
3. In the Delete Policy dialog, click **Yes** to delete the policy.

**Responder network devices**

Responder supports a number of hardware infrastructure elements. These elements work off of one or both of two separate authentication methods, RADA and 802.1x.

**Note:** If there are network devices defined and the RADIUS proxy has not been enabled, Active Responder uses RFC 1493 (BRIDGE-MIB) to provide a MAC address to switch IP and port mapping. Device scripts that perform the actual switch actions must be developed separately.

The Network Devices screen in the Responder workspace enables you to add network devices that you want to configure for Responder, and lists the supported network device types.

**Auto discovery of switches**

The SMS can automatically discover network devices for use by IP/MAC Correlation and Responder. This feature discovers the network devices on your network and allows you to choose the devices you want to add. You can add a single device or multiple devices. Because the discovery process uses SNMP to discover the devices, SNMP must be enabled and a common authorization method must be used on the devices to be discovered. IP/MAC Correlation uses Layer 3 devices (routers) that support RFC 1213. Switch actions use Layer 2 devices (access switches) to disconnect access ports or change their VLAN.

**Note:** In order to initiate a switch level response, the SMS must know the MAC address of the target device and then match that to an IP address targeted for the Response action.

**Configure auto discovery of network devices**

**Note:** Before you begin, you must enable SNMP and make sure all devices share the same SNMP credentials.

1. On the Responder navigation pane, click **Network Devices**.
2. On the Network Devices screen, click **Discover**.
3. On the Discover Network Devices dialog, select options for the following:
   - Search Method — Select Subnet and enter an IP Range, or select Cisco Discovery Protocol and enter a router.
• SNMP — Enter a port number, select a version, and then click OK.

4. Select the device or devices to include, and then click Add.

5. On the Active Responder Options tab, select options for the following:
   RADIUS Options
   • Use RADIUS Authentication
   • Enforce switch actions using RADIUS
   • Prefer VLAN symbolic name over ID
   Device Usage
   • Use this device for IP to MAC Correlation
   • Use this device for Access Control

6. Click Next, or select SNMP Settings.

7. On the SNMP Settings tab, select the appropriate SNMP Settings:
   • Community-based Security Model
   • User-based Security Model

8. Click Next, or select Telnet Settings.

9. On the Telnet Settings tab under the User Authentication area, enter the administrative Username and Password for the selected access device(s).

10. On the Telnet Settings tab under the Connection Settings area, select the Session Timeout and the Telnet Port to be used for the connection.

11. Click Finish. The selected device(s) are added to the Network Devices table.

12. Click Finish to close.

Adding a switch

Some network architectures employ switches for managing and maintaining traffic. Typical equipment includes:

• Network ingress switches — Switches in your network to which quarantinable end-stations are directly connected.

• Edge routers — Those routers that are closest to quarantinable end-stations. Edge routers should have no other layer-three devices between them and end-stations, and should be able to see the true MAC address of end-stations.

The following device types are currently supported by Responder:

• 3Com4400, 5500, and 7750
• Cisco 2950 IOS, 6500 IOS
• Generic Cisco Switch
• Generic Router
• Generic Switch

Add or edit a switch

For information about supported device types, see Adding a switch on page 270.

1. On the Responder navigation pane, click Network Devices.
2. On the Network Devices screen, click New, or select an existing entry in the in the Network Devices list, and then click Edit.

   The Network Equipment wizard displays.
3. On the Device Address and Type screen, enter an IP Address for the switch and select a Switch Type from the drop-down menu.
4. Click SNMP Settings (or click Next), and then provide the SNMP Version and the SNMP Port for the device.
5. In the Community-based Security Model section, provide the appropriate values for Read Community and Write Community.
6. In the User-based Security Model area, provide the appropriate information in the following fields:
   • Engine ID
   • User Name
   • Authentication Protocol
   • Authentication Key
   • Privacy Protocol
   • Privacy Key

   Note: The 3Com 7750 and 3Com 5500 switches support RFC1213 IP Correlation. To use IP Correlation with these switches, be sure to select Use this device for IP to MAC Correlation (ARP, via RFC 1213) on the configuration screen for your particular 3Com switch.

7. If you want to test this action, click Test.
8. Click Next, or select Implementation in the wizard navigation pane.
9. Click Finish.
RADIUS

The SMS can be configured to use a RADIUS server for authentication. See Configure RADIUS authentication on page 545. Before you create policies and actions for switch devices, you must first configure the RADIUS server. After you configure RADIUS, you must then point the RADIUS authentication to the SMS Server IP address for Responder.

Configure RADIUS

1. On the Responder navigation pane, click RADIUS.
2. On the RADIUS Status screen, click Edit on the Local RADIUS Settings panel.
   - The Local RADIUS Setting dialog displays.
3. On the Local RADIUS Settings dialog, do the following:
   - a. Port — Type the authentication port.
   - b. Secret — Type the secret.
   - c. Confirm Secret — Re-type the secret.
   - d. Click OK.
4. On the Proxied RADIUS Servers panel, click Add.
   - The Add Proxied RADIUS Server dialog displays.
5. To change an existing entry, select it, and then click Edit.
6. In the Add Proxied RADIUS Server dialog, enter the host address, authentication port, and secret.
7. Confirm the secret, and then click OK.
8. To enable the local setting, click Enable on the Local RADIUS Settings panel.
9. Click Test to test the RADIUS configuration.

Note: After configuring RADIUS, you must point the RADIUS authentication to the SMS Server IP address.

IP Correlation

IP Correlation is the method by which the SMS looks up the IP addresses of hosts under inspection, learns the associated MAC address of an IP from a source, and then resolves which switch this MAC is connected to. The SMS can then engage switch actions to begin acting on hosts. This setup is required for Responder to work with non-IPS infrastructure equipment, such as switches and other network access points.

This section contains the following topics:

• Configuring IP Correlation on page 273
• *IP Correlation web services* on page 275

• *Testing IP Correlation* on page 276

**Configuring IP Correlation**

The IP Correlation Network Mapping Table is used to create a static map of IP address to MAC address one entry at a time. Mapping of the end-station to its IP address is a requirement for the Responder to properly control access on a host. When configured for IP Correlation, the SMS:

• Watches events from an IPS

• Finds the end-station responsible for those events

• Uses the information to initiate a response

The various IP Correlation configuration options that are available include:

• *Network mapping using the GUI* on page 273 (describes how to *Add/edit network mapping* on page 273)

• *Network mapping – bulk load via service mode* on page 274

• *IP Correlation configuration – RFC1213* on page 274

• *IP Correlation configuration – 3Com Network Director or 3Com Enterprise Management Suite* on page 274

• *IP Correlation configuration – external Web API* on page 274

**Network mapping using the GUI**

Network mapping for IP correlation is an essential part of implementing Responder switch actions. You can configure the IP correlation by using the *Add/edit network mapping* on page 273 entries to the mapping table in the *Active Response (Responder)* screen.

**Add/edit network mapping**

Use the GUI to add network mappings one entry at a time. For other IP correlation options, see *Configuring IP Correlation* on page 273.

1. On the Responder navigation pane, click **IP Correlation**.

2. On the IP Correlation Network Mapping area, click **New**, or select an existing entry in the list, and then click **Edit**.
   
   The IP Correlation dialog displays.

3. Specify the following information:
   
   • IP Address (in 0.0.0.0 format)
   
   • MAC Address (in 00:00:00:00:00:00:00 format)
Note: If you enter an existing MAC address, it will not validate.

4. Click OK.

Network mapping – bulk load via service mode

Network mapping using bulk load via service mode requires service mode access, a properly formatted static map file, and a twiddle command to force the file to load into the database.

IP Correlation configuration – RFC1213

RFC1213 Network Identification lookup is configured under the Active Response (Network Devices) screen. This requires Layer 3 SNMP-enabled devices.

3Com 7750 and 3Com 5500 switches have a setting under each switch configuration. To enable the setting, select the check box next to Use this device for IP to MAC Correlation (ARP, via RFC 1213).

When IP correlation is executed, the SMS uses SNMP to query each layer 3 device configured and attempts to locate the end-station for the IP of the target.

IP Correlation configuration – 3Com Network Director or 3Com Enterprise Management Suite

The SMS supports 3Com Network Director™ and 3Com Enterprise Management Suite™ to perform IP Correlation. To enable this mode, add a Web Service URL to the IP Correlation Web Services table.

3Com Network Director and 3Com Enterprise Management Suite use the following Web Service URL for this configuration:

http://<ip of 3ND or EMS instance>:8158/cgi-bin/IPCorrelation

3Com Network Director and 3Com Enterprise Management Suite give the SMS the ability to perform additional functions beyond IPS Quarantine and RADIUS reauthentication. See the documentation on the NMS Trap action type to review these features in detail.

IP Correlation configuration – external Web API

Advanced users can write a custom external IP Correlation engine with a Web-based (http) interface and a static (base URL) address. IP Correlation Web Services directs the SMS to that interface using a Web API. The URL for this API must point to the Web page interface (base URL) where you are hosting this lookup agent and must be entered into the IP Correlation Web Services table. HTTP(S) is used to provide Responder with network identity management.

IP Correlation query configuration

The SMS uses the HTTP header information to determine success or failure. The body of the response contains the results in name-value pair format. A successful response expects an HTTP 2 status code. Any other response is considered an error condition and causes the call to fail.
Each line on the response is in the following format: Attribute=Value

Example: MAC=00:00:02:fe:ed:ed

- **PCIP** — IP address of the end-station
- **PCMAC** — MAC address of the end-station
- **SWITCHIP** — IP address of the switch that the end-station is connected to
- **SWITCHPORT** — Port on the switch that the end-station is connected to

**Build IP Correlation queries over HTTP(S)**

The base URL is used to make HTTP GET requests to query the network.

**Table 74. Build IP Correlation parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol</td>
<td>HTTP</td>
</tr>
<tr>
<td>IP</td>
<td>10.100.230.111</td>
</tr>
<tr>
<td>CGI Script</td>
<td>cgi-bin/myNetLookup</td>
</tr>
</tbody>
</table>

The SMS can make two calls to the configured URL. Both calls are GETs.

http://<ip of 3ND or EMS instance>:8158/cgi-bin/IPCorrelation

OR

<configuredURL>?METHOD=MACLOOKUP&MAC=<macAddress>

Example:

http://10.100.000.111/cgi-bin/myNetLookup?METHOD=IPLOOKUP?IP=1.2.3.4

**IP Correlation web services**

From the IP Correlation screen, you can add new Web services, edit existing Web service entries, and control which order in the correlation each service is checked by adjusting the precedence of the Web service URLs. By default, the network mapping table is checked first, followed by each subsequent Web service URL in the IP Correlation Web Services table. The order of the entries is lowest value first.

You can perform the following tasks:
Add/edit web services

1. On the Responder navigation pane, click **IP Correlation**.
   The Active Response (IP Correlation) screen displays.
2. In the IP Correlation Web Services area, click **New**, or select an existing entry in the list, and then click **Edit**.
   The IP Correlation Web Services dialog displays.
3. Specify the Web Services URL. If you are using basic authentication, enter the Username and Password.
4. Click **OK**.

Control web service precedence

1. On the Responder navigation pane, click **IP Correlation**.
   The Active Response (IP Correlation) screen displays.
2. From the IP Correlation Web Services area, select the Web Service URL entry.
3. Use the Up and Down arrow buttons to move the entry up or down in the list.

Testing IP Correlation

From the IP Correlation screen, you can use an IP Address or a MAC address to test IP Correlation. The SMS attempts to use IP Correlation to display its IP, MAC, Switch IP, and Switchport. Switchport is an optional value reserved for future use. Other attributes can be returned (as documented in **IP Correlation configuration – external Web API** on page 274), but these attributes that the SMS uses are the requirements for Responder via an infrastructure action.

Perform a test of IP Correlation

1. On the Responder navigation pane, click **IP Correlation**.
2. On the Active Response (IP Correlation) screen, click **Test**.
   The IP Correlation Test dialog opens.
3. Select a Correlation Method: **IPLOOKUP** or **MACLOOKUP**.
4. Enter an address for the type of method selected: IP or MAC.
5. Click **Query**.
   The results of the query display in the results section.
6. Click Close.

**Working with the Responder (Response History)**

Use the Response History screen in the Responder workspace to:

- Filter and refresh active responses
- Close responses
- Drill in to event details for a host

Responder monitors traffic according to SMS Active Responder policies. When traffic matches a filter in an associated Active Responder policy, response actions are enacted against the host. The Response History table tracks response actions that have been taken.

The top portion of the Response History screen contains filters you can use to filter by policy, status, target address, and time range. The bottom portion of the Response History screen displays the Response History table, which displays the results of your filters. The number of results displays in parentheses. The following table describes the columns listed on the Response History table.

**Table 75. Responder**

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Unique identifier for the host.</td>
</tr>
<tr>
<td>Time</td>
<td>Date timestamp of the response.</td>
</tr>
<tr>
<td>Policy Name</td>
<td>Name of the Responder policy that triggered the response. If the device triggers the response, the SMS does not display the policy name.</td>
</tr>
</tbody>
</table>
| State          | • Active — Response action identified in the response policy is performed, and the host that triggered the policy is listed in the Response History table.  
                 | • Closed — Response action has been closed. This entry remains in the list until the database entries clear it or a year passes. |
| Source         | The SMS can identify the response source as either IPS or SMS and allow the response action to apply accordingly. The source field in the Response History list shows the source of the event that created the entry. |
### Column Description

- **SMS Response Source** — If the SMS initiates the response, the Active Responder policy is enforced.
- **IPS Response Source** — If an IPS initiates the response AND an IPS-to-SMS escalation policy exists, that policy is enforced.

**Note:** When you end a response action targeting a host in the SMS Response History table and this was acted on by an IPS, the IPS Unquarantine (IPS name for Responder) takes precedence and is performed.

The SMS response cessation does not end the Response activity period if:

- An Active Responder policy has Escalate enabled, but does not have IPS Quarantine selected as an action.
- The IPS initiates the response AND no escalation policy exists.

The escalation policy does not contain an IPS Quarantine action.

- **User** — A user-initiated action on an existing host, whether it is a manual response or a request to close an action.
- **IPS** — The IPS has initiated a change in status on the policy. This is observed when dealing with Active Responder policies that execute an IPS Quarantine action. The IPS has quarantined the host and put them into the listed status.
- **SMS** — The SMS has initiated a change in status on the policy.
- **Policy** — An SMS policy threshold violation has caused a response regarding the offending host. An expire of the trigger results in the host exiting the response condition.

See *Monitoring and managing responses* on page 279.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP</td>
<td>IP address of the host. This column is aggregated with the following information; click the plus (+) symbol to expand the column.</td>
</tr>
<tr>
<td></td>
<td>• Geo (Map) — Geographical map; click the link to display the map.</td>
</tr>
<tr>
<td></td>
<td>• Region — Identified region where the host is located.</td>
</tr>
<tr>
<td></td>
<td>• City — Identified city where the host is located.</td>
</tr>
<tr>
<td></td>
<td>• Named Rsr — Named resource.</td>
</tr>
<tr>
<td>MAC</td>
<td>MAC address of the host.</td>
</tr>
</tbody>
</table>
Monitoring and managing responses

Careful monitoring of the entries in the Response History list allows you to isolate and manage threats to your network. The Response History table enables you to monitor the status of systems in your network including any policies that are associated with those systems.

**Important:** If the IPS is rebooted, active memory including tables and quarantines, is cleared from the SMS.

Filter responses

1. On the navigation panel for the Responder workspace, click **Response History**. The Response History screen displays.
2. Click a policy on the Policies list.
   - Press either the **CTRL** or **SHIFT** key while you click a policy to select multiple policies.
3. Select a status: Active or Closed responses, or All.
4. (Optional) Select a target address on the Target Address(es) list.
   - Press either the **CTRL** or **SHIFT** key while you click an address to select multiple addresses.
   - To add a new IP addresses, enter an IP address in the field, and then click **Add**.
   - To remove an existing target address, select an address on the list, and then click **Remove**.
5. Select a time range from the following:
   - **Real Time**
   - Prescribed time interval (last minutes, hours, days, or month)
   - Start and End time range — Type in the field or click the calendar to select a date
6. Click **Refresh**.
   - The SMS refreshes and lists the responses in the Response History table.

Create a named resource

1. Select response filters, and then click **Refresh**.
   - The SMS refreshes and lists the responses in the Response History table.
2. Right-click an IP address line item in the table, select **Named Resource**, select **IP**, and then click an IP address.
   - The Create Named IP Address dialog displays.
3. On the Create Named IP Address dialog, do the following:
a. Name — Type a meaningful name in the field. Do not include spaces or special characters.
b. IP Address — Select an IP Host, IP Subnet, or an IP Range.

4. Click **OK**.

**Close a response**

1. Select response filters, and then click **Refresh**.
   
The SMS refreshes and lists the responses in the Response History table.

2. Right-click a host entry line item in the table, and then select **Close Response**.
   
   All actions in the policy are set to unquarantined.

**View events for a response**

1. Select response filters, and then click **Refresh**. The SMS refreshes and lists the responses in the Response History Search for a response.

2. On the Response History list, do one of the following:
   
a. Double-click a host entry in the list.
b. Select a host entry in the list, and then click **Details**.
c. Select a host entry in the list, expand Response History, and then click **Events** on the Responder navigation pane.

   Response History is linked to the Events for Host screen that enables you to monitor Response events for a specific host. In addition, this screen lists all events for a specific host, sorted in chronological order, the type of action that was enforced, and the associated details, as described in the following table.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time</td>
<td>Time the response occurred.</td>
</tr>
<tr>
<td>Type</td>
<td>Type of event that triggered the action.</td>
</tr>
<tr>
<td>Status</td>
<td>Current status.</td>
</tr>
<tr>
<td>Action</td>
<td>Action enforced in the response.</td>
</tr>
<tr>
<td>Source</td>
<td>Source that triggered the response.</td>
</tr>
<tr>
<td>Column</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>Description</td>
<td>Details that describe the event.</td>
</tr>
</tbody>
</table>
Devices

The Devices workspace provides a dynamic view of your entire system, graphically depicting TippingPoint devices currently under SMS management, their segments, and the hosts and services on those segments. Through this workspace, you can monitor and manage all the TippingPoint devices on your system.

Managing devices includes such activities as adding devices to your SMS system, combining devices into related groups, changing device or network configurations, installing TippingPoint operating system (TOS) updates, temporarily unmanaging a device, replacing a device, or deleting a device from your system.

When you assume management of a device, you can control networking configuration, virtual segments and segment groups, filters and customizations, and distribution of filters and software. You can also monitor traffic processing, health, and hardware status on each device and its segments.

Note: When SuperUser or Admin User access or authority is specified, the user must have the respective SuperUser or Admin capabilities. See Authentication and authorization on page 542.

The All Devices screen in the Devices workspace displays images that represent each TippingPoint device that has been added to the SMS, whether the device is currently managed or unmanaged. Each image displays the name of the device or component, status indicators, networking information, and other details.

Note: A device icon or shelf-level graphic that appears with red crossbars is not currently managed by the SMS. See Unmanaging or remanaging a device on page 330 for details.

To open the Devices workspace, click Devices on the SMS toolbar.

Devices (All Devices)

The All Devices screen provides a summary of each device that is being managed by the SMS. This screen enables you to add new devices, device groups, segment groups, or clusters to the SMS and import or export device configurations.

The top of this screen, beneath the SMS toolbar, contains a drop-down menu to adjust device view options and a shortcut menu that provides quick access to member summary screens. Select one of the following view options from the drop-down menu to change how devices are represented in the All Devices area. Changing the icon size applies the change to all device group views.

- **Large details** - System health, performance, and port health status indicators appear next to the device icon. The image also includes the device model, IP address, and system name.

- **Large** - System health, performance, and port health status indicators appear next to the device icon. The image also includes the device model, IP address, and system name.

- **Medium** - Device icon displays the same information as the large device icon, but smaller.

- **Small** - System name is displayed to the right of the device icon.
In the Devices view, unread notifications are indicated by a number icon that is displayed in the bottom-left of the icon. If the notification icon is gray with no number, there are no unacknowledged notifications for the device.

The shortcut menu, next to the view options menu, provides quick access to the following screens:

- **Members** - Member Summary, which shows configuration information for managed devices.
- **Network** - Network Summary, which lists physical segments and ports for managed devices.
- **Events** - Member Summary Events, which lists events such as firewall sessions; blocked, rate limited, and trusted streams; quarantined hosts; and adaptive filters.
- **Health** - Member Summary System Health, which displays memory, temperature, and file system information.
- **Performance** - Member Summary Performance, which displays packet statistics and CPU performance information.

The bottom portion of the screen displays a table with detailed information about the added devices. Double-click a row in the table to view the Device Details. The table details the following:

**Table 76. All Devices**

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the device.</td>
</tr>
<tr>
<td>IP</td>
<td>The IP address used to make a connection to the device.</td>
</tr>
<tr>
<td>Model</td>
<td>The device model.</td>
</tr>
<tr>
<td>System Health</td>
<td>The health status indicator that provides information about the hardware components of the managed device.</td>
</tr>
<tr>
<td>Performance</td>
<td>The performance status indicator that provides top-level information about the managed device.</td>
</tr>
<tr>
<td>Port Health</td>
<td>The port health monitoring indicator that tracks key port statistics for the managed device.</td>
</tr>
<tr>
<td>TOS</td>
<td>The software package version installed on the device.</td>
</tr>
<tr>
<td>Column</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>Digital Vaccine</td>
<td>Active Digital Vaccine (DV) version number.</td>
</tr>
</tbody>
</table>

**Member Summary**

For a top view of configuration settings for all managed devices, expand **All Devices**, and then select **Member Summary**.

The Member Summary screen lists the managed devices on the SMS and specific configuration information about those devices. Tabs on this screen correspond with **Device Configuration**:

- Management Information
- Management Routes
- Services
- High Availability
- Servers
- Remote Syslog Servers
- Time Settings
- TSE Settings

**Network Summary**

The **All Devices > Member Summary > Network Summary** screen provides a tabbed interface with top-level information about the following items for managed devices:

- Physical Segments
- Physical Ports
- Interfaces

To access the Network Summary listings, use the Devices navigation pane to navigate to the Network summary option for All Devices - Member Summary.

Additional network configuration information is available through the Network Configuration feature for a specific device, see *Network configuration and tasks – TPS and IPS (S-Series, N-Platform, and NX-Platform)* on page 285.

To edit segment and port properties, select the appropriate tab, select a device, and then click **Edit**. You can also access network configuration options by expanding the entries for a specific device from the left navigation pane and then selecting **Network Configuration** for that device.
To edit interface properties, select the Interfaces tab, select an interface, and then click **Edit**.

**Network configuration and tasks – TPS and IPS (S-Series, N-Platform, and NX-Platform)**

Through the SMS, you can view information about all of the segments on all of the IPS devices you are managing. You can view and configure the networking and traffic processing of those segments through the Device (Network Configuration) screen. To access this information, you expand the device entry in the Devices navigation pane and select **Network Configuration**.

The section has the following topics:

- **Segments tab – IPS (S-Series and N-Platform)** on page 286
- **Ports tab** on page 290

You can perform the following tasks:

- **Import IPS profile** on page 289
- **Events configuration – TPS and IPS (S-Series, N-Platform, NX-Platform)** on page 300
- **Delete a virtual segment** on page 341
- **Import IPS profile** on page 289

**I/O module replacement – TPS (TX Series)**

On a TPS TX Series device, **hot swapping** allows you to add, remove, or replace an I/O module without shutting down the device. When the device is turned on, you can hot swap an I/O module without interruption to the TPS device.

**Note:** Hot-swapping I/O modules during system initialization is not supported.

When you hot swap an I/O module, keep the following points in mind:

- The module port configuration is always reset.
- The module segment configuration, including link-down synchronization, Intrinsic HA, and inspection bypass, is always preserved.

When the device is turned off, **cold swapping** allows you to add, remove, or replace an I/O module as you would when you hot swap. However, when you cold swap an I/O module, if the replacement module type is the same, the module port configuration is preserved.
When the device is managed by the SMS, a delay of up to 1 minute can occur before the SMS recognizes the changed I/O module.

**Note:** When you insert a bypass I/O module, the bypass I/O module always starts up in bypass mode. A bypass I/O module remains in bypass mode until you remove it from bypass mode through the CLI, LSM, or SMS. Rebooting the TPS does not change the bypass mode of the bypass I/O module.

Segments tab – IPS (S-Series and N-Platform)

The Segments tab displays the following information in table format.

**Physical segments**

Segments are the portions of your network that you protect as discrete units. Traffic for one segment flows in and out of one port pair. By default, a filter applies to all segments that you are protecting. Physical segments set up a partition for traffic between two physical ports. This allows you to identify streams of traffic that flow between two defined physical ports.

Physical segments can be grouped together to form segment groups. You can apply a security profile (policy) to a physical segments and segment groups.

- **Name** — Segment name.
- **No.** — Segment number.
- **Direction** — Traffic direction for the segment.
- **Intrinsic Network HA** — Level of action for Intrinsic Network HA: Block All or Permit All.
- **Link-Down** — Mode, such as Hub, Breaker or Wire.
- **Port A, Port B** — Associated port for the segment.
- **Segment Group** — Membership in a segment group.
- **Profile Name** — Associated profile for the segment.

**Virtual segments**

Virtual segments define traffic using an endpoint pair, a VLAN ID, or both that are assigned to one or more physical segments.

See *Virtual segments* on page 416 and *Segment groups* on page 419.

- **Name** — Segment name.
- **Direction** — Traffic direction for the virtual segment.
- **VLAN(s)** — Virtual LAN.
- **Side A, Side B** — User-defined labels that are used to monitor traffic flow.
• **Physical Ports** — Associated physical ports for the virtual segment.

• **Segment Group** — Membership in a segment group.

• **Profile Name** — Associated profile for the virtual segment.

**Modules & Segment tab – TPS (TX Series) and IPS (NX-Platform)**

The Modules & Segments tab displays the following information about IPS NX-Platform and TPS TX Series devices:

• **Modules**
  - **Slot** — IO slot from 1 to 4 for IPS NX-Platform and TPS 8400TX devices. IO slot from 1 to 2 for TPS 8200TX devices
  - **Module** — Information about the module
  - **Serial No.** — Serial number of the module
  - **Status** — Active status of the module

• **Physical Segments**
  - **Name** — Segment name
  - **No.** — Segment number
  - **Direction** — Traffic direction for the segment
  - **Intrinsic Network HA** — Level of action for INHA: Block All or Permit All
  - **Link-Down** — Mode, such as Hub, Breaker or Wire
  - **Port A, Port B** — Associated port for the segment
  - **Segment Group** — Membership in a segment group
  - **Profile Name** — Associated profile for the segment
  - **sFlow®** — Sampled traffic on segment for analysis

• **Virtual Segment Assignments**
  - **Name** — Segment name
  - **Order** — Sequential order
  - **VLAN(s)** — Virtual LAN
  - **Src Addr/Dst Addr** — Source/destination IP address
  - **Segment Group** — Membership in a segment group
  - **Profile Name** — Associated profile for the virtual segment
From the **Segments** tab, you can:

- *Import IPS profile* on page 289
- Unassign physical segments from a virtual segment
- *Delete a virtual segment* on page 341

See *Network configuration and tasks – TPS and IPS (S-Series, N-Platform, and NX-Platform)* on page 285

**Note:** For SMS 3.0 managed devices using virtual segments, management and distribution is performed on a per-device level.

**Note:** Virtual segments are used with v. 2.5 and above devices. For v. 2.5 and above, physical segments can be used but cannot be created. Prior to v.2.5, IPS network configuration supported only IPS segments and ports. See *Network configuration and tasks – TPS and IPS (S-Series, N-Platform, and NX-Platform)* on page 285

**Link-Down Synchronization**

When editing a segment, you have the option to enable Link-Down Synchronization. Also called Sympathetic HA, this feature allows you to configure the device to force both ports down on a segment when the device detects a link state of down on one of the ports. When Link-Down Synchronization is enabled, the device monitors the link state for both ports on a segment. If the link goes down on either port, both ports on the segment are disabled. This functionality propagates the link state across the device.

In the case of Router A and Router B, if the link to router A goes down, then the ports both ports are disabled, resulting in the link to Router B going down, which Router B detects. With Link-Down Synchronization, ports respond according to the configured setting.

The settings include the following:

- **Hub** — When a port goes down, the system ensures the partner port remains up.
- **Breaker** — When a port goes down, the system disables the partner port until both ports are manually restarted. The breaker option requires manually restarting both ports.
- **Wire** — When a port goes down, the system disables the partner port, automatically restarting both ports when the link is re-established.

In addition to the ability to enable Link-Down Synchronization for each segment, you can change the amount of time after detecting a link is down before forcing both ports down on a segment. The default is one second. You can configure the setting to any number of seconds in the range of zero to 240.

After you enable Link-Down Synchronization for a segment, monitoring of that segment begins only after link up is detected on both ports. When Link-Down Synchronization disables the ports on a segment, two audit log messages are generated. The first message in the audit log corresponds to the port with the link down. The second message corresponds to the segment partner. Additionally, an error message is added to the system log indicating which port was detected with the link down, activating Link-Down Synchronization for that segment.
Edit TPS/IPS segment details

1. On the Devices screen, expand the All Devices in the navigation pane.
2. Select a TPS or IPS device, and then expand the options.
3. Select Network Configuration, and then select the Segments tab.
4. In the Physical Segments table, select an entry, and then click Edit.
5. Modify the Segment Name.
6. For Segment Group, select the appropriate group entry from the drop down box.
7. For Intrinsic Network HA, select a Layer-2 Fallback action:
   - Block All - All traffic is blocked while in Layer-2 Fallback.
   - Permit All -
8. For Link Down Synchronization, select a mode, and then enter a value in seconds for the Wait Time (0-240).
   - Hub (port goes down, partner port remains up).
   - Breaker (port goes down, partner taken down, both require manual restart).
   - Wire (port does down, partner taken down, automatically restart when link reestablished). When selected, if one interface is down for an amount of time exceeding the time-out period, both interfaces are managed according to the selected option.

Import IPS profile

1. From the navigation menu, expand the All Devices listing and select an IPS device by the device name. Open the tree of options for that device, and then select Network Configuration.
2. Select segment from the IPS Segments table, and then click Import IPS Profile.
3. The SMS imports the filters from the device into the SMS. The SMS names the profile using the segment name.
4. Click OK.

Note: As you import filters into an SMS Profile, the system migrates the filters into their new categories. The system assigns an action set of Recommended for all filters without customizations. If the filters have customized settings for action set, those settings are retained.

Note: You must distribute the profile from the SMS to the device prior to reviewing events or running reports. After importing the profile from the device, see Distribute profiles on page 142.

Edit a virtual segment

Edit a virtual segment to specify the traffic of interest.
1. On the Devices navigation pane, click **Virtual Segments**.

The Devices (Virtual Segments) screen displays.

2. To edit a virtual segment, select a virtual segment entry in the Virtual Segments table, and then click **Edit** to access the Virtual Segment wizard.

3. On the Name & Traffic Criteria screen, make any needed changes to the following description entries for the virtual segment.
   - **Name** — Must be unique among all existing virtual segments.
   - **Description** — Brief explanation about the virtual segment.

4. Make any needed changes to the following criteria you want to use to define the traffic for the virtual segment:
   - **VLAN** — Can be one or more comma-separated VLAN IDs or a Named Resource.
   - **Source IP Address** — Can be one or more comma-separated CIDRs or a Named Resource. Ranged-based Named Resources is not supported.
   - **Destination IP Address** — Can be one or more comma-separated CIDRs or a Named Resource. Ranged-based Named Resources is not supported.

5. Select **Physical Segments** from the left navigational menu to make changes to the physical segments.
   - Select one or more physical segments from the Physical Segments list that you want to assign to the virtual segment.

   **Note:** Physical segments tied to a TOS version 2.2 or earlier device which does not support virtual segments are disabled but displayed in the physical segment lists.

6. Select **Validation Report** from the left navigation menu to view the results of the validation check.
   - For complete report details, select an entry in the Validation Report table.
   - Click **Details**.

7. Click **OK** to preserve the new settings.

**Ports tab**

The Ports tab displays the following information:

- **Type** — Type of port, such as Management Port or Data Port.
- **Slot** — IO slot is numbered from 1 to 4 for IPS NX-Platform and TPS 8400TX devices. For TPS 8200TX devices, the IO slot is numbered from 1 to 2.
- **Port** — Port designation.
- **Segment** — Segment associated with the port.
- **Enabled** — enabled/disabled status.
- **Auto Negotiation** — check mark indicates the port auto-negotiates for line speed.
- **Configured** — Speed and duplex configuration.
- **Info** — Information on module (TPS TX Series and IPS NX-Platform devices only).
- **Negotiated** — Negotiated setting.
- **State** — Health status of the port.
- **Qualifiers** — Health status information.
- **Media** — Type of media for the port, such as copper or fiber.

**Note:** Fiber ports can only be set to 1000 Mbps line speed and full duplex. Although the port might negotiate different settings, you cannot arbitrarily downgrade line speed on a fiber Gigabit Ethernet port.

**Edit port details**

1. On the Devices screen, expand the **All Devices** in the navigation pane.
2. Select a device and expand the options.
3. Select **Network Configuration**, and then select the **Ports** tab.
4. Check the **IPS Segments** table to determine which port number is associated with Port A and which port number is associated with Port B.
5. From the **Ports** table, select the entry that corresponds to the Port entry in the **IPS Segments** table, and then click **Edit**. The Port Details - Edit dialog displays.
6. For **Hardware**, modify the **On** check box if the hardware is physically on or off.
7. For **Auto-Negotiation**, modify the **Enabled** check box if the port allows auto-negotiation for line speed.

    **Note:** If you use a copper-fiber translator (such as Netgear), you should leave Auto-Negotiation disabled. See the information at the end of these instructions.

8. If you are not using Auto Negotiation, modify the following settings:
   - **Line Speed**.
   - **Duplex** setting: **Full** or **Half**.
9. Click **OK**.
10. Repeat steps 5 through 9 for Port B.
Resolve out-of-service mode

If the SMS has errors and refuses to locate the device, check the connections on the device. If you use a copper-fiber translator (such as Netgear) and it is disconnected or loose, the device driver will attempt to re-initialize the port several times before timing out and placing the port in an Out-of-Service mode. Netgear does not support auto-negotiation. When you remove the copper cable or the cable is loose, Netgear does not attempt to auto-negotiate with the device.

1. From the Ports table on the Network configuration screen, select the entry that corresponds to the Port A entry in the IPS Segments table, and then click Edit.

   The Port Details - Edit dialog displays.

2. For Auto-Negotiation, clear the Enabled check box. This disables the option.

3. Click OK.

4. Repeat steps 1 through 4 for port B.

   Leave auto-negotiation disabled. The port should reset.

VLAN translation tab – TPS and IPS (N-Platform and NX-Platform)

Some TippingPoint security devices can translate VLAN IDs per segment. The translation occurs after the inspection so incoming VLANs are used for virtual segments.

VLAN translation is supported on the following TippingPoint security devices:

- N-Platform and NX-Platform IPS devices
- TPS devices (vTPS does not support VLAN translation)

Note: For VLAN Translation, STP is not supported on the links attached to the IPS.

The VLAN Translation tab displays the following information:

- **Slot** — IO slot is numbered from 1 to 4 for IPS NX-Platform and TPS 8400TX devices. For TPS 8200TX devices, the IO slot is numbered from 1 to 2.

- **Incoming Port** — port number of incoming traffic.

- **Incoming VLAN ID** — VLAN ID for incoming traffic.

- **Outgoing VLAN ID** — VLAN ID for outgoing traffic.

- **Auto reverse** — reverse mapping setting.

Create/edit VLAN translation

1. On the Devices screen, expand the All Devices in the navigation pane.

2. Select an IPS (N-Platform or NX-Platform) or TPS device (vTPS is not supported) and expand the options.
For a stack of devices, select the segment reference device (SRD). For more information about VLAN translation for a stack of devices, see Security policy configuration on page 526.

3. Select **Network Configuration**, and then select the **VLAN Translation** tab.

4. Perform one of the following tasks:
   - To edit a VLAN Translation, select an entry from the table, and then click **Edit**.
   - To create a new VLAN Translation, click **New**.

5. Enter the **Incoming VLAN ID** and **Outgoing VLAN ID** numbers from 1 to 4094.

6. In the Port Selection area select the appropriate settings for each segment (1 to 11).
   
   **Note:** For NX-Platform and TX Series devices, the segments are grouped by slots. The segment lists the slot number and the segment number.
   
   - **No mapping** — Do not use mapping for selected segment.
   - **A > B** — For traffic arriving on side A with the specified **Incoming VLAN ID**, the VLAN ID is set to the specified **Outgoing VLAN ID** prior leaving side B.
   - **A < B** — For traffic arriving on side B with the specified **Incoming VLAN ID**, the VLAN ID is set to the specified **Outgoing VLAN ID** prior leaving side A.
   - **Reverse mapping** — Automatically creates an inverse mapping. Changes the VLAN ID for traffic in the reverse direction from the Outgoing value to the Incoming value.

7. Click **OK**.

**NGFW network configuration and tasks**

For NGFW appliances, the Network Configuration screen displays relevant network information including a tabbed section that displays interfaces, segments, and port information.

**Interfaces tab (NGFW)**

Network interfaces are the network access points on the appliance and are defined as either physical or logical interfaces. NGFW provides full IPv4 and IPv6 support on the appliance and for all the interfaces. From a deployment perspective, a network interface on the NGFW Appliance is either a segment, bridge, or routing interface. Interfaces must be manually configured to belong to a segment, bridge, or router which determines the type of actions performed by the firewall and packet forwarding methods performed.

Interfaces include the following types:

- Aggregated Link (AggLink)
- Bridge
- Ethernet
The Ethernet interfaces are enabled by default, but can be disabled when needed, for administrative purposes. An Ethernet interface can be bound in a configuration of any of the following objects: Aggregated Link, Bridge, PPPoE, VLAN, Security Zone, and Source NAT rules.

For more information on NGFW interfaces, see the *TippingPoint Next Generation Firewall Local Security Manager User Guide*.

**Segments tab (NGFW)**

A network segment is created by joining an Ethernet pair of interfaces on the appliance such to allow traffic flow and inspection between the two network ports. Segments can be configured between vertical port pairs only. Network ports are stacked in pairs on the appliance. Segments are easily configured and are used in transparent, bump-in-the-wire, configurations. This type of transparent mode configuration can be useful for isolating a particular network segment to monitor and manage the IP traffic or for drop-in deployments. Segments are generally used if a transparent deployment with only two interfaces is required.

For more information on NGFW segments, see the *TippingPoint Next Generation Firewall Local Security Manager User Guide*.

**Ports tab (NGFW)**

The Ports screen displays the port numbers currently used by your network interfaces. You can set the port speed to auto-negotiate or manually set the port speed and duplex.

**Anti-Spoofing Filters tab (NGFW)**

The Anti-Spoofing Filters tab enables you to configure anti-spoofing/reverse path filters for each configured ethernet interface. Anti-spoofing ensures that packets are dropped if they have a source address that is not from the expected network. Anti-spoofing supports and is compatible with IPv4 and IPv6 addresses.

***Add an anti-spoofing filter***

1. On the Devices (Network Configuration) page, select the Anti-Spoofing Filters tab.
2. Click **New**.
3. Select an interface from the list.
4. Select one of the following options:
   - Include IPv4 addresses only – Enable anti-spoofing with IPv4 addresses.
• Include IPv6 addresses only – Enable anti-spoofing with IPv6 addresses.
• Include both IPv4 and IPv6 addresses – Enable anti-spoofing with IPv4 and IPv6 addresses.

5. Select **Log filter activity** to log the detected spoofed packets. When spoofed packets are detected by the firewall they can be tracked and logged.

6. Click **OK**.

For more information on Anti-Spoofing/Reverse Path Filters, see the *TippingPoint Next Generation Firewall Local Security Manager User Guide*.

**DNS/DHCP**

You can configure the NGFW Appliance to act as a DHCP server for appliances on its LAN-side interfaces that require IP address configuration. A DHCP server allows computers on your network to obtain an IP address and subnet mask automatically. DHCP assigns a temporary IP address and subnet mask to any PC that requires IP configuration information and reallocates that address when the PC disconnects from the network.

By default, DNS service uses the management interface. If you want to run it on a data interface you will need to use the management service.

On the DNS/DHCP screen, configure Dynamic Host Configuration Protocol (DHCP) support, scopes, relays, and servers. In the DNS Settings tab, you can edit the DNS server and proxy cache settings.

For more information on these services, refer to the *TippingPoint Next Generation Firewall Local Security Manager User Guide*.

**ARP/NDP**

The NGFW appliance supports address resolution protocol (ARP) and neighbor discovery protocol (NDP) for the address resolution on an interface. To handle IPv4 address resolution, ARP entries can be added to the ARP table and enabled for an interface. To handle IPv6 address resolution, static entries can be added to the NDP table and enabled for an interface.

On the ARP/NDP screen, configure the IP address, MAC address, and interface for ARP entries in the ARP Settings tab, and for NDP entries in the NDP Settings tab.

For more information on these services, see the *TippingPoint Next Generation Firewall Local Security Manager User Guide*.

**Events summary**

The **All Devices > Member Summary > Events** screen provides a top view of event information for all managed devices.

To access the Events listings, use the Devices navigation pane to navigate to the Events option for All Devices or the Events option for a specific device. See *View events for all devices* on page 333 and *View events for a specific device* on page 334.
For information on system details for an individual device, see *Device Details* on page 321.

**Blocked and rate limited streams**

The SMS provides a feature for displaying the blocked and rate limited streams of the connection table. To view, search, and flush the streams, click on one of the following tabs:

- **Blocked Streams** — Connections blocked by filters.
- **Rate Limited Streams** — Connections rate limited by filters.

Both tabbed screens display the 5-tuple for each stream, including the protocol, source IP address, destination IP address, source port, and destination port.

The tabbed screens include a **Connection Table Search Criteria** section for searching the blocked streams. The first table allows you to search the blocked streams. You can search by source or destination IP addresses and ports. The returned streams display in this table.

The streams display in the TSE Connection Table section of the screen. You can flush these connections from the connection table on this page. The **Flush All** option removes all blocked streams (including blocked streams not displayed) from the connection table. The effect is as though the blocked streams all timed out at the same time. You can also select blocked streams to be flushed. The **Flush Selected** option only removes the blocked streams selected from the list of displayed entries.

The **Blocked Streams** and **Rate Limited Streams** tabs provide the following information:

**Table 77. Blocked streams and Rate Limited streams**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device</td>
<td>Device name.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Protocol of the blocked or rate limited stream.</td>
</tr>
<tr>
<td>Src/Dest Address</td>
<td>Source IP address, destination IP address.</td>
</tr>
<tr>
<td>Port</td>
<td>Port address.</td>
</tr>
<tr>
<td>Slot</td>
<td>IO slot from 1 to 4 for IPS NX-Platform and TPS 8400TX devices. IO slot from 1 to 2 for TPS 8200TX devices.</td>
</tr>
<tr>
<td>Segment</td>
<td>IP address of the segment.</td>
</tr>
<tr>
<td><strong>Option</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>-----------------------------</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Source Interface</td>
<td>Specific source network interface (for NGFW only).</td>
</tr>
<tr>
<td>Destination Interface</td>
<td>Specific destination network interface (for NGFW only).</td>
</tr>
<tr>
<td>Profile</td>
<td>Name of the profile for the filter triggered.</td>
</tr>
<tr>
<td>Reason</td>
<td>Reason for the blocked stream.</td>
</tr>
</tbody>
</table>

Firewall sessions

The Firewall Sessions tab on the Events summary page displays the current firewall sessions running on the device. You can specify the properties by which to search, order, and flush sessions.

Trusted streams

The Trusted Streams tab is available for TPS TX Series devices, IPS (N/NX-Platform) devices, and NGFW appliances managed by the SMS. You can search the table and display results by:

- Protocol
- Source or Destination Address
- Port Number

The Trusted Streams table provides the following details:

**Table 78. Trusted streams**

<table>
<thead>
<tr>
<th><strong>Entry Title</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Device</td>
<td>Device name.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Protocol of the blocked or rate limited stream.</td>
</tr>
<tr>
<td>Src/Dest Address</td>
<td>Source or Destination IP address.</td>
</tr>
<tr>
<td><strong>Entry Title</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>----------------</td>
<td>----------------</td>
</tr>
<tr>
<td>Port</td>
<td>Port address.</td>
</tr>
<tr>
<td>Src/Dest Address</td>
<td>Source or Destination IP address.</td>
</tr>
<tr>
<td>Port</td>
<td>Port address.</td>
</tr>
<tr>
<td>Slot</td>
<td>IO slot from 1 to 4 IPS NX-Platform and TPS 8400TX devices. IO slot from 1 to 2 for TPS 8200TX devices.</td>
</tr>
<tr>
<td>Segment</td>
<td>IP address of the segment.</td>
</tr>
<tr>
<td>Source Interface</td>
<td>Specific source interface.</td>
</tr>
<tr>
<td>Destination Interface</td>
<td>Specific destination interface.</td>
</tr>
<tr>
<td>Profile</td>
<td>Name of the profile for the filter triggered.</td>
</tr>
<tr>
<td>Reason</td>
<td>Reason for the trusted stream.</td>
</tr>
</tbody>
</table>

**Tip:** If available, you can click the plus symbol (+) in the Src/Dest Address columns to display additional information, including Geography, Region, City, and Named Resource.

**Quarantined hosts**

The Quarantined Hosts tab enables you to unblock IP addresses quarantined by filters. The quarantine option for action sets blocks IP addresses that trigger associated filters. Through the Quarantined Hosts tab, you can search for a specific host IP Address and unquarantine individual hosts or all hosts.

When a filter with a quarantine action triggers, the system places a block on the IP address for a set amount of time unless manually flushed. Depending on the settings of the action set, the user might receive a message or be rerouted to a Web page detailing the reason for the blocked traffic.

The Quarantined tab provides the following information:
Table 79. Quarantined hosts

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device</td>
<td>Device name.</td>
</tr>
<tr>
<td>Host Address</td>
<td>Quarantined IP address.</td>
</tr>
<tr>
<td>Slot</td>
<td>I/O slot.</td>
</tr>
<tr>
<td>Segment</td>
<td>Segment the IP address is quarantined on.</td>
</tr>
<tr>
<td>Source Interface</td>
<td>Specific source network interface (for NGFW only).</td>
</tr>
<tr>
<td>Destination Interface</td>
<td>Specific destination network interface (for NGFW only).</td>
</tr>
<tr>
<td>Profile</td>
<td>Name of the profile for the filter triggered.</td>
</tr>
<tr>
<td>Filter</td>
<td>Name of the filter that triggered quarantine.</td>
</tr>
</tbody>
</table>

Adaptive filter

You can view a list of the 10 most recent filters managed by adaptive filtering.

The Adaptive Filter tab provides the following information:

Table 80. Adaptive filter

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Name</td>
<td>Device name.</td>
</tr>
<tr>
<td>Filter Type</td>
<td>Indicates whether the filter is a Security filter or Application filter.</td>
</tr>
<tr>
<td>Filter Name</td>
<td>Name of the filter that triggered.</td>
</tr>
</tbody>
</table>
### Filter State

Indicates the filters state:

- **Enabled** — Displays **Enabled** if the filter is enabled and running.
- **Disabled** — Displays an empty value if the filter is disabled. To enable, edit the filter.

### Events configuration – TPS and IPS (S-Series, N-Platform, NX-Platform)

Through the Events screen for an individual device, you can monitor system-specific information. The default displays data from the past 24 hours. Realtime data is available for most monitoring parameters. The data in the graphs can be printed or exported. To format, right-click on the graph.

**Note:** When first adding a device to the SMS, all of the graphs might not have 24-hours of data.

This section contains the following topics:

- *Event monitoring* on page 301
- *System health* on page 302
- *Performance* on page 305
- *Port health* on page 306
- *Traffic* on page 307
- *System log* on page 307
- *Audit log* on page 310

For additional information on monitoring your IPS device, see *Events summary* on page 295.

The Events screen for IPS devices provides a central location for viewing important information about the devices. From the main screen, you can access the following areas:

- *Blocked and rate limited streams* on page 296
- *Quarantined hosts* on page 298
- *Adaptive filter* on page 299

The Events screen for IPS (N-Platform or NX-Platform) and TPS devices provides a central location for viewing important information about the devices. From the main screen, you can access the following areas:

- *Blocked and rate limited streams* on page 296
- *Trusted streams* on page 297
Event monitoring

In the Devices (Events) area, you can perform the following tasks to help you monitor events:

- **View realtime graph data** on page 301
- **View log** on page 301
- **Reset events/logs** on page 301

**View realtime graph data**

1. On the Devices screen, expand the **All Devices** in the navigation pane.
2. Select a device and expand the options.
3. Expand the **Events** entry and then select the events area you want to view.
4. Click the **Realtime** button associated with the graph that displays the information you are tracking.
5. To copy a device graph data to the clipboard, right-click on the graph.

**View log**

1. On the Devices screen, expand the **All Devices** in the navigation pane.
2. Select a device and expand the options.
3. Expand the **Events** entry and then select a log option:
   - **Audit Log** — Displays the audit log. See **Audit log** on page 310.
   - **System Log** — Displays the system log. See **System log** on page 307
   
   The appropriate screen displays.
4. To view the current log, review the screen as it displayed. Click **Refresh** to update.
5. To view a span of log entries by date, do the following:
   a. Select a **Start Time**. Click the calendar icon and select the start and end times for the range.
   b. Select an **End Time**. Click the calendar icon and select the start and end times for the range.
   c. Click **Refresh**.

**Reset events/logs**

1. On the Devices screen, expand the **All Devices** in the navigation pane and select a device.
2. Do one of the following:
   - On the top menu bar, select the **Edit > Reset Device** menu item.
• Right-click and select **Edit > Reset Device**.

3. Select the log you want to reset. The **Reset Device > All Logs** option resets all logs except the audit log. To clear the audit log, you must specifically select the **Reset Device > Audit Log** menu option.

   **Note:** This option removes the system and audit logs from the IPS but does NOT remove these logs from the SMS.

System health

The system health monitoring for IPS devices tracks key health areas for managed devices and provides information in textual and graphical formats. Monitored statistics include temperature, memory, and HA state of the selected managed device. To display current values, click **Refresh**.

**Table 81. System health**

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
</table>
| Name   | The components of the system:  
  • CPU  
  • Disk/ramLog, Disk/ramRO, Disk/ramTmp  
  • Disk/system  
  • Disk/user  
  • Memory  
  • Temperature  

The following item also displays for IPS NX-Platform and TPS TX Series devices:  
  • Voltage  

The following items also display for IPS NX-Platform and TPS TX Series devices:  
  • CPU  
  • Fans  
  • Power Supply #1, Power Supply #2  
  • Voltage  

The following items also display for IPS 5000E:  
  • Disk/boot  
  • Disk/log
<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Disk/usr</td>
</tr>
<tr>
<td></td>
<td>• Disk/opt</td>
</tr>
<tr>
<td></td>
<td>The following item also displays for IPS 50:</td>
</tr>
<tr>
<td></td>
<td>• Disk/usb0</td>
</tr>
<tr>
<td>State</td>
<td>One of the following status indicators:</td>
</tr>
<tr>
<td></td>
<td>• Red square icon — critical</td>
</tr>
<tr>
<td></td>
<td>• Yellow square icon — major</td>
</tr>
<tr>
<td></td>
<td>• Green square icon — normal</td>
</tr>
<tr>
<td>Current Value</td>
<td>The percentage amount of the component used.</td>
</tr>
<tr>
<td>Details</td>
<td>The amount used of the total available megabytes (MB).</td>
</tr>
</tbody>
</table>

**Note:** For details about disk and memory usage, refer to the *TippingPoint Local Manager User Guide.*

**Note:** If you receive errors or have issues distributing profiles to devices due to exceeded limits of objects or filters, see *SMS error messages* on page 678.

See *System health summary* on page 311.

**Health stats**

The **Health Stats** section displays the following information about the managed system health:

**Health thresholds**

Health thresholds determine whether a current setting for disk, memory or temperatures shows a major or critical status. A major threshold must be lower than critical.

In the SMS, configure system health thresholds for IPS security devices. You cannot change the system health thresholds for TPS devices or NGFW appliances. The following table lists the default health threshold settings for the IPS.
Table 82. Default IPS system health thresholds

<table>
<thead>
<tr>
<th>Factor</th>
<th>Major Parameters</th>
<th>Critical Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Memory</td>
<td>( \geq 90% )</td>
<td>( \geq 95% )</td>
</tr>
<tr>
<td>Temperature (IPS)</td>
<td>( \geq 73^\circ \text{ C} )</td>
<td>( \geq 75^\circ \text{ C} )</td>
</tr>
<tr>
<td>Temperature (IPS N-Platform or NX-Platform)</td>
<td>( \geq 46^\circ \text{ C} )</td>
<td>( \geq 51^\circ \text{ C} )</td>
</tr>
<tr>
<td>File System space</td>
<td>( \geq 90% )</td>
<td>( \geq 95% )</td>
</tr>
</tbody>
</table>

To set health thresholds

1. On the Devices screen, expand the **All Devices** in the navigation pane.
2. Select a device and expand the options.
3. Expand the **Events** entry, and then select **System Health**.
4. In the Health Stats section, click **Settings**.
5. In the Devices - Health Thresholds dialog,
   - For **Storage**, enter a **Major** and **Critical** amount. The amount should be between 60% to 100%.
   - For **Memory**, enter a **Major** and **Critical** amount. The amount should be between 60% to 100%.
   - For **Temperature**, enter a **Major** and **Critical** amount. The amount should be between 40 to 80 Celsius.

System health graphs

The Health Graphs area displays graphs for the following items:
- **Temperature** — temperature (measured in degrees C) of the IPS
- **Memory** — how much memory the IPS is using
- **HA State** — is the IPS in an HA state

To display current values, click **Refresh**. To view Realtime data, click **Realtime**. See [View realtime graph data](#) on page 301.
Performance monitoring for IPS devices tracks key performance areas for managed devices and provides information in textual and graphical format. Monitored statistics include performance protection, packet status, and CPU for the selected managed device.

See Performance on page 312.

The Performance area provides Performance Data for monitoring and graphing IPS device packet statistics and information about tier statistics. The screen has the following tabbed views:

- Performance data on page 305
- Tier Statistics tab on page 306

Performance data

Monitored Performance data is displayed in textual and graphical formats. The Packet Stats Text section displays the following information:

Table 83. Performance data

<table>
<thead>
<tr>
<th>Entry Title</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device</td>
<td>Name of the device.</td>
</tr>
<tr>
<td>Total Packets</td>
<td>The total number of packets for the device.</td>
</tr>
<tr>
<td>Blocked</td>
<td>The number of blocked packets.</td>
</tr>
<tr>
<td>Permitted</td>
<td>The number of permitted packets.</td>
</tr>
<tr>
<td>Rate-Limited (IPS N-Platform and NX-Platform, TPS TX Series)</td>
<td>Number of rate-limited packets.</td>
</tr>
<tr>
<td>Trusted (IPS N-Platform and NX-Platform, TPS TX Series)</td>
<td>Number of trusted packets.</td>
</tr>
<tr>
<td>Dropped</td>
<td>The number of dropped packets.</td>
</tr>
</tbody>
</table>
Performance graphs

The Performance graphs area displays graphs for the following items:

- **Performance Protection** — Performance Protection activated in the IPS.
- **Packet Statistics** — Status of packets inspected by IPS.
- **CPU** — How much of the CPU capacity is in use.
- **Deep Packet Inspection (S-Series)** — The counts of packets that undergo greater inspection.
- **Tiers (Ratio to next tier)** — Represented in percent over time as a ratio to next tier.
- **Tier 1 Transmit and Receive Rates** — Represented as Mbps over time.
- **Tier 4 Reason** — Represented as percent over time.
- **Tier 1 Balance** — Represented as percent over time.
- **Tier 1 Bypass** — Represented as Mbps over time.

To display current values, click **Refresh**. To view Realtime data, click **Realtime**. See *View realtime graph data* on page 301.

Tier Statistics tab

The Tier Statistics tab provides information on packets and speed by tier. This area also displays Ratios and Utilization for A-side and B side traffic.

For more information about tier statistics for IPS NX-Platform and TPS TX Series devices, see *Tier statistics for the vTPS, TPS, and IPS (NX-Platform) devices* on page 409.

Port health

Port health monitoring for IPS devices tracks key port statistics for managed devices and provides information in textual and graphical formats. For IPS NX-Platform and TPS TX Series devices, the SMS displays the slot number in addition to the other port information.

Port statistics

The textual display provides data by segment and includes the following information:

- Total In/Out Byte
- Total In/Out Discards
- Total In/Out Errors

To display current values, click **Refresh**.

The graphical display tracks Input/Output by port and provides information about the following items:
• Media
• Line Speed
• Link Status
• Duplex Status

To display current values, click **Refresh**.

You can edit port information directly from the graph area of the Events - Port Health screen. To edit port details, click the **Edit** button associated with the graph that displays the port information you want to edit. See *Import IPS profile* on page 289.

**Traffic**

The **Traffic** section tracks and compiles information on all traffic managed by the device.

**Traffic graphs**

• **Frame Size** — Traffic profile by frame size, by specified byte ranges.

• **Frame Type** — The frame types of the packets flowing through the IPS.

• **Protocol** — Displays attack traffic categorized by protocol. Includes the number of filtered packets for each protocol and the percentage of total traffic the number represents. Protocols include: ICMP, UDP, TCP, and IP-Other.

• **Severity** — Displays the number of attacks categorized as Low, Minor, Major, and Critical. Also shows the percentage of total traffic for each severity level. The severity levels are assigned by the TippingPoint Digital Vaccine team and are included as part of the filter definition.

To display current values, click **Refresh**. To view Realtime data, click **Realtime**. See *View realtime graph data* on page 301 and *Device Traffic templates* on page 104.

**System log**

The system log contains information about the software processes that control TippingPoint devices including startup routines, run levels, and maintenance routines. System log entries can provide useful troubleshooting information if you encounter problems with your TippingPoint device.

The system log also includes event information regarding device health. If the status indicator for the device displays an error or issue, you can view the log to locate information on the health events. See *System health summary* on page 311.

The following table details the system log details:
Table 84. System log

<table>
<thead>
<tr>
<th>Heading</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>The ID of the alert in the log.</td>
</tr>
<tr>
<td>Message</td>
<td>The description of the alert.</td>
</tr>
<tr>
<td>Entry Time</td>
<td>The time of the alert added to the log.</td>
</tr>
<tr>
<td>Severity Level</td>
<td>The severity level of the alert in the log.</td>
</tr>
<tr>
<td>Component</td>
<td>The component affected by the alert or event, such as report, policy, and OAM.</td>
</tr>
</tbody>
</table>

You can do the following:

- *View log* on page 301 — Details how to view a log
- *Reset events/logs* on page 301 — Details how to reset logs

**Device health event entries**

Issues with the health of a device list as event entries in the system log. These health events detail information about the status of your device depending on triggered filters. These events provide information about the issues of a device or group of devices.

The following events might occur on a device, component, resource, or host:

Table 85. Device health event entries

<table>
<thead>
<tr>
<th>Event</th>
<th>Origin</th>
<th>Component</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add Device</td>
<td>SMS</td>
<td>device name</td>
<td><em>Component</em> has been discovered and configured.</td>
</tr>
<tr>
<td>Alert Status</td>
<td>SMS</td>
<td>device name</td>
<td>The alerts status of <em>component</em> has changed to <em>status</em>.</td>
</tr>
<tr>
<td>Block Status</td>
<td>SMS</td>
<td>device name</td>
<td>The block status of <em>component</em> has changed to <em>status</em>.</td>
</tr>
<tr>
<td>Event</td>
<td>Origin</td>
<td>Component</td>
<td>Definition</td>
</tr>
<tr>
<td>------------------</td>
<td>--------</td>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Cold Start</td>
<td>device</td>
<td>device name</td>
<td>Component has been rebooted.</td>
</tr>
<tr>
<td>Config Sync</td>
<td>SMS</td>
<td>device name</td>
<td>SMS management data has been synchronized with component.</td>
</tr>
<tr>
<td>Connection Down</td>
<td>SMS</td>
<td>device name</td>
<td>Component has stopped communicating with the SMS.</td>
</tr>
<tr>
<td>Connection Up</td>
<td>SMS</td>
<td>device name</td>
<td>Component is now communicating with the SMS.</td>
</tr>
<tr>
<td>Device Availability</td>
<td>device</td>
<td>device name</td>
<td>Component entered Fall Back state at \textit{time} or Component was available for service (not in the Fall Back state) at \textit{time}</td>
</tr>
<tr>
<td>Delete Device</td>
<td>SMS</td>
<td>device IP</td>
<td>Component has been deleted from the SMS.</td>
</tr>
<tr>
<td>Delete Host</td>
<td>SMS</td>
<td>device component</td>
<td>Component has had a host removed from the SMS.</td>
</tr>
<tr>
<td>Fall Back Status</td>
<td>SMS</td>
<td>device-name</td>
<td>Component is in Fall Back state or Component is available for service (not in the Fall Back state)</td>
</tr>
<tr>
<td>Hardware Health</td>
<td>device</td>
<td>device component type</td>
<td>Component is status.</td>
</tr>
<tr>
<td>Hardware Status</td>
<td>SMS</td>
<td>device component</td>
<td>The health status of component has changed to status.</td>
</tr>
<tr>
<td>Manage Device</td>
<td>SMS</td>
<td>device name</td>
<td>The SMS is now managing component.</td>
</tr>
<tr>
<td>Managed From Device</td>
<td>device</td>
<td>device name</td>
<td>Component is now managed by the SMS.</td>
</tr>
<tr>
<td>New Host</td>
<td>SMS</td>
<td>device component</td>
<td>Component has a new host found by the SMS.</td>
</tr>
</tbody>
</table>
### Event Management

<table>
<thead>
<tr>
<th>Event</th>
<th>Origin</th>
<th>Component</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resource Health</td>
<td>device</td>
<td>resource name</td>
<td>Resource-name has changed from pre-status to post-status.</td>
</tr>
<tr>
<td>Resource Status</td>
<td>SMS</td>
<td>device component</td>
<td>The resource status of component has changed to status.</td>
</tr>
<tr>
<td>Unmanage Device</td>
<td>SMS</td>
<td>device name</td>
<td>The SMS is no longer managing component.</td>
</tr>
<tr>
<td>Unmanaged From Device</td>
<td>device</td>
<td>device name</td>
<td>Component is no longer managed by the SMS.</td>
</tr>
<tr>
<td>Warm Start</td>
<td>device</td>
<td>device name</td>
<td>Component has been restarted.</td>
</tr>
</tbody>
</table>

### Audit log

The audit log keeps track of device user activity that might have security implications. This activity includes user attempts (successful and unsuccessful) to do the following:

- Change user information
- Change device configuration
- Gain access to controlled areas (including the audit log)
- Update system software and attack protection filter packages
- Change filter settings

**Note:** Only SuperUser level users can view, reset, and download the audit log.

### Table 86. Audit log

<table>
<thead>
<tr>
<th>Heading</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>The ID of the alert in the log.</td>
</tr>
<tr>
<td>Time</td>
<td>The time of the alert added to the log.</td>
</tr>
<tr>
<td><strong>Heading</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>------------</td>
<td>----------------</td>
</tr>
<tr>
<td>Access Level</td>
<td>The access level of user causing the alert. Can include SMS for the system, SuperUser, and so on.</td>
</tr>
<tr>
<td>Interface</td>
<td>The interface used that generated the alert or event: WEB or SYS.</td>
</tr>
<tr>
<td>IP Address</td>
<td>The IP address of the system that generated the alert or event.</td>
</tr>
<tr>
<td>Component</td>
<td>The component affected by the alert or event, such as report, policy, and OAM.</td>
</tr>
<tr>
<td>Result</td>
<td>The result of the event, such as PASS for successful.</td>
</tr>
<tr>
<td>User</td>
<td>The user account causing the alert.</td>
</tr>
<tr>
<td>Message</td>
<td>The description of the alert.</td>
</tr>
</tbody>
</table>

You can do the following:

- View log on page 301
- Reset events/logs on page 301

When you view the log, the user listed for the logged events might include SMS, LSM, and CLI. These entries are entered by those applications into the audit log, as a SuperUser level of access.

**NGFW events**

The Events screen provides a top view of event information for all managed NGFW appliances. See Events summary on page 295.

**System health summary**

The System Health screen provides information on the health of your system. Through the screen, you can view the following system health information for managed devices:

- Memory
- Temperature
- File Systems
Additional system health information is available through the Events feature for a specific device. For more information, see *Events configuration — TPS and IPS (S-Series, N-Platform, NX-Platform)* on page 300.

To open the System Health screen:

- Expand **All Devices > Member Summary** in the Devices navigation pane, and then select **System Health**.

  Health Status indicators provide information about the hardware components of a device. Select the appropriate tab to view the associated information.

**Note:** For IPS devices only, top-level indicators can be configured. For more information, see *Health thresholds* on page 303. You cannot reset health threshold preferences for TPS devices or NGFW appliances.

### Performance

The **All Devices > Member Summary > Performance** screen provides top-level information about managed devices and includes the following areas:

- **Packet Statistics** — The number and status of packets processed by the device since boot time.
- **CPU** — The state and performance value expressed as a percentage.

#### Packet statistics

The Packet statistics section displays the number of packets processed by the device since boot time in the terms displayed in the following table. You can click **Reset** to reset the counters and **Refresh** to display current values.

**Table 87. Packet statistics**

<table>
<thead>
<tr>
<th>Heading</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device</td>
<td>Name of the device.</td>
</tr>
<tr>
<td>Incoming</td>
<td>Number of Incoming packets.</td>
</tr>
<tr>
<td>Outgoing</td>
<td>Number of outgoing packets.</td>
</tr>
<tr>
<td>Blocked</td>
<td>Number of Blocked packets.</td>
</tr>
<tr>
<td>Permitted</td>
<td>Number of permitted packets.</td>
</tr>
</tbody>
</table>
### Table 88. Device User Accounts

<table>
<thead>
<tr>
<th>Table heading</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>Enabled or disabled state of the user account associated with the device.</td>
</tr>
<tr>
<td>Name</td>
<td>Unique identifier for the user account on the device.</td>
</tr>
<tr>
<td>Role</td>
<td>Access level assigned to the user.</td>
</tr>
<tr>
<td>Table heading</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Group</td>
<td>Group assigned to the user.</td>
</tr>
<tr>
<td>Password Expiration</td>
<td>Number of days until the password expires.</td>
</tr>
<tr>
<td>Auth Type</td>
<td>Indicates whether the user authenticates locally or remotely (through RADIUS or TACACS+).</td>
</tr>
<tr>
<td>Family</td>
<td>Displays the family name of the managed device, such as IPS, TPS, or NGFW.</td>
</tr>
<tr>
<td>Device</td>
<td>Unique name associated with the device.</td>
</tr>
</tbody>
</table>

The Device Users screen provides the following actions:

- **Copy** — Allows the user to select which devices receive a copy of the selected device users. This option is disabled when no users are selected or the user is not authorized to manage user accounts for devices. Use the following authentication guidelines when copying users:
  - Provide and confirm a password for users who require local authentication.
  - When you copy only users who use remote authentication, the New Password and Confirm Password fields are disabled. In addition, these users can only be copied to devices that support RADIUS or TACACS+ authentication. Devices that do not support RADIUS or TACACS+ are disabled in the device selector panel.
  - When you copy users who use local authentication mixed with users who authenticate remotely, only users who match the current authentication type configured for the device can be authenticated. For example, if the current authentication type is RADIUS, only RADIUS-authenticated users can be authenticated on the device. All devices are selectable and a password is required. The password is ignored for RADIUS and TACACS+ users that get copied to devices that support remote authentication servers. Attempts to copy RADIUS and TACACS+ users to a device that does not support these servers return a confirmation dialog, prompting you to confirm the action. If you decline, the operation is aborted. If you confirm the operation, the user is copied to the non-RADIUS device as a local user, and the password requirement applies.

- **Enable** — Enables a user account for a specified device.

**Note:** A device user might be in a disabled state due to too many failed login attempts or a failure on the part of the user to perform a required password update.

- **New/Edit** — Create or edit a user account for a specific device. Each device user consists of a User ID, password, the role performed by that device user, and the user’s authentication method. When creating a
new device user the User ID field must be unique for the device. The User ID cannot be edited. Use the following authentication guidelines when creating or editing users:

- If RADIUS or TACACS+ is selected as the authentication method for a new user, only devices that support those servers are selectable, and the New Password and Confirm Password fields are disabled. Only users who use local authentication require a password.

- When editing multiple users across multiple devices, the preselected authentication method matches the authentication method of all the users if they authenticate in the same way.

- When you edit users with a mix of authentication methods, a No Change authentication is preselected and an automatic password is generated. Changing the password will apply only to local users. Changing authentication from No Change to Local clears the automatic password and requires a new password. Changing authentication from No Change to RADIUS or TACACS+ impacts only devices that support those servers.

- **Delete** — Delete the specific device users. Multiple device users can be deleted at the same time.

- **Refresh** — Refresh all device user accounts.

**Note:** It's a best practice to refresh the device user accounts after you create or update a device user account.

### Traffic capture

Traffic capture allows permitted users to view and manage traffic capture files residing either on the SMS or on a managed device. A traffic capture file contains one or more packets captured by a device on a single segment or all segments. From the **Devices** menu, expand **All Devices** and select **Member Summary** to see all the captures from all the devices in a device group (select the **Show All Devices** check box to see all the device groups). Traffic capture files are saved in packet capture (PCAP) file format and support either an internal or external viewer.

#### Concurrent traffic capture

The SMS allows multiple captures to run concurrently. Traffic capture files are created by the device at the request of a user through SMS or LSM. After traffic captures are manually stopped, the traffic capture files move from the device to the SMS if they were created from the SMS or if the user wants to work with the file.

Packet capture summary information and management options can be accessed in the following areas:

- **All Devices** — **All Devices** > **Member Summary** > **Traffic Capture**

- **Device Groups** — **All Devices** > [device group] > **Member Summary** > **Traffic Capture**

- **Device** — **All Devices** > [device] > **Traffic Capture**

To display traffic captures for all devices, select the **Show All Devices** option on the Traffic Capture summary screen for **All Devices** or **Device Groups**.
The Traffic Capture screen provides the following tables:

- **Current Traffic Capture** — provides information about the current traffic capture and the following options:
  - **New** — Create a new traffic capture.
  - **Stop** — Stop all current traffic capture on the devices. A confirmation message is displayed.
  - **Refresh Statistics** — Refresh the current traffic capture statistics.

- **Existing Captures** — Provides a listing of existing captures and the following options:
  - **View** — View an existing traffic capture with a configured viewer.
  - **Export** — Export existing traffic capture.
  - **Transfer to SMS** — Transfer an existing traffic capture from the device to the SMS.
  - **Delete** — Delete an existing traffic capture.

### Table 89. Existing captures

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the new traffic capture file.</td>
<td>Current, Existing</td>
</tr>
<tr>
<td>Date</td>
<td>Date of the traffic capture.</td>
<td>Current, Existing</td>
</tr>
<tr>
<td>Slot</td>
<td>I/O slot (from 1 to 4 for NX and 8400TX devices, from 1 to 2 for 8200TX devices)</td>
<td>Current, Existing</td>
</tr>
<tr>
<td>Segment</td>
<td>Segment on which traffic is captured.</td>
<td>Current, Existing</td>
</tr>
<tr>
<td>File Size</td>
<td>Size of file from 1 to 10,000,000 bytes.</td>
<td>Current, Existing</td>
</tr>
<tr>
<td>Packets</td>
<td>Number of packets from 1 to 10,000 packets. For TPS devices, this value will always be N/A.</td>
<td>Current</td>
</tr>
<tr>
<td>Device</td>
<td>Name of the device.</td>
<td>Current, Existing</td>
</tr>
<tr>
<td>Column</td>
<td>Description</td>
<td>Type</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------</td>
</tr>
<tr>
<td>On Device</td>
<td>File status on the device. A check mark indicates the traffic capture file is present on the device.</td>
<td>Existing</td>
</tr>
</tbody>
</table>

**Note:** Traffic capture files on the SMS are placed in the backup restore area of the SMS drive. Traffic captures placed on an SMS are not sent to the secondary HA system.

Traffic capture expressions (based on TCDump) are used in traffic captures to refine the types of packets that are captured. The following table outlines the use of traffic capture expressions:

**Table 90. Traffic capture expressions**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip</td>
<td>IPv4 traffic. By default, only IPv4 traffic is captured.</td>
</tr>
<tr>
<td>ipv6</td>
<td>IPv6 traffic.</td>
</tr>
<tr>
<td>proto</td>
<td>Designates the protocol of captured traffic. Can be an explicit number or tcp, udp, or icmp.</td>
</tr>
<tr>
<td>src</td>
<td>Specifies the source of the traffic. This parameter can be applied to both host and port.</td>
</tr>
<tr>
<td>dst</td>
<td>Specifies the destination of the traffic. This parameter can be applied to both host and port.</td>
</tr>
<tr>
<td>host</td>
<td>Designates a host IP address. IPv4 and IPv6 addresses are supported, as is CIDR format.</td>
</tr>
<tr>
<td>port</td>
<td>Designates the port; you must also specify a port number.</td>
</tr>
</tbody>
</table>

**Examples:**

| host 172.31.255.254 | Captures all traffic to and from 172.31.255.254. |
### Parameter Table

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>src 172.31.255.254</td>
<td>Captures all traffic from 172.31.255.254.</td>
</tr>
<tr>
<td>dst 172.31.255.254</td>
<td>Captures all traffic to 172.31.255.254.</td>
</tr>
<tr>
<td>src 172.31.255.254 &amp; dst 10.10.10.10</td>
<td>Captures all traffic from 172.31.255.254 to 10.10.10.10.</td>
</tr>
<tr>
<td>ip proto tcp</td>
<td>Captures only TCP traffic.</td>
</tr>
<tr>
<td>ip proto tcp &amp; src port 63</td>
<td>Captures only TCP traffic on port 63.</td>
</tr>
</tbody>
</table>

**Note:** You can use the ampersand (&) operator to concatenate parameters. Do not use the “or” operator.

### Traffic Capture Configuration

Traffic capture enables permitted users to view and manage traffic capture files residing either on the SMS or on a managed device. A traffic capture file contains one or more packets captured by a device on a single segment or all segments. Users can see the files for only one device at a time. Traffic capture files are saved in PCAP format and support either an internal or external viewer.

The Traffic Capture screen for a device provides the following tables:

- **Current Traffic Capture** — Provides information about the current traffic capture and the following options:
  - **New** — Create a new traffic capture.
  - **Stop / Stop All** — Stop current traffic capture. For TPS devices, to stop one traffic capture you have to stop them all using the **Stop All** button.
  - **Refresh** — Manually refresh the current traffic capture statistics

- **Existing Captures** — Provides a listing of existing captures and the following options:
  - **View** — View an existing traffic capture with a configured viewer
  - **Export** — Export existing traffic capture
  - **Transfer to SMS** — Transfer an existing traffic capture from the device to the SMS
  - **Delete** — Delete an existing traffic capture
- **Refresh**—Manually refresh the existing traffic capture statistics

### Table 91. Current Captures table

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the new traffic capture file.</td>
</tr>
<tr>
<td>Date</td>
<td>Date of the traffic capture.</td>
</tr>
<tr>
<td>Slot</td>
<td>I/O slot (from 1 to 4 for IPS NX-Platform and TPS 8400TX devices, from 1 to 2 for TPS 8200TX devices).</td>
</tr>
<tr>
<td>Segment/</td>
<td>The segment on which traffic is captured.</td>
</tr>
<tr>
<td>Interface</td>
<td></td>
</tr>
<tr>
<td>File Size</td>
<td>Size of file from 1 to 10,000,000 bytes.</td>
</tr>
<tr>
<td>Packets</td>
<td>Number of packets from 1 to 10,000 packets. For TPS devices, this column is not applicable and does not display by default. You can display it if you right-click on the table and select the column in the Table Properties. However, the values in this column will always be N/A for TPS devices.</td>
</tr>
</tbody>
</table>

### Table 92. Existing Captures table

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the new traffic capture file.</td>
</tr>
<tr>
<td>Date</td>
<td>Date of the traffic capture.</td>
</tr>
<tr>
<td>Slot</td>
<td>I/O slot (from 1 to 4 for IPS NX-Platform and TPS 8400TX devices, from 1 to 2 for TPS 8200TX devices).</td>
</tr>
<tr>
<td>Segment/</td>
<td>Segment on which traffic is captured.</td>
</tr>
<tr>
<td>Interface</td>
<td></td>
</tr>
</tbody>
</table>
### Column Description

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>File Size</td>
<td>Size of file from 1 to 10,000,000 bytes.</td>
</tr>
<tr>
<td>On Device</td>
<td>File status on the device; a check mark indicates the traffic capture file is present on the device.</td>
</tr>
</tbody>
</table>

**Note:** Traffic capture files on the SMS are placed in the backup restore area of the SMS drive. Traffic captures placed on an SMS are not sent to the secondary HA system.

#### Traffic capture expressions

Traffic capture expressions are used to narrow down the types of traffic that are captured. This feature supports true tcpdump expressions. For more information about expression usage, refer to external tcpdump and libpcap documentation.

To capture only TCP traffic enter the following expression in the **Expression** field:

```
tcp
```

The following example captures IPv4 HTTP packets that are transmitting to and from port 80 and only includes packets that contain data. SYN, FIN, and ACK packets are excluded.

```
tcp port 80 and (((ip[2:2] - ((ip[0]&&0xf)<<2)) - ((tcp[12]&&0xf0)>>2)) != 0)
```

#### Create a new traffic capture file

1. Select **Devices > All Devices**, and select a device.
2. From the navigational pane expand the options for the device and then select **Traffic Capture**.
3. In the Current Traffic Capture area, click **New** to create a new traffic capture.
4. In the New Traffic Capture dialog, specify the following information:
   - **Name** — Name of the new traffic capture file.
   - **Segment** — Segment on which traffic is captured.
     - **Note:** The IPS (NX Series) and TPS (TX Series) device segments indicate slot number and segment number.
   - **Maximum Packets** — Maximum number of packets of the capture file (from 1 to 10,000 packets).
   - **Maximum File Size** — maximum size of the capture file (from 1 to 10,000,000 bytes).
   - **TCPDump Expression** — Expression based on standard TCPDump parameters that refines the types of packets that are captured.
**Note:** When you want to capture MAC-in-MAC (IEEE 802.1ah) traffic, keep the following points in mind:

- Device support for MAC-in-MAC is limited to the TPS TX Series (8200TX and 8400TX).
- You can verify the device recognizes MAC-in-MAC traffic by running the `debug np stats show npParseStatsInst` CLI command on the device or by taking a packet capture. When you configure the packet capture, specify a TCPDump expression that identifies the Backbone MAC address (B-MAC) or Backbone VLAN identifier (B-VID) of the traffic you want, or capture all packets for particular segment.

5. Click **OK**.

**Export a traffic capture file**

1. Navigate to the **Devices > All Devices** area, select a device.
2. From the navigational pane expand the options for the device, and then select **Traffic Capture**.
3. In the **Existing Captures** table, select a listing, and then click **Export**.
4. In the **Save File** dialog box, navigate to the desired location, specify a name for the file, and then click **Save**.

**Transfer traffic capture files to the SMS**

1. Navigate to the **Devices > All Devices** area, select a device.
2. From the navigational pane expand the options for the device and then select **Traffic Capture**.
3. In the **Existing Captures** table, select a listing that has a capture file on the IPS device (indicated with a check mark in the **On Device** column).
4. Click **Transfer to SMS**.

**Device Details**

The Device Details screen provides a consolidated view of information and configuration settings for an individual device. To view the Device Details screen, do one of the following:

- From the **All Devices** screen, double-click a device entry.
- From the navigation pane, expand **All Devices**, and then select a specific device from the list.

The top portion of the screen displays a shelf-level image of the managed device and a System Health & Performance chart. The bottom portion of the screen displays a table with detailed information about the managed device, such as the hardware serial number and software versions. The table details the following:
Table 93. Device details

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Component</td>
<td>Name of the device component, such as model, license, software, and segments.</td>
</tr>
<tr>
<td>Type</td>
<td>Type of component, such as chassis or copper port.</td>
</tr>
<tr>
<td>Segment</td>
<td>Device segment.</td>
</tr>
<tr>
<td>System Health</td>
<td>Health status of the device. See Status indicators on page 322.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> For IPS NX-Platform and TPS TX Series devices, system health displays details about the fans and power supplies.</td>
</tr>
<tr>
<td>Details</td>
<td>Status details or description.</td>
</tr>
</tbody>
</table>

**Note:** If the System Health indicator displays an error or issue, you can review the System Log for information on these health events. See Events summary on page 295.

**Note:** If you receive errors or have issues distributing profiles to devices due to exceeded limits of objects or filters, see SMS error messages on page 678.

### Status indicators

A status indicator is a colored icon that appears next to a graphic or a text item in a table. Status indicators on each graphic in the Devices screen facilitate device monitoring by displaying information about the traffic processing, health, and hardware behavior on each device and its segments.

### Status indicator legends

Status indicators usually appear as colored circles or squares next to a device, device group, segment or hardware component. In the detailed device chassis graphic, the following port graphics actually change their color as their status changes.
Table 94. Components

<table>
<thead>
<tr>
<th>Graphic</th>
<th>Component</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Copper ports" /></td>
<td>Copper ports</td>
</tr>
<tr>
<td><img src="image" alt="Fiber ports" /></td>
<td>Fiber ports</td>
</tr>
</tbody>
</table>

Status indicators appear in the following colors.

Table 95. Status indicator colors

<table>
<thead>
<tr>
<th>Color</th>
<th>Status</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="white with gray stripes" /></td>
<td>Ignore</td>
<td>Ignore the status of this element.</td>
</tr>
<tr>
<td><img src="image" alt="red" /></td>
<td>Critical</td>
<td>Respond immediately.</td>
</tr>
<tr>
<td><img src="image" alt="yellow" /></td>
<td>Major</td>
<td>Respond quickly.</td>
</tr>
<tr>
<td><img src="image" alt="cyan" /></td>
<td>Minor</td>
<td>Respond as time permits.</td>
</tr>
<tr>
<td><img src="image" alt="gray" /></td>
<td>Informational</td>
<td>You might be interested in this event.</td>
</tr>
<tr>
<td><img src="image" alt="unknown" /></td>
<td>Unknown</td>
<td>Status is unknown for this item.</td>
</tr>
<tr>
<td>Color</td>
<td>Status</td>
<td>Meaning</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>white</td>
<td></td>
<td></td>
</tr>
<tr>
<td>green</td>
<td>Normal</td>
<td>No issues exist for this item.</td>
</tr>
<tr>
<td>status color</td>
<td>Acknowledged</td>
<td>The color varies because acknowledging a status adds gray stripes to the current status indicator. When the status for the component changes, a status indicator set to Acknowledged changes to a color representing the new status.</td>
</tr>
<tr>
<td>with gray</td>
<td></td>
<td></td>
</tr>
<tr>
<td>stripes</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Additional device monitoring is available through the Events feature for a specific device. See *Event monitoring* on page 301.

**Device Configuration wizard**

For each hardware device or appliance that is managed through the SMS, you can use the Device Configuration wizard to configure or edit certain groups of settings, depending on your specific device.

For information about how you can configure a stack of devices, see *Security policy configuration* on page 526.

To open the Device Configuration wizard, expand **All Devices > [device name]** in the navigation pane, and then select **Device Configuration**. On the Device Configuration screen, click **Edit**. The configurable groups of settings can include the following, depending on your device:

- **Management Information** — Set the hostname and location for the device. If the device supports it, you can configure management port settings.
- **Management Network** — Configure the management network settings for your device.
- **Management Routes** — Configure routing options that enable you to communicate with network subnets other than the subnet where the management port is located. If you will manage your TippingPoint device from a different subnet, you must define a route between the subnet to which your workstation is connected and the subnet to which your TippingPoint Host Management Port is connected.
- **NAT** — Option to enable Network Address Translation (NAT). NAT is a networking standard that lets you minimize the number of internal IP addresses that are exposed to the Internet. NAT technology converts private IP addresses on an internal private network to one or more public IP addresses for the Internet. If you use a NAT server, you can configure the setting on the NAT screen of the Device Configuration Wizard.
- **Host IP Filters** — Configure IP filter settings to prioritize traffic or implement security policy. Filter rules set to Deny affects the SMS management of the appliance.
Services — Configure settings for system services. SSH must be enabled to enable the SMS to communicate with the Core Controller. Port traffic statistics are used in traffic reports. Configure whether a management service is provided through the network port or the management port.

AFC Settings — Set Adaptive Filtering Configuration (AFC) options that automatically manage your device under extreme load conditions and protect against the potential adverse effects of a defective filter. For NGFW appliances, set this in Device Settings.

HA (High Availability) — Configure IPS devices to provide continued network traffic support in case of a failure or a loss of power. The Core Controller supports Intrinsic HA and Zero Power HA.

Performance Protection — Configure logging mode settings for alerts.

SNMP Settings — Configure your security device for Simple Network Management Protocol (SNMP) support. Specify the Engine ID, the SNMP trap destinations, the SNMPv2 communities, and SNMPv3 users.

Note: You must enable Encrypted Alert Channel if your profile's Capture Additional Event Information setting includes HTTP. SNMP does not support HTTP context.

Log Configuration — Configure user encryption policy, specify your master key, and set the notification contact properties and threshold severities of audit, system, VPN and quarantine logs.

NMS — Configure NMS traps to allow monitoring of the device by a restricted NMS. Port 162 is the default SNMP trap port.

Remote Syslog or Remote System Log — Designate a remote syslog server on your network and define the aggregation period.

Servers or Email Server — Configure Domain Name Service (DNS) and default email settings. You might have to configure a management route so that your device can communicate with the SMTP server that handles the notifications.

Time Settings — Configure options to keep time internally using the CMOS clock, or to use a Simple Network Time Protocol (SNTP) server to check and synchronize time.

TSE Settings or Device Settings — Configure device-specific global settings, such as IDS and quarantine settings, timeout settings, and asymmetric routing (DDoS filters cannot work if this feature is enabled). For an IPS device, additional Threat Suppression Engine (TSE) configuration includes GZIP decompression settings and HTTP inspection processing properties. For NGFW appliances, additional configuration includes adaptive filter properties, and auto-reboot enablement.

Authentication Preferences — Configure user password and security parameter settings for the device.

sFlow® — For NX-Platform IPS devices and for TPS devices running TOS v5.0.0 or later only, specify whether sFlow sampling, which analyzes a random flow of traffic to a server, is enabled. Configure which network segments have sFlow enabled, the size of the sample rate at the segment level, and the IP address...
of the collection repository. Beginning with version 4.2.0, the SMS Collector server can be configured as the
data collection repository in addition to a third-party server.

**Note:** vTPS devices do not support sFlow sampling.

**Application Visibility** — Enable or disable application visibility for an NGFW appliance. Application
visibility allows you to see what applications are being used on your network using SMS

### System update and snapshots

On the Device Configuration (System Update) screen, you can manage software versions and snapshots
for a specific device. The SMS maintains a history of versions installed for your device. The Previous TOS
Version panel displays a list of previous TOS versions. You can rollback to a previous version of the device
software.

**Note:** Prior to rolling back to a software version, make sure to review the release notes for any specific
notations and warnings regarding the functionality for that version.

### System snapshots

The System Snapshots panel enables you to manage snapshots of device filters and settings. You can create
these snapshots through the Device Configuration screen for a specific device. Creating a new snapshot
places a copy on the device. Archiving a snapshot places a copy on the SMS. Deleting a snapshot removes
the system snapshot from the device and, if present, the snapshot on the SMS.

Snapshots for IPS (N-Platform or NX-Platform) and TPS devices have the option to include LSM-created
Reputation Entries as well as ThreatDV- and SMS-created entries.

The Device Configuration (System Update) screen displays the following information:

- **Previous TOS Version** — Version of the TOS.
- **System Snapshot**:
  - **Name** — Name of the snapshot.
  - **Date** — Date of the snapshot.
  - **TOS Version** — Version of the TOS running when the snapshot was made.
  - **DV Version** — Version of the Digital Vaccine package when the snapshot was made.
  - **Archived on SMS** — Indicates if there is an archived copy on the SMS.
  - **Allow Restore** — Indicates if you can restore the snapshot.

### Common device tasks

Use the following topics to perform tasks common to all SMS-managed devices:
Adding, editing, or deleting a device

After you add a device to the SMS, you can track, control, and report on the traffic that passes through it; update the software and filters installed on it; and manage its network configuration.

After you add a TPS device, NGFW appliance, or IPS device to the SMS, it is under the exclusive control of the SMS. The Local Security Manager (LSM) Web interface does not allow you to make configuration changes unless you unmanage the device first.

**Important:** When you add a TPS or vTPS device, always distribute an inspection profile to all segments to begin protecting network traffic. By default, when you add a vTPS or TPS device, all filter categories are disabled in the Default security profile. When a TPS or vTPS device is unmanaged or deleted, there is no change in the filters.

**Note:** You must have SuperUser rights on the SMS to add or delete a device.

Read the product documentation and follow instructions shipped with an TippingPoint product before you add the device to the SMS. A device must be installed and powered on before you can add it.

You must configure Threat Protection System (TPS) devices, Next Generation Firewall (NGFW) appliances, and Intrusion Prevention System (IPS) devices to allow SMS control before you can manage them in the SMS. Before you can manage a Core Controller, you must run the OBE. Before you add a device, read the product documentation for that particular TippingPoint product.

**Note:** You can add an NGFW appliance to the SMS only after an application-enabled Digital Vaccine has been activated.

You can use the SMS client to add or edit a single device or multiple devices at once. After you add a device to the SMS, you can unmanage and re-manage the device without having to remove it. The SMS allows you to add multiple devices using a text file. The text file must contain one valid IP address per line or a comma-delimited list of valid IP addresses. All devices in the list must have the same username and password.
Add a device

Add a device to the SMS so that you can track, control, and report on the traffic that passes through it; update the software and filters installed on it; and manage its network configuration.

**Important:** When you add a TPS or vTPS device, always distribute an inspection profile to all segments to begin protecting network traffic. By default, when you add a vTPS or TPS device, all filter categories are disabled in the Default security profile.

1. On the Devices screen, click **New Device**.
2. In the New Device wizard, do any of the following:
   a. To add a single device, select **Add Device(s)**, and enter the device IP Address.
   b. To add multiple devices, select **Add Device(s)**, and enter the device IP addresses, separated by commas.
   c. To use a text file to add multiple devices, select **Add Multiple Devices Using a File**, and then click **Browse** to locate the file.

**Note:** When you add multiple devices, they must all use the same authentication (user name and password), and they must all be part of the same device group. SSL appliances cannot be added with other devices. After you manage a TPS device, you cannot switch the mode from the SMS.

3. Provide the Username and Password for the devices.
4. Select a Device Group for the device(s) you are adding.
5. Select the appropriate Device Type.
6. Optionally, you can click Options in the navigation pane and select from the following new device options:
   a. Select **Synchronize Device Time with SMS** to synchronize time on the device with the SMS.
   b. Select **Configure the Device** to launch the Device Configuration wizard after the device(s) are added. You can also select **Clone an existing device** to copy settings from an existing device.

**Note:** Depending on the managed device, some device configuration settings do not support cloning. For example, you cannot clone FIPS Settings.

**Note:** To clone the Remote Authentication setting and RADIUS or TACACS+ servers, select **Remote Authentication Settings** in the Devices – Copy Device Settings dialog during the clone. RADIUS and TACACS+ authentication settings can only be cloned to devices that support RADIUS (all TPS devices, N-Platform or NX-Platform devices running TOS v3.7.0 or later) and TACACS+ (TPS and vTPS devices running TOS v5.0.0 or later, N-Platform or NX-Platform devices running TOS v3.8.0 or later).

7. Click **OK**.
When a device is successfully added to the SMS, the device appears in the All Devices area and in the navigation tree under the All Devices node. If the device is functioning properly, the Health Status indicator is green. When you add a device, the system saves historical data for the device.

If you choose to permanently remove a device from your SMS, you must delete it. Deleting a device removes it and its related managed objects from the SMS database. The system retains historical data unless you choose to delete it as well.

**Editing one or more devices**

1. On the Devices screen, expand **All Devices** in the navigation pane.
2. Select **Member Summary** in the navigation pane.
3. In the right pane, select the **Management Information** tab.
4. Select the device or devices you want to edit, and then click **Edit**.
5. Use the Device Configuration dialog to make any device changes.

   The Devices Being Modified screen lists every device that is being modified. Use the icons located on a screen to quickly see if the information for a category applies to an IPS devices or an NGFW appliance. A binoculars icon \( \text{\textvisiblesymbol} \) indicates that the information applies to an IPS device. A fire icon \( \text{\textvisiblesymbol} \) indicates that the information applies to an NGFW appliance. The number in the parentheses indicates the number of devices. On any Device Configuration screen, you can hover your mouse over the binoculars and fire icons to the respective fields.

6. When editing devices, note the following:

   - During a multiple-devices edit, FIPS Settings are not available and will not display on the Device Configuration screen.
   - Remote authentication for TPS devices is not supported as part of a multiple-device update.
   - During a multiple-devices edit, setting a RADIUS or TACACS+ server as the Remote Authentication or changing one of these servers only updates IPS devices that support those types of remote authentication (for RADIUS authentication, N-Platform or NX-Platform devices running TOS v3.7.0 or later; for TACACS+ authentication, N-Platform or NX-Platform devices running TOS v3.8.0 or later).
   - The RADIUS and TACACS+ options and the RADIUS Servers and TACACS+ Servers sections are displayed in Authentication Preferences only if at least one of the managed devices supports RADIUS and TACACS+ authentication. Devices that do not support these remote authentication options do not get updated.
   - If you replace an IPS device with a TPS device, any configured TACACS servers for the replaced IPS device become a TACACS group in the TPS device.
Delete a device

1. On the Devices screen, click the device you want to remove.
2. Click the Edit menu, and select Delete.
3. In the Delete Selected Device dialog, click Delete.

When the process is complete, the device name is no longer displayed in any SMS window.

If you prefer to unmanage a device instead of deleting it, refer to Unmanaging or remanaging a device on page 330.

**Important:** A TPS device can be managed by the SMS as an IPS device or NGFW appliance, depending on the selected mode. However, once a TPS device has been managed by the SMS, you cannot change the mode of the device without a factory reset.

Creating or deleting a device group

The SMS client enables you to organize device segments into device groups that can be managed more easily. Each device group displays its own member summary information, and the group structure allows you to act more easily on multiple devices at the same time.

Create a device group

1. On the Devices screen, click the File menu and select New > Device Group.
2. In the New Device Group dialog, provide a device group name.
3. Select a parent group from the Add to Device Group drop-down menu. The default value is All Devices.
4. Click OK.

Delete a device group

1. On the Devices screen, select the device group.
2. Click the Edit menu, and select Delete.
3. In the Delete Selected Group dialog, click Delete.

**Note:** Deleting a device group moves its member devices to the parent group and purges the group information from the database.

Unmanaging or remanaging a device

While a device is being managed, you can control device configuration, software updates, profile distribution, and filters through the SMS client. SMS management overrides the use and configuration control of the Local Security Manager (LSM). If you want to manage a device, the device must be
configured to allow SMS control. For more information, see the *TippingPoint Local Manager User Guide* for your device.

Unmanaging a device returns control of the device to the device itself and its Local Security Manager (LSM). You can temporarily return control to the LSM by unmanaging the device from the SMS.

**Note:** You cannot unmanage a device while it is receiving or distributing a software or security package.

**Note:** You must have Administrator access on the SMS to unmanage a device.

### Unmanage a Device

1. On the Devices screen, select a managed device in the All Devices area.
2. Click the **Edit** menu and select **Unmanage Device**.
3. In the Unmanage Device dialog, click **Unmanage**.
4. In the navigation pane and in All Devices area, the device icon is overlaid with a red X, which indicates that the device is no longer being managed. The SMS cannot update or distribute packages to an unmanaged device.

   After you unmanage a device, you can resume control of the device by re-managing it. When you manage a device, you are resuming control of a device that has been unmanaged.

### Manage a device

1. In the All Devices area, select the unmanaged device.
2. Click the **Edit** menu and select **Manage Device**.
3. In the Manage Device dialog, provide the Username and Password for the device.
4. Click **Manage**.

You can now configure and manage the device using the SMS.

### Importing or exporting device configuration

The SMS provides export and import functions of the settings that you can use to configure device settings that are common across multiple devices. The first step is to configure a device with the settings that you want to use across multiple devices. The settings can be exported to a device settings file. The device settings in the file can then be imported into multiple devices.

This option is useful when deploying multiple devices that have the same or similar configuration requirements. For devices with similar configurations requirements, you can set up base settings that can then be tuned on each device after the settings file is imported.

**Note:** Depending on the managed device, some device configuration settings do not support import/export. For example, you cannot import or export FIPS Settings.
Export device settings
1. On the Devices (All Devices) screen, select a device and click Export Configuration.
2. In the Export Config dialog, specify the location for the exported file.
3. Do one of the following:
   • To export all of the device settings, select Select All Options.
   • To export selected specific device settings, select the settings you want to export.
   
   **Note:** When you export settings from a device that authenticates using RADIUS or TACACS+, select the Remote Authentication Settings checkbox to include those settings in the export.
4. Click OK.

Import device settings
1. On the Devices (All Devices) screen, click Import Configuration.
2. In the Import Device Configuration wizard, specify the name and location of the file to be imported or click Browse to find and select the file.
   
   To review the settings in the import file, click View Details.
3. Select Device Configuration Settings from the left navigational menu or click Next.
4. Do one of the following:
   • To import all of the device settings, select the check box labeled Select All Options.
   • To import specific device settings, select the check boxes associated with the desired settings.
   
   **Note:** When you import settings from a device that authenticates using RADIUS or TACACS+, select the Remote Authentication checkbox to include those settings in the import.
5. Select Device Targets from the left navigational menu or click Next.
6. Select the device or devices that are the targets for the imported settings. If a device is grayed out or lists an error, the device might not be compatible with the device settings, be unmanaged, or have another issue.
7. To view the status details of a listed device, click the device listing. The status summary displays in the table below the Target table.
8. Click Finish to import the selected setting from the import file to the selected target devices.

Viewing and searching events
Use the following search criteria when you search events:
Table 96. Event search criteria

<table>
<thead>
<tr>
<th>Status</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blocked Streams</td>
<td>• Protocols: All, TCP, UDP, ICMP, ICMPv6</td>
</tr>
<tr>
<td></td>
<td>• Src/Dest Address: Source/Destination IP Address</td>
</tr>
<tr>
<td></td>
<td>• Port</td>
</tr>
<tr>
<td>Rate Limited Streams</td>
<td>• Protocols: All, TCP, UDP, ICMP, ICMPv6</td>
</tr>
<tr>
<td></td>
<td>• Src/Dest Address: Source/Destination IP Address</td>
</tr>
<tr>
<td></td>
<td>• Port</td>
</tr>
<tr>
<td>Trusted Streams</td>
<td>• Protocols: All, TCP, UDP, ICMP, ICMPv6</td>
</tr>
<tr>
<td></td>
<td>• Src/Dest Address: Source/Destination IP Address</td>
</tr>
<tr>
<td></td>
<td>• Port</td>
</tr>
<tr>
<td>Quarantined Hosts</td>
<td>• Host Address</td>
</tr>
</tbody>
</table>

**Note:** When you click **Apply**, the SMS restarts the segment, updating the hardware settings for the device and restarting the auto-negotiation process. If an error occurs, the copper cable translator might not support auto-negotiation. See **IPS port out-of-service** on page 678.

**Note:** Not all Traffic Normalization filters result in blocked streams.

**View events for all devices**

1. On the Devices screen, expand the **All Devices** in the navigation pane.
2. Expand **Member Summary** in the navigation pane, and then select **Events**.
3. Select the tab associated with the event you want to view:
   - Blocked Streams
   - Rate Limited Streams
   - Trusted Streams
   - Quarantined Hosts
• Adaptive Filter

**View events for a specific device**

1. On the Devices screen, expand the **All Devices** in the navigation pane.
2. Select a device and expand the options.
3. Select **Events** from the navigation pane.
4. On the Events screen, select the tab associated with the event you want to view:
   • Blocked Streams
   • Rate Limited Streams
   • Trusted Streams
   • Quarantined Hosts
   • Adaptive Filter

**Flush events lists**

1. Do one of the following: *View events for all devices* on page 333 or *View events for a specific device* on page 334.
2. Select one of the following tabs:
   • Blocked Streams
   • Rate Limited Streams
   • Trusted Streams
3. To flush all blocked or rate limited streams, click **Flush All**.
4. To flush selected streams, select entries, and then click **Flush Selected**.
5. Click **OK**.

**Managing versions, updates, and snapshots**

On the Device Configuration (System Update) screen, you can manage software versions and snapshots for a specific device.

For information about how you can manage versions, updates and snapshots on a stack, see *System updates and snapshots* on page 530.

**Rollback to a previous version**

A rollback operation reverts the currently running software on your device to a previous working version that you select.
Important: (TPS and vTPS only) After you rollback, always make sure the master key on the device is the same as the master key that was used to secure the keystore in the rollback TOS image.

Note: Prior to rolling back to a software version, make sure to review the release notes for any specific notations and warnings regarding the functionality for that version. For information about how you can rollback a stacking device to a previous version, see System updates and snapshots on page 530.

Note: After you install the 2K key, you will lose device management functionality on the SMS, if you roll back to the following versions: TPS devices running TOS v4.0 and NGFW appliances running TOS v1.2.1 or earlier. For more information, see SMS certificate key on page 537.

1. Select a device, expand the device entry in the left navigational menu, and then expand the Device Configuration entry.
2. Select the System Update entry.
   The Device Configuration (System Update) screen displays.
3. From the Previous TOS Versions table, select a software version entry.
4. Click Previous Version Rollback and follow any instructions.

(TPS and vTPS only) When the rollback completes, verify the master key on the device is the same as the master key that was used to secure the keystore in the rollback TOS image. From the CLI, edit and save the configuration. If a “Device keystore is locked” message is displayed, the master key does not match. To resolve this issue, complete the following steps:

- If you know the master key that was set in the TOS rollback image, set the master key to that passphrase. Use the LSM or the master-key set CLI command to set the master key.
- If you do not know the master key:
  a. (TOS 4.x.x images only) Clear the master key and reset the keystore by using the master-key clear reset-keystore CLI command.
  b. (TOS 5.x.x images only) Reset the keystore by using the master-key reset-keystore CLI command.
  c. Reset the master key by using the LSM or the master-key set CLI command.
  d. If the keystore persisted sensitive information, such private keys for SSL inspection, import the private keys into the keystore and assign the new keys to the appropriate SSL servers.
  e. If the external user disk is encrypted, synchronize the ThreatDV URL Reputation Feed and User-defined URL Entries database to the device.

Note: If you change the master key while the external user disk is encrypted, the contents of the external user disk, which include the ThreatDV URL Reputation Feed and User-defined URL Entries database, are erased.
Delete a previous TOS version

1. Select a device, expand the device entry in the left navigational menu and expand the **Device Configuration** entry.
2. Select the **System Update** entry.
   The Device Configuration (System Update) screen displays.
3. From the Previous TOS Versions table, select a software version entry.
4. Click **Delete**.
   A confirmation message displays.
5. Select the appropriate action to delete the entry.

Create a new system snapshot on the device

1. Select a device, expand the device entry in the left navigational menu, and then expand the **Device Configuration** entry.
2. Select the **System Update** entry.
   The Device Configuration (System Update) screen displays.
3. From the System Snapshots area, click **New**.
4. A new snapshot image is created of the device and the entry displays in the table.

   **Note:** The snapshot procedure might take time. Allow sufficient time for the procedure to complete.

Import a system snapshot from a file

1. Select a device, expand the device entry in the left navigational menu and expand the **Device Configuration** entry.
2. Select the **System Update** entry.
   The Device Configuration (System Update) screen displays.
3. From the System Snapshots area, click **Import**.
   A file browsing window displays.
4. Browse to and select the local file, and then click **OK**.
   The system uploads the snapshot to the list of entries.

Export a system snapshot to a file

1. Select a device, expand the device entry in the left navigational menu and expand the **Device Configuration** entry.
2. Select the **System Update** entry.
   The Device Configuration (System Update) screen displays.

3. In the System Snapshots table, select a snapshot to export.

4. Click **Export**.
   A file browsing window displays.

5. Select a location for the file export.
   The system exports the snapshot to a file.

**Archive a system snapshot to the SMS**

1. Select a device, expand the device entry in the left navigational menu and expand the **Device Configuration** entry.

2. Select the **System Update** entry.
   The Device Configuration (System Update) screen displays.

3. In the System Snapshots table, select a snapshot to archive.

4. Click **Archive to SMS**.
   The system archives the snapshot to the SMS.

**Restore from a system snapshot**

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 you restore a snapshot, keep in mind the following points:

- 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.
• (TX Series) The port configuration for each slot is preserved after you restore a snapshot when the same I/O module is installed in the same slot. Otherwise, the port configuration resets to the default.

• 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.

**To restore from a system snapshot**

1. Select a device, expand the device entry in the left navigational menu and expand the Device Configuration entry.

2. Select the System Update entry.

   The Device Configuration (System Update) screen displays.

3. In the System Snapshots table, select a snapshot to rollback to and click **Restore**. When you rollback, the snapshot overwrites all settings for a profile to the device with the snapshot settings.

   The system might prompt with a warning or further steps.

   **Note:** The snapshot procedure might take time. Give sufficient time for the procedure to complete.

**Delete a system snapshot**

1. Select a device, expand the device entry in the left navigational menu and expand the Device Configuration entry.

2. Select the System Update entry.

   The Device Configuration (System Update) screen displays.

3. In the System Snapshots table, select a snapshot to delete.

   **Important:** This action deletes the system snapshot from the device and, if present, the snapshot on the SMS.

4. Click **Delete**.

5. If a confirmation message displays, select the appropriate option to delete the snapshot.

**Importing and downloading the TOS**

You can import and download updated versions of the TippingPoint operating system (TOS) for distribution to your TippingPoint system. The TOS software updates the operating system software for devices. The Devices (TippingPoint OS) screen allows you to download and import many versions of the software to give you more control over your device software.

The TOS version listings are filtered by IPS, Core Controller, N-Platform or NX-Platform IPS devices, and TPS devices. If no devices were added to the SMS, the IPS TOS versions are listed. When you add new devices to the SMS device inventory, the TOS version list is updated the next time the SMS contacts the TMC. At any time, you can refresh the TOS list by clicking **Refresh** on the TOS download dialog.
You can distribute the software updates to all devices or a particular segment group. You can do the following:

- Download the TOS software on page 339
- Import TOS software from a file on page 339

After importing and downloading the file(s), you need to distribute and manage the files. See the following:

- Managing TOS distribution on page 340
- Distribute the TOS on page 340

**Download the TOS software**

1. In the Devices navigation menu, select TippingPoint OS.
2. On the Devices (TippingPoint OS) screen, click Download from TMC in the TOS Inventory section.
3. In the Devices - New Device Software Download dialog, verify that the Available Device Software selection is correct, and click Download.

   The Download Software Package from TMC displays, and the TOS software download begins.
4. The TOS Inventory list displays the downloaded package, and it is ready to be distributed.

**Import TOS software from a file**

1. In a Web browser, open https://tmc.tippingpoint.com.

   If you have not already done so, create a TMC account using your Customer ID and Serial Number.
2. From the top menu bar on the TMC home page, click Releases > Software > [model_type] > [model_number].
3. Locate the package you want to download and perform one of the following actions:
   - Click View to review the information about the package, and then click Download.
   - Click Download to download the package without reviewing the package information.
4. Follow the download instructions for your specific browser.

   **Note:** To avoid unexpected behavior on the SMS, do not change the name of this file.
5. In the SMS client, open the Devices (TippingPoint OS) screen.
6. In the TOS Inventory section, click Import.
7. In the Choose File dialog, select the file and click OK.

   After the file imports, the file displays in the TOS Inventory section and is ready to be distributed.
Managing TOS distribution

After you have downloaded and imported TippingPoint OS software packages into the SMS, you can distribute the updates to devices. Each distribution process is shown on the Distribution Progress panel of the Devices (TippingPoint OS) screen.

You can also review the details and manage the available TOS entries in the TOS Inventory section. You can keep multiple versions of the TOS software.

**Note:** You cannot cancel a TOS update when it is in-progress. When you begin the installation of the update TOS package, you cannot stop or cancel the device.

### Distribute the TOS

1. On the Devices navigation pane, click **TippingPoint OS**.
   
   The Devices (TippingPoint OS) screen displays.
2. Select an **TippingPoint OS** entry from the TOS Inventory.
3. Do one of the following:
   - Click **Distribute**.
   - On the top menu bar, select the **File > Distribute TOS to Device** menu item.
   
   The distribution process displays on the Distribution Progress panel.

   For information about how you can distribute the TOS package to a stack of devices, see *Security policy configuration* on page 526.

Managing virtual segments

Virtual segments define traffic using an endpoint pair, a VLAN ID, or both that are assigned to one or more physical segments.

### Create a virtual segment

**Tip:** For better management, you might want to create a unique segment group prior to creating a new virtual segment.

1. On the Devices navigation pane, click **Virtual Segments**, and then click **New** on the Devices (Virtual Segments) screen.
2. On the Name & Traffic Criteria screen, complete the following description entries for the virtual segment.
   - **Name** — Must be unique among all existing virtual segments.
   - **Description** — A brief explanation about the virtual segment.
3. Complete any of the following criteria you want to use to define the traffic for the virtual segment:
   • **VLAN** — Can be one or more comma-separated VLAN IDs or a Named Resource.
   • **Source IP Address** — Can be one or more comma-separated CIDRs or a Named Resource. Ranged-based Named Resources is not supported.
   • **Destination IP Address** — Can be one or more comma-separated CIDRs or a Named Resource. Ranged-based Named Resources is not supported.

   **Note:** Physical segments tied to a TOS version 2.2 or earlier device which does not support virtual segments are disabled but displayed in the physical segment lists. For TPS TX Series devices and IPS NX-Platform devices, the slot number is represented.

4. When the Segment Group Membership dialog box displays, select a group for this virtual segment.
5. If no custom segment groups have been created, the virtual segment is automatically assigned to the default segment group. To create a new segment group or change group membership, see Create a segment group on page 343 and Edit segment group membership on page 344.
6. From the left navigational menu, select **Physical Segments**.
   • Select one or more physical segments from the **Physical Segments** list that you want to assign to the virtual segment.
   • To add a physical segment to the list, select **Add**. From the Select Physical Segment screen, select the segment or segments to add.

   When you create a virtual segment on a stack of IPS devices, the available physical segments consist of network segments on slots 1–3. For more information, see Security policy configuration on page 526.

   **Note:** For IPS NX-Platform and TPS TX Series devices, the segments are listed by slot numbers.
   • Click **OK** to return to the Virtual Segments wizard.
7. To validate the virtual segment setup, select **Validation Report** from the left navigational menu.
   • The Validation Report screen provides information about the severity and summary of error status.
   • To view additional information, click **Details**.
8. Click **OK** to preserve the settings and return to the main Virtual Segments screen.

**Delete a virtual segment**
1. On the Devices navigation pane, click **Virtual Segments**. The Devices (Virtual Segments) screen displays.
2. In the Virtual Segments table, select a virtual segment entry.
3. Do one of the following:
   • Click **Delete**.
• On the top menu bar, click **Edit** and select **Delete**.

A verification message displays.

4. Click **Yes**.

**Analyze traffic flow for virtual segments**

1. On the Devices navigation pane, click **Virtual Segments**.

   The Devices (Virtual Segments) screen displays.

2. In the Traffic Flow Analyzer area, select one or more of the following options and enter the required information:
   • Source Address
   • Destination Address
   • Device Segment
   • VLAN ID

3. Click **Find** to view the virtual segments that match the search criteria you entered.

**Managing segment groups**

*Note:* When SuperUser or Admin user access or authority is specified, the user must have the respective SuperUser or Admin capabilities. See *Authentication and authorization* on page 542.

You can view, create, and delete segment groups through the Devices (Segment Groups) screen. These groups allow you to manage software and profile updates on your TippingPoint System. Segment groups can contain an unlimited number of devices. However, you cannot add a segment to more than one group.

*Note:* A segment can only be a member of one group and have only one distributed profile at any given time. You cannot add a segment to multiple groups. However, you can have many profiles point to the same segment. When you distribute a profile the segment replaces the currently used profile.

When you create a new group, the group displays as an:
   • Entry on the Devices (Segment Groups) screen
   • Expanded option on the Devices navigation pane

You can do the following:
   • *View segment group details* on page 343
   • *Create a segment group* on page 343
   • *Edit segment group membership* on page 344
View segment group details

1. Perform one of the following tasks:
   • From the left navigational menu, select a segment group listing.
   • From the Devices (Segment Groups) screen, select an entry from the Segment Group table, and then click Details.

2. The Segment Group area lists the Group Name.

3. The Members area lists the following information:
   • **Segment** — Segment member of the group.
   • **Slot** — IO slot from 1 to 4 (for IPS NX-Platform and TPS 8400TX devices) and IO slot from 1 to 2 for TPS 8200TX devices.
   • **Device** — Device whose segments are members of the group.
   • **Direction** — Traffic direction for the segment.
   • **Profile** — Profile of filters associated with the group.
   • **Description** — User-entered description about the group.

4. If desired, you can perform the any of the following tasks:
   • [Create a segment group](#) on page 343
   • [Edit segment group membership](#) on page 344
   • [Edit the name and descriptions for a segment group member](#) on page 345
   • [Create a segment group](#) on page 343
   • [Editing the management port settings for the S-Series devices](#) on page 355

Import a device profile

After you have added and started managing a device, you might need to upload (or import) the filters of that device into an SMS profile. This feature allows you to import filters from a device with customizations not currently in a profile managed by the SMS system.

1. On the Devices (Segment Groups) screen, select an entry from the Segment Groups list, and then click Details.
2. From the Members list, select an entry for a device, and then click Import Profile.

Create a segment group

1. On the Devices (Segment Groups) screen, click New to create a new segment group.
The Segment Group Edit dialog displays.

2. In the Group Name field, specify a name for the group.

3. In the **Non Members** pane, select how you want to organize the list: by **Device** or by **Segment Group**.

4. Select one or more devices from the list.

   You can select multiple devices by clicking and dragging your cursor over the names and using the **SHIFT** and **CTRL** keys.

   When creating a segment group for a stack of devices, choose from the physical segments on the segment reference device. For more information, see *Security policy configuration* on page 526.

   **Note:** For IPS (NX-Platform) and TPS (TX Series) devices, the Segment Group table lists the slot number associated with the segment group.

5. Click the right arrow button to move the selected device to the right members pane.

6. If you want to remove one or more devices before you create the segment group, select one or more devices in the **Group Members** list and click the left arrow to move the selected devices back to the **Non Members** list.

7. Click **OK**.

   The segment group displays in the Devices navigation pane and Devices (Segment Group) screen.

---

**Edit segment group membership**

1. On the Devices (Segment Groups) screen, select an entry from the Members table, and do one of the following:
   - Click **Edit Membership**.
   - Right-click and select **Edit Membership**.
   - Go to the top menu bar and select **Edit > Edit Membership**.

   The Segment Group Edit dialog displays.

2. If desired, modify the **Group Name**.

3. In the **Non Members** pane, select how you want to organize the list: by **Device** or by **Segment Group**.

4. Select one or more devices from the list. You can select multiple devices by clicking and dragging your cursor over the names and using the **SHIFT** and **CTRL** keys.

5. Click the right arrow button to move the selected device to the right members pane.

6. If you want to remove a device or devices from the segment group, select a device or multiple devices from the Group Members area, and then click the left arrow button to move the device or devices.
7. Click **OK**.

**Edit the name and descriptions for a segment group member**

1. On the Devices (Segment Groups) screen, select an entry from the Members table, and do one of the following:
   - Click **Edit**.
   - Right-click and select **Edit**.
   
   The Segment Group Member - Edit dialog displays.

2. Make desired modifications to the **Name** and **Description**.

3. Click **OK**.

**Edit permissions for a segment group member**

1. On the Devices (Segment Groups) screen, select an entry from the Members table.
2. Go to the top menu bar and select **Edit > Permissions**.

   The Segment Group - Permissions dialog displays.

3. By default, permissions are granted to SuperUsers. If you want to grant permissions to other roles, select the appropriate check box in the Permissions area.

4. Click **OK**.

**Distribution queue configuration – TPS and IPS (S-Series, N-Platform, and NX-Platform)**

SMS supports queuing of any package distributions to an IPS or TPS device. The types of packages that can be distributed to a device include:

- Tipping Point Operating System (TOS)
- Profiles
- Digital Vaccine (DV)
- Digital Vaccine Toolkit (DVT)

The queuing of distributions to a device allows you to start a distribution of different packages to the same device. Distributions are placed in the device distribution queue and displayed in table format. Queued distributions are processed when the device is available and in a normal communication state. Each device
A distribution queue has one queue and can contain any of the available distribution types. The order in which the distributions are added to the queue is maintained and can be changed.

You can perform the following tasks:

- **View distribution queues for a device** on page 346
- **Change or delete a distribution queue entry** on page 346

For additional information about package distributions, see:

- **TippingPoint Operating System** on page 414
- **Distribute profiles** on page 142
- **Digital Vaccines** on page 188

**View distribution queues for a device**

1. On the Devices screen, expand the All Devices in the navigation pane.
2. Select a device and expand the options.
3. Select the Distribution Queue option.
4. The Distribution Queue table lists all the packages in the queue and the following information about each queue:
   - **Order** — Number represent the sequential order of the distribution.
   - **Distribution Type** — Type of distribution (TOS, Profile, DV, DVT).
   - **Package** — Name of the package and the version that is being distributed.
   - **Time Entered** — Time distribution was started.
   - **Status** — Waiting in queue or in distribution.

**Change or delete a distribution queue entry**

1. Select Devices > All Devices.
2. Select a device and expand the options.
3. Select the Distribution Queue option.
4. To change the order of the entries, select an entry and click Move-Up or Move-Down.
5. To delete an entry, select an entry, and then click Delete.
**Inspection Bypass configuration – TPS and IPS (N-Platform and NX-Platform)**

Through the Events screen for IPS (N-Platform or NX-Platform) and TPS devices, you can create and manage Inspection Bypass Rules that are a set of criteria used to determine if a given packet should be routed through the device without further inspection.

**Note:** The Inspection Bypass feature is only available for TippingPoint IPS (2500N, 5100N, 6100N, and NX-Platform) and TPS devices. vTPS devices are not supported. The maximum number of bypass rules is 8 for IPS devices and 32 for TPS devices.

To access the Inspection Bypass feature for a device, use the left navigational menu to navigate to the device and select the **Inspection Bypass** listing.

**Table 97. Inspection bypass rules**

<table>
<thead>
<tr>
<th>Entry title</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Reference ID of the rule in the listing.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Enable/disabled status.</td>
</tr>
<tr>
<td>Name</td>
<td>Name of the bypass rule. The name is an SMS-only feature and does not appear on the managed device.</td>
</tr>
</tbody>
</table>
| Ethernet Type | Type of Packets that are exempt from traffic based on the Rules criteria:  
  - IP — Type of IP packets that are exempt.  
  - Not IP — All non-IP packets that are exempt from inspection.  
  - Protocol — Packets from a specified protocol that are exempt. |
<p>| IP Protocol | Transport layer protocol of packets to exempt from inspection. |
| Statistics  | Number of packets that match a bypass rule. |
| Src IP      | Source IP address of packets to exempt from inspection. |</p>
<table>
<thead>
<tr>
<th>Entry title</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Src Port</td>
<td>Source port of packets to exempt from inspection. This field is valid only if TCP or UDP is specified in the <strong>IP Protocol</strong> field.</td>
</tr>
<tr>
<td>Dst IP</td>
<td>Destination IP address of packets to exempt from inspection.</td>
</tr>
<tr>
<td>Dst Port</td>
<td>Destination port of packets to exempt from inspection. This field is valid only if TCP or UDP is specified in the <strong>IP Protocol</strong> field.</td>
</tr>
</tbody>
</table>
| Action      | Action that the rule applies to the traffic.  
  - Bypass (default) – Bypasses the traffic.  
  - Block – Blocks the traffic.  
  - Redirect – Redirects the traffic. A **Target Port** field (required) is displayed for you to specify which segment port the traffic gets redirected to. This option is unselectable if no target port is available.  
  - Ingress mirror – Mirrors (copies) traffic entering the port to another segment port before the traffic gets inspected. A **Target Port** field (required) is displayed for you to specify which segment port the traffic gets mirrored to. Four mirror-to-port (MTP) configurations are supported. This option is unselectable if no target port is available.  
  - Egress mirror – Mirrors (copies) inspected traffic exiting the port to another segment port. A **Target Port** field (required) is displayed for you to specify which segment port the traffic gets mirrored to. Four MTP configurations are supported. The port-assigned Virtual LAN (VLAN) is recorded inside the captured packet. This option is unselectable if no target port is available. |

Configuring Inspection Bypass Rules includes the following areas:

- **Name** — Descriptive name and enabled state option.
- **Action** — Action that the rule applies to the traffic.
- **Protocol** — Ethernet frames that match these settings and the settings specified for VLAN are delivered directly to the other side of the IPS segment. They are not routed for inspection.
- **VLAN** — Configure the VLAN tag. Ethernet frames that match these settings and the settings specified for Protocol are delivered directly to the other side of the Device segment. They are not routed to an iLink for inspection.
• **Segments** — Segments with traffic that are subject to the Inspection Bypass Rule.

**Create or edit an inspection bypass rule**

Before you begin, review the information in *Device Details* on page 321.

**Note:** Prior to configuring an inspection bypass rule, the segment must have a profile distributed to it.

1. Navigate to the **Devices > All Devices** area, select a device that supports inspection bypass.
2. From the navigational pane expand the options for the device and then select **Inspection Bypass**.
   
   For a stack of devices, select the segment reference device (SRD). For more information about inspection bypass rules for a stack of devices, see *Security policy configuration* on page 526.

3. Click **New** to create a new rule or select an existing listing and click **Edit** to change an existing rule.
4. In the Inspection Bypass Rule wizard, select **Name** from the left navigational menu.
5. Specify a **Name** for the exception rule and then indicate the desired **Enabled** status for the rule.
6. Click **Next** or select **Action** from the wizard navigation pane.
7. Specify the action to be performed on the traffic.
   
   For a description of the available actions, see *Inspection Bypass configuration – TPS and IPS (N-Platform and NX-Platform)* on page 347.

8. Click **Next** or select **Protocol** from the wizard navigation pane.
   
   • Select the Ethernet Type.
   
   • For IP Protocol, specify the Source/Destination ports and addresses.

9. Click **Next** or select **VLAN** from the wizard navigation pane. By default VLAN tag, MPLS label, or tunneling checks are NOT performed.
   
   • To match all frames, do not select the **VLAN** check boxes.
   
   • To exempt frames from inspection, select the **VLAN** or **MPLS** option and define the value or range of frames.
   
   • To exempt tunneling frames from inspections, select the appropriate options (**GRE, MIPv4, IPv6in4**) and select an option (**Any, Present, Absent**).

10. Click **Next** or select **Segments** from the wizard navigation pane and then select the segments where the inspection bypass rule should be applied.

   **Note:** For NX series and TX Series devices, the segments are listed by slot numbers.

11. Click **Finish**.
Editing device configurations

This topic contains procedures for configuring your security device and for basic device management tasks.

You can configure the network parameters and the filter behavior for each device. As necessary, you can temporarily relinquish SMS control by unmanaging the device, or you can permanently remove it by deleting it from the SMS.

Which of the features are available depend on the managed device.

User activities

When you assume management of a device at the SMS, you can:

• View all the activity on that device.
• Define, edit or export the device configuration.
• Import a device configuration.

User access

For information about user authority, see Authentication and authorization on page 542.

⚠️Caution: If an error occurs, the copper cable translator might not support auto-negotiation. See Events configuration – TPS and IPS (S-Series, N-Platform, NX-Platform) on page 300 or IPS port out-of-service on page 678.

The Device Configuration wizard enables you to configure or edit device-specific settings, depending on your device. See Device Details on page 321.

Management information

You use the Management Information page in the Device Configuration wizard to view and update general information about the device. The fields on this page collectively give you a complete view of the management information for a specific device.

Depending on the device, you can perform these options from the Management Information page:

• Update the host name of your device and add descriptions for the device location and contact information.
• Review the device model and serial number.
• View or configure the management port settings.
• View the Network Mask and Default Gateway and enter settings for fast ethernet port located on the management processor module. The IP address for this port is the IP address through which you access
the device. This port must be contained within your local network, but must not be contained within any of the subnets that pass traffic through the Multi-Port Defense Module of the device.

- Review the currently installed TippingPoint Operating System (TOS) package, Digital Vaccine (DV) version number, and Auxiliary DV. For more information, see *TippingPoint Operating System* on page 414 and *Digital Vaccines* on page 188.

- Reboot or shutdown the device.

- Reset IPS filters to their recommended state. Use this option to reset filters due to issues or settings. The recommended settings for a filter might differ by state (enabled/disabled), notification contacts, exceptions, and action sets.

- Go to the associated device. Click the **View LSM** or **SSH Terminal** to access the device from the SMS.

**Table 98. Management information**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Valid Input</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
<td>The host name of your device. It should be the same host name as the one listed for the device IP address in your network DNS lookup.</td>
<td>A valid host name on your network segment, a maximum of 32 characters.</td>
</tr>
<tr>
<td>Location</td>
<td>A description of the location of your device.</td>
<td></td>
</tr>
<tr>
<td>Contact</td>
<td>A contact name for your device.</td>
<td>A maximum of 32 characters describing the device contact.</td>
</tr>
<tr>
<td><strong>Note:</strong> This feature is only available on TPS devices.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Model</td>
<td>The number of your device model, such as 2200T-IPS.</td>
<td>—</td>
</tr>
<tr>
<td>Serial Number</td>
<td>The serial number of your device.</td>
<td>—</td>
</tr>
<tr>
<td>Mgmt IP Address</td>
<td>The IP address that you use to make a network connection to your device.</td>
<td>A valid IP address on the network segment the device is attached to in dotted decimal notation (255.255.255.255) notation.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
<td>Valid Input</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Network Mask</td>
<td>The network mask in effect on the subnet that your device is attached to.</td>
<td>A valid network mask for the network segment on which your device resides in dotted decimal IP address (255.255.255.255) notation.</td>
</tr>
<tr>
<td>Default Gateway</td>
<td>The gateway through which your IPS device communicates with external network entities, and through which external network entities communicate with your device. You can enter a number of gateways for Gateway and Routing.</td>
<td>A network device that contains routing tables that list your device and external network entities as well.</td>
</tr>
<tr>
<td>Edit Management Port Settings</td>
<td>Informational dialog that provides Port Details and allows you to enable/disable auto negotiation.</td>
<td>Enable/disable auto negotiation</td>
</tr>
<tr>
<td>View Management Port Settings</td>
<td>Click View Mgmt Port Settings to view management port settings and current state details.</td>
<td></td>
</tr>
<tr>
<td>TOS</td>
<td>TippingPoint Operating System (TOS).</td>
<td></td>
</tr>
<tr>
<td>DV</td>
<td>Digital Vaccine (DV) version numbers.</td>
<td>Settings related to this item have moved to Digital Vaccines on page 188.</td>
</tr>
</tbody>
</table>

**Note:** This feature is only available on select IPS devices.

**Note:** For TPS devices, if the package is a TPS IPS only package, i displays at the end of the TOS. If the package is a TPS NGFW only package, f displays at the end of the TOS.
### Auxiliary DV's

Enables you to update to the latest malware filters if you subscribe to this service. For subscription information, contact your TippingPoint representative.

### Resetting IPS filters

1. In the Device Configuration wizard, click **Management Information**.
2. Click **Reset IPS Filters**.

   A message prompts you to confirm that you want to reset all filters back to their recommended state.
3. Click **OK**.

   After resetting the IPS filters on an IPS, a message notifies you that the reset is complete; the reset process might take several minutes. Any profile distributions attempted before the reset has completed will fail, as the device is still busy resetting the filters.

   **Note:** This notification is not implemented in a pre-2.5 device. For those devices, the filter reset message displays immediately at the beginning of the reset process. For pre-2.5 devices, you can check the device System Log to determine when a filter reset is complete.

### Management network

From this screen you can configure the management network settings for your device. These settings only affect the device's management port and its ability to communicate with the SMS. They do not modify filters or otherwise change the way traffic is inspected.

IPv6 is an Internet protocol that uses 128-bit addresses, which increases the number of possible addresses and adds increased security. Expressed in a series of four-digit hexadecimal numbers that are separated by colon (:) notation, IPv6 addresses allow the Internet to grow in terms of connected hosts and data traffic.

**Note:** Incorrect settings for the default gateway or management port prevent management communication with the device.

From this screen you can:

- Enable IPv6.
- Automatically assign IPv6 addresses to the management port.
- Configure the default gateway.
- Choose one of the following ways to manage the device.
• Specified IPv6 address to the management port interface.
• Link-Local IPv6 address — the device and the SMS MUST be on the same physical network.
• Auto IPv6 address — Global unicast address assigned during network initialization.

• Enable the configured IPv6 IP address to manage the device.

Note: If you do not select Use IPv6 address to manage this device, the IPv4 address or Public IP Address on the Management Information page is used to manage the device. See Management information on page 350.

Configure the management network – TPS and IPS (N-Platform and NX-Platform)

Note: The management network configuration only impacts the device management port and its ability to communicate with the SMS. These settings do NOT modify filters or change the way traffic is inspected.

1. In the Device Configuration wizard, select Management Network from the navigation pane. The Device Configuration (Management Network) page displays. The following Management Network options are available:
   • **Communications:** Device Management Protocol — IPv4 or IPv6.
   • **Configuration:** Management Port Traffic Protocol — IPv4, IPv6 or both.

2. To set the protocol for managing the device, go to the Communication area and select one of the following protocol options:
   • **Use IPv4** to manage device to manage the device using its IPv4 address.
   • **Use IPv6** to manage device to manage the device using its IPv6 address.

   Note: If you are editing the Network Management configuration and want to disable IPv4, use IPv6 to manage the network BEFORE you disable IPv4. If you are editing the Network Management configuration and want to disable IPv6, use IPv4 to manage the network BEFORE you disable IPv6.

3. For IPv4 Configuration:
   • **Enable IPv4** — Select this check box to configure the device management port with an IPv4 address.

     Important: If this check box is not selected, the IPv4 stack is disabled.

     • **IP Address** — Specify the IP (IPv4) address to assign to the device management port interface.
     • **Network Mask** — Specify the subnet mask to assign to the device management port interface.
     • **Default Gateway** — Specify the IP address of the route to use to send packets addressed to other networks.
• **Default Gateway Enabled** — Select this check box to assign the specified IPv4 default gateway to the device management port interface. Deselect this check box to disable gateway configuration.

**Important:** If this check box is not selected, the device and the SMS MUST be on the same subnet.

4. For IPv6 Configuration:

• **Enable IPv6** — Select this check box to configure the device management port with an IPv6 address.

**Note:** If this check box is not selected, the IPv6 stack is disabled.

• **Automatically configure network interface** — Select this check box use IPv6 stateless address auto configuration to assign IPv6 addresses to the management port.

• **Management Address** — Choose one of the following ways to manage the device:
  - **IP Address** — user-specified IPv6 address to the management port interface.
  - **Link-Local** — local IPV6 address assigned during network initialization. The SMS and the device MUST be on the same physical network.
  - **Auto** — local unicast address assigned during network initialization.

• **Default Gateway** — Specify the IP address of the route to use to send packets addressed to other networks.

• **Default Gateway Enabled** — Select this check box to assign the specified IPv6 default gateway to the device management port interface. Deselect this check box to disable gateway configuration.

**Important:** If this check box is not selected, the device and the SMS MUST be on the same subnet.

**Note:** If you do not select Use IPv6 address to manage this device, the IPv4 address or Public IP Address on the Management Information page is used to manage the device. See Management information on page 350.

5. Click **OK**.

**Editing the management port settings for the S-Series devices**

1. In the Device Configuration wizard, click **Management Information**.

2. On the Management Information screen, provide the following information:

   • **Name** — Specify or edit the name of the device.

   • **Location** — Specify device location.

3. On the Host Management Port section, enter the Network Mask.

4. On the Gateway and Routing section, do the following:

   a. Select the **Enabled** check box.
b. Enter the Default Gateway IP.

c. Enter the Destination IP, Subnet Mask, and Gateway IP.

5. Click **OK**.

### Management routes

Routing options enable the device to communicate with network subnets other than the subnet on which the Management Port is located. If you will manage your TippingPoint device from a different subnet, you will need to define a route between the subnet to which your workstation is connected and the subnet to which your TippingPoint Host Management Port is connected.

### NAT

Use NAT to minimize the number of internal IP addresses that are exposed to the Internet. NAT technology converts private IP addresses on an internal private network to one or more public IP addresses for the Internet. If you use a Network Address Translation (NAT), you can configure the setting on the NAT screen in the Device Configuration wizard.

**Note:** The NAT IP address is only saved on the SMS and is used when communicating with the device.

**Configure NAT**

1. On the Device Configuration wizard, click **NAT**.
2. To enable NAT, select **Enable**.
3. Enter the Public IP Address for the device.
4. Click **Apply**.
5. Click **OK**.

### Host IP filters

IP filters prioritize traffic and implement security policy. When you specify filter settings, you control system access by services that use the management port. Filter rules set to Deny affects the SMS management of the appliance.

### Services

On the Device Configuration (Services) screen, you can configure settings for system services. For Services, you can enable one or more remote services for secure connections. These services provide connections for the Command Line Interface (CLI) and Web (HTTPS). Each of these interfaces can be configured using non-secure communications (Telnet) for setup and debugging purposes, but you should not operate
the TippingPoint device using these non-secure options. During normal operations, you should use secure communications (SSH and HTTPS) to operate the CLI and the Web interfaces.

**Note:** HTTPS service is an integral service for the SMS, always enabled and available.

SSH and telnet require SuperUser access.

The Command Line Interface (CLI) can be accessed using either Telnet or SSH. Both of these access methods require client software. Although Telnet clients are more commonly distributed with some operating systems than with SSH clients, you should not configure the TippingPoint device to run the Telnet server during normal operations. Telnet communications are not secure, and a malicious party could intercept device user names and passwords.

⚠️ **Warning!** The Management Port Services options enable you to select a Telnet client when enabling the CLI. Telnet is not a secure service. If you enable Telnet, you endanger the security of your TippingPoint device. Use SSH instead of Telnet when enabling the CLI.

SSH provides secure remote access and Telnet does not. If you disable both SSH and Telnet, you cannot run or access the CLI.

For devices using V 2.1 or higher TOS, the system can use an encrypted channel for sending messages between the device and SMS. The encrypted channel polls the device according to the polling interval for the mode.

The Encrypted Alert Channel Settings option provides three modes:

- **Enabled Normal Mode** — Disables the SNMP traps and enables an SSL connection between the SMS and the device to transfer Alert messages reliably and securely by polling the device approximately every five seconds. This option is the default.

- **Enabled Batch Mode** — Disables the SNMP traps and enables an SSL connection between the SMS and the device to transfer Alert messages reliably and securely by polling the device according to a configured amount of minutes, which reduces network traffic slightly but increases the average time for the SMS to become aware of device Alerts.

- **Disabled (Use SNMP)** — Uses the existing SNMP trap mechanism.

**Table 99. Device Configuration (Services)**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSH</td>
<td>Secure connection for using the CLI. Requires a user with SuperUser capabilities.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Telnet</td>
<td>Unsecure connection for using the CLI. Requires a user with SuperUser capabilities.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Telnet is not supported on TPS devices.</td>
</tr>
<tr>
<td>HTTPS</td>
<td>Secure network communication for Web pages. Enabling HTTPS enables Web services for the SMS. See <em>TippingPoint SMS External Interface Guide</em>.</td>
</tr>
<tr>
<td>HTTP</td>
<td>Unsecure network communication connection for Web pages. Enabling HTTP enables Web services for the SMS. See <em>TippingPoint SMS External Interface Guide</em>.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> See <em>TSE Settings</em> on page 375 for HTTP mode on TPS devices.</td>
</tr>
<tr>
<td>Encrypted Alert Channel Settings</td>
<td>Compiles and sends alerts. Encrypted for security. You can disable this service to use SNMP.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Enable Normal Mode</strong> — Sends alerts as they are received</td>
</tr>
<tr>
<td></td>
<td>• <strong>Enable Batch Mode</strong> — Compiles alerts according to a configured <strong>Wait Time Interval</strong> (minutes ranging from 1 to 60). Enter an amount of minutes if selecting this option.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Disabled (Use SNMP)</strong> — Alerts are sent using SNMP, disabling this service.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> You must enable Encrypted Alert Channel if your profile’s Capture Additional Event Information setting includes HTTP. SNMP does not support HTTP context.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Encrypted Alert Channel settings are not supported on TPS devices or NGFW appliances.</td>
</tr>
<tr>
<td>Data Retrieval Service</td>
<td>Enables the SMS to retrieve and display traffic stats by port per device.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Data Retrieval Services only apply to IPS devices.</td>
</tr>
</tbody>
</table>
SNMP

Alerts are sent using SNMP. If your devices support both SNMP v2 and SNMP v3, you can configure the device to use one or both versions.

**Note:** To use SNMP v3 for NMS traps, you must configure Services for SNMP v3 or Both.

TLS Settings

Enable or disable the TLS versions (v1.0, v1.1, and v1.2) for a managed device.

**Note:** TLS Settings are only supported on TPS devices running TOS v4.1 or later.

**Services**

The services page allows you to configure whether specific services are enabled and whether a management service is provided through the network port or the management port.

You can enable one or more remote services for secure connections. These services provide connections for the Command Line Interface (CLI) and Web (HTTPS).

**Note:** HTTPS service is an integral service for the SMS, always enabled and available.

SSH requires SuperUser access.

The Device Configuration (Services) screen includes the following information:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSH</td>
<td>Secure connection for using the CLI. Requires SuperUser access.</td>
</tr>
<tr>
<td>HTTPS</td>
<td>Secure network communication for Web pages. Enabling HTTPS enables Web services for the SMS. See the <em>TippingPoint SMS External Interface Guide</em>.</td>
</tr>
<tr>
<td>Inband Mgmt.</td>
<td>Specifies that appliance management is done locally through the network itself.</td>
</tr>
<tr>
<td>DNS Lookup</td>
<td>Supplies the address or addresses that should be consulted for host name to IP address resolution.</td>
</tr>
<tr>
<td>Column</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>NTP Lookup</td>
<td>Designated primary SNTP Server.</td>
</tr>
<tr>
<td>RADIUS Lookup</td>
<td>Server for administrative login authentication and network user authentication.</td>
</tr>
<tr>
<td>LDAP Lookup</td>
<td>Server for administrative login authentication and network user authentication.</td>
</tr>
<tr>
<td>Remote Syslog</td>
<td>Sends filter alerts to a syslog server on your network. You can have one or more remote syslog servers.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Designating a remote system log server does not automatically send attack and shield notifications to that server. You must select the Remote System Log contact for action sets. After you apply these changes, active filters associated with the modified action set will send remote messages to the designated server.</td>
</tr>
<tr>
<td>Email Notifications</td>
<td>Server for email alerts.</td>
</tr>
</tbody>
</table>

**AFC settings**

Adaptive Filter Configuration (AFC) allows the Threat Suppression Engine (TSE) to manage filter behavior automatically when the SMS is under extreme load conditions due to filter failure and network congestion. Using adaptive filtering, the SMS can identify filters that are likely to cause network congestion and take action, based on a number of factors including filter settings and device configuration. You can configure managed devices to protect against the potential adverse effects of a defective filter. The SMS client shows filters that consume excessive resources and that are disabled on the Device Events screen in the Devices workspace.

Most filters provide configuration settings for adaptive filtering. If you do not want a filter to be subject to adaptive filtering, you can edit the filter and disable the adaptive filtering option. Filter settings that are relevant to adaptive filtering include filter category, AFC setting, and filter state:

- **Category** — Each filter category has a default adaptive filter configuration (AFC) setting for the entire group of filters. You can override the group setting for an individual filter by changing the Adaptive Configuration Setting for the filter.

- **AFC** — Individual filters contain Adaptive Configuration Settings that can be enabled or disabled. If AFC is disabled for particular filter, then that filter is never affected by adaptive filtering settings on the device.
• **State** — The TSE manages only filters that are enabled. Disabled filters do not affect network traffic and are not monitored for adaptive filtering.

In addition to filter settings, individual managed devices can be configured with Adaptive Filtering settings, including AFC Mode and AFC Event Severity.

AFC Mode determines whether the SMS is permitted to disable filters in the device profile automatically or whether the SMS leaves the filters enabled but generates a system message. In general the following options are available for AFC Mode:

• **Auto** — Enables the device to disable a defective filter automatically and generate a system message.

• **Manual** — Enables the device to generate a system message for the defective filter but does not automatically disable the filter.

The AFC Event Severity determines the severity of the system log message that is automatically generated when a filter triggers the Adaptive Filter function:

• Info

• Warn

• Error

• Critical

**HA (High Availability)**

You can use HA (High Availability) to configure settings for Intrinsic, Transparent, and Zero Power HA.

**Intrinsic HA**

Intrinsic HA determines how the device manages traffic on each segment in the event of a system failure.

• **Layer-2 Fallback (L2FB) mode** 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.

• **Normal mode** configures the device to inspect traffic according to the Threat Suppression Engine (TSE) settings.

A lack of reported errors or congestion through the TSE does not guarantee that the components receive correct and error-free traffic. The INHA monitors for several points of failure and applies failure detection logic against the system. All components for the Intrinsic HA are checked for failure.

The device performs the following checks to detect a failed condition and trigger a Layer-2 Fallback:

• Check back-pressure — Presence of back-pressure indicates packets are queued for processing. It indicates a failure if it does not process packets.

• Determine traffic requirements — If the device does not pass traffic, the ability to detect a failure is more difficult. A minimum rate of traffic must pass through the device for best failure detection.
• Handle non-atomic nature of the data path — Packet pass through each component at different times and rates. The status of each component is determined independently of each other. INHA uses sampling to determine health.

• Check and transmit the inbound receive counters — Each component has receive counters incremented by packets received from the previous component. The component transmits these counters incremented as packets to the next component. These counters are the most accurate and most complicated way of detecting health.

• Dropped packets exceeds threshold — If too many packets awaiting deep inspection are queued up, packets are dropped.

• Memory lows — Whether available system memory is too low for proper operations.

• Various chip set errors — Represents possible hardware problems.

Intrinsic HA monitors the device to detect hardware operating system failures and to automatically switch to the Layer-2 Fallback mode when a server outage or system failure is detected. You can

You can use the Layer-2 Fallback mode to permit or block all traffic according to the fallback settings for each device segment.

Transparent HA

Deploy Transparent HA in a redundant network configuration so that a partner device takes over in the event of system failure. Transparent HA partner devices constantly update each other with their managed streams information (blocked streams, trusted streams, and quarantined hosts). If a system failure occurs, interruptions to network protection are minimized because the partner device does not have to rebuild all of the current managed streams information.

**Important:** When Transparent HA is enabled, a hijacked partner device or a rogue device that impersonates the IP address of a Transparent HA partner device can communicate with the partner device.

When you configure TPS devices for Transparent HA, keep the following points in mind:

• Connect the following TPS devices:
  ◦ 440T devices, 2200T devices, or a mix of both. Connect 440T and 2200T devices by using the HA ports.
  ◦ 8200TX devices, 8400TX devices, or a mix of both. Connect 8200TX and 8400TX devices by using the management (MGMT) ports.

• TRHA requires the same TOS version on each TRHA device.

• THRA partners must be able to communicate with each other on TCP port 9591.

• On a TippingPoint Virtual Threat Protection System (vTPS) security device, Transparent HA is not supported.
After you configure TRHA, keep this point in mind:

- If you plan to change the global timeout interval on the connection table, be sure to update both partner devices. Transparent HA does not synchronize changes to the global timeout interval.

**Zero Power HA**

*Zero-Power High Availability (Zero Power HA)* ensures constant, non-interrupted flow of traffic. During a system outage, Zero Power HA bypasses the device and provides continuous network traffic. Configure Zero Power HA to determine how the device routes traffic in the event of a loss of system power:

- **Bypass mode** bypasses the Threat Suppression Engine (TSE) and maintains high availability of any network segments that have ZPHA support. When the device is in ZPHA bypass mode, any network segments that do not have Zero Power HA support are disconnected.

- **Normal mode** configures the device to inspect traffic according to the Threat Suppression Engine (TSE) settings.

Bypass is available for the IPS as an external modular device or as optional bypass I/O modules on NX-Platform and TX Series devices.

TPS device support for Zero Power HA varies by device:

- On a TippingPoint TX Series device, optional bypass I/O modules provide high availability for copper and fiber segments.

  **Note:** When you insert a bypass I/O module, by default the I/O module starts up in bypass mode.

- On a TippingPoint 2200T security device, Zero Power HA support is built-in for copper segments. An external Zero Power HA module is required to enable Zero Power HA on SFP and SFP+ segments.

- On a TippingPoint 440T security device, Zero Power HA support is built-in for copper segments only.

- On a TippingPoint Virtual Threat Protection System (vTPS) security device, Zero Power HA is not supported.

**Configure network HA**

For information on how to configure HA for firewall appliances, see *Create a device HA cluster* on page 425.

1. Select **Device Configuration > HA (High Availability)**.
2. To configure **Intrinsic HA**, do one of the following:
   - Select **Normal** to override all Intrinsic HA settings and configure the device to inspect traffic according to the Threat Suppression Engine (TSE) settings.
   - Select **Layer-2 Fallback** to permit or block all traffic according to the fallback settings.
   - Click **Apply**.
3. To configure **Transparent HA**, do the following:
   - Select the **Enable** check box to configure the device to constantly be updated with TCP flow information.
   - Select a **Partner Device** to configure Transparent HA.
   - Select the **Encrypt Traffic** check box to protect network traffic between the devices, and enter and confirm the **Passphrase**.

4. To configure **Zero Power HA** (enable/disable the Bypass Mode on an installed Bypass module), do the following:
   - **Note:** If the TPS TX Series device or IPS NX-Platform device does not have an installed BIOM, this option is not available.
   - Select **Normal** to configure the device to inspect traffic according to the TSE settings.
   - Select **Bypass IPS** to pass all network traffic regardless of the fallback configuration on each segment.
   - Click **Apply**.

5. Click **OK**.

**Enable and disable the bypass mode on an installed bypass module – TPS (TX Series) and IPS (NX-Platform)**

1. In the Device Configuration wizard, select **HA (High Availability)** from the navigation pane. The Device Configuration HA (High Availability) screen displays.
2. Choose the state for the installed bypass module.
   - **Note:** If the NX-Platform or TX Series security device does not have an installed BIOM, this option is not available.

**Performance Protection**

The Logging Mode section allows you to configure settings for alerts. On the Device Configuration (Logging Mode Settings) screen, you can enable or disable alerting of permitted and blocked packets. You have the option of setting the Logging Mode to **Always** or **Disable if congested**.

If you set the Logging Mode to **Disable if congested**, you can set the following logging options:
   - **Congestion Percentage** — percentage of congestion that must be met in order for logging to be disabled.
   - **Disable Time** — amount of time in seconds (between 60 and 3600 seconds) that logging will be disabled after the congestion percentage is met.
NMS

The settings for the NMS, including trap IP address, trap port, and community string. NMS is the protocol for monitoring the device by a restricted NMS, such as OpenView TM. On the Device Configuration (NMS) screen, you can enable applications to monitor your IPS device. You can create a new trap destination with the option to use SNMP v2 or SNMP v3, edit, or delete existing trap destination settings.

**Note:** The option to use NMS SNMP v3 is available only when editing the configuration for an N-Platform or NX-Platform IPS device running TOS v3.1 or later.

**Configure NMS settings for IPS (SNMP v2)**

1. In the Device Configuration wizard, select **NMS Settings** from the navigation pane.
   1. The Device Configuration (NMS Settings) screen displays.
2. Enter or edit a **Community String** (1-31 characters).
3. Click **New** for a new configuration or select an existing NMS listing, and then click **Edit** to change an existing configuration.
   1. The Create NMS Trap Destination dialog displays.
4. Enter the **IP Address** and the **Port** (port 162 is the default port) for the trap settings.
5. Click **OK** to return to the Device Configuration wizard.
6. Click **OK** to save your settings.

**Configure NMS for N-Platform or NX-Platform IPS (SNMP v3)**

**Important:** To use SNMP v3 for NMS traps, you must configure Services for SNMP v3 or Both.

1. In the Device Configuration wizard, select **NMS Settings** in the navigation pane.
   1. The Device Configuration (NMS Settings) screen displays.
2. Enter or edit a **Community String** (1-31 characters).
3. Click **New** for a new configuration or select an existing NMS listing, and then click **Edit** to change an existing configuration.
   1. The Create NMS Trap Destination dialog displays.
4. Enter the **IP Address** and the **Port** (port 162 is the default port) for the trap settings.
5. For the trap destination, select **SNMP v3**.
6. Enter the **Engine ID**, **User Name**, **Password**, and then **Verify Password**.
7. Select the **Privacy Protocol** from the drop-down box.
8. Click **OK** to return to the Device Configuration wizard.
9. Click **OK** to save your settings.

**SNMP settings**

Configure your device for Simple Network Management Protocol (SNMP) support. When SNMP is not enabled, an SSL connection between the SMS and the device transfers Alert messages reliably and securely. Alerts sent using SNMP can be encrypted if DES or AES is selected in the SNMP User Privacy settings.

Specify the properties for SNMP traps, users, and communities.

**Note:** To use SNMP v3 for NMS traps, you must configure Services for SNMP v3 or Both.

You can create multiple SNMPv2c communities to support NMS, IPs, or subnets. Each community can have multiple rules; however, the source IP address must be different. For example, you can create a rule for a Community named Public with a source IP address of 1.1.1.1. You can have a second rule for Public with a source IP address of 2.2.2.2.

After you enable SNMP, it might take a couple of seconds to start the SNMP demon. In the unlikely case of a collision with another device, you can change the Engine ID to a different value; however, the new value must be unique. Note that changing the Engine ID regenerates each read-only user, which affects connectivity.

**Note:** For S-Series, N-Platform/NX-Platforms, you must reboot the device for the SNMP settings to take effect.

**Log Configuration**

Use the Log Configuration screen to configure user encryption policy, specify your master key, and set the notification contact properties and threshold severities of audit, system, VPN and quarantine logs.

See the following topics:

- *View log* on page 301
- *Reset events/logs* on page 301

**Data Security – vTPS and TPS**

For vTPS 5.0 (and later) and TPS devices, use the Data Security screen to secure the system keystore with a new master key and to secure the external user disk (CFast or SSD).

(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.

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. The external user disk (CFast or SSD) stores all traffic logs, snapshots, ThreatDV URL Reputation Feed, User-defined URL Entries database, and packet capture data.
Before you encrypt the external user disk, keep in mind the following points:

- You cannot change the encryption status of external user disk on the vTPS.

- When you change the encryption status of the external user disk, the device automatically formats the disk and all data is 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.

**Remote syslog**

A remote syslog server is another channel that you can use to report filter events. Remote syslog sends filter alerts to a syslog server on your network. You can have one or more remote syslog servers.

**Note:** Designating a remote system log server does not automatically send attack notifications to that server. You must select the Remote System Log contact for action sets. After you apply these changes, active filters associated with the modified action set will send remote messages to the designated server.

Security devices that run TOS 3.6 or later can collect a client’s true IP address before it is overwritten by a forwarding proxy IP address. X-Forwarded-For and True-Client-IP technologies identify a request’s source IP address without administrators having to refer to proxy logs or Web server logs. When the **Additional Event Information** options are turned on, additional fields in the event logs display the True-Client-IP address and any HTTP URI information associated with the event. This visibility lets security teams set a more accurate network-based user policy.

If you intend to use Action Sets that include the Notify Remote Syslog option, you must create an entry for the devices to use. The system uses collectors for the settings. Collectors are specified by the required settings for the IP address and port, including options for a delimiter and facility numbers for alert messages, block messages, and misuse/abuse messages. The settings for the facilities are optional. Valid delimiters include horizontal tab, comma (,), semicolon (;), and bar (|). See **Profiles** on page 122.

The log format for the remote syslog includes changes detailed below. The following is an example of packet data sent to a collector. Make note that collectors might display the header portion of the stream differently.

```
<13>Jan 13 12:55:01 192.168.65.22 ALT,v4,20050113T125501+0360,"i robot"/192.168.65.22,1017,Alert,1,1,
00000002-0002-0002-0002-000000000164,"0164:
ICMP: EchoRequest (Ping)","0164: ICMP: Echo Request
(Ping)".icmp,216.136.107.233:0,216.136.107.91:0,20
050113T125205+0360,199,",1,3:1
```

In this example, the header follows the standard syslog format. Using the previous log entry as the example, the message is as follows:

```
ALT,v4,20050113T125501+0360,"i robot"/192.168.65.22,1017,Permit,1,Low,
```
The character located between each field is the configured delimiter. In this case, the delimiter is a comma. The following table details the fields and their descriptions.

**Table 100. Remote syslog fields and descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Log-type; ALT = alert, BLK = block, P2P = misuse and abuse</td>
</tr>
<tr>
<td>2</td>
<td>Version of this message format</td>
</tr>
<tr>
<td>3</td>
<td>ISO 8601 Date-Time-TZ when this alert was generated</td>
</tr>
<tr>
<td>4</td>
<td>Hostname/IP address that generated the alert; note that the quotes are required for this release because of a bug in the hostname validation (note the space in the name)</td>
</tr>
<tr>
<td>5</td>
<td>Sequence ID</td>
</tr>
<tr>
<td>6</td>
<td>(reserved)</td>
</tr>
<tr>
<td>7</td>
<td>Action performed (Block or Permit)</td>
</tr>
<tr>
<td>8</td>
<td>Severity (Low, Minor, Major, or Critical)</td>
</tr>
<tr>
<td>9</td>
<td>Policy UUID</td>
</tr>
<tr>
<td>10</td>
<td>Policy Name</td>
</tr>
<tr>
<td>11</td>
<td>Signature Name</td>
</tr>
<tr>
<td>12</td>
<td>Protocol name (icmp, udp, tcp, or unknown)</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td>13</td>
<td>Source address and port, colon delimited</td>
</tr>
<tr>
<td>14</td>
<td>Destination address and port, colon delimited</td>
</tr>
<tr>
<td>15</td>
<td>ISO 8601 Date-Time-TZ when the aggregation period started</td>
</tr>
<tr>
<td>16</td>
<td>Number of events since start of aggregation period</td>
</tr>
<tr>
<td>17</td>
<td>Traffic Threshold message parameters</td>
</tr>
<tr>
<td>18</td>
<td>Packet capture available on device (available = 1; none = 0)</td>
</tr>
<tr>
<td>19</td>
<td>Slot and segment of event</td>
</tr>
</tbody>
</table>

**Create/edit remote syslog servers**

1. In the Device Configuration wizard, select **Remote Syslog** from the navigation pane. The Device Configuration (Remote Syslog) screen displays.

2. Click **New** for a new configuration or select an existing listing, and then click **Edit** to change an existing configuration.

3. Specify an **IP Address** and **Port** for the remote server. The default port is 514.

4. Select an **Alert Facility** from the drop-down menu: none or select from a range of 0 to 31.

5. Select a **Block Facility** from the drop-down menu: none or select from a range of 0 to 31.

6. Select a **Delimiter** for the generated logs: **Horizontal Tab**, **Comma**, **Semi-colon**, or **Pipe**.

7. Click **OK**.

8. On the Device Configuration (Remote Syslog) screen, click **OK**

**Note:** When you click **OK**, the SMS restarts the segment, updating the hardware settings for the device and restarting the auto-negotiation process. If an error occurs, the copper cable translator might not support auto-negotiation. See **IPS port out-of-service** on page 678.
Servers

From the Device Configuration (Servers) screen, you can configure settings for DNS and email servers. Domain Name Service (DNS) supplies the address or addresses which should be consulted for host name to IP address resolution. Email server supplies the default email settings for email alerts.

Note: You must be sure that the device can reach the SMTP server that will be handling the email notifications. You might have to add a management route so that the device can communicate with the SMTP server.

Email server

Configure default email settings. You might have to configure a management route so that your appliance can communicate with the SMTP server that handles the notifications. Specify the following information:

- IP Address
- Domain Name (such as mail.com)
- From Email address (such as KSmith@mail.com). The email address setting is used as the sender address when the SMS sends alerts to notification contacts.
- Threshold which is the maximum emails per minute from 1 to 35 emails

Time settings

On the Device Configuration (Time Settings) screen, you view the current device time and configure the settings for how the system tracks time. A device comes with pre-defined time zone entries. Although system logs are kept in Universal Time (UTC), the SMS translates UTC time values into local time values for viewing purposes.

You must choose one of the following radio buttons:

- NTP Server (one server required when selected) — Establishes an NTP server to record accurate log file timestamp information. Adjust the polling period as necessary, optionally set an authorization key, and specify the hostname or IP address of the NTP server. NTP settings for a device remain even after the device is unmanaged and then remanaged.
- Remote SNTP Server — Sets the IPS to use an Simple Network Time Protocol (SNTP) server. You must define the Primary SNTP Server Address. Optionally, you can define a second server.

Note: This feature is not supported on TPS devices or NGFW appliances.

Note: We recommend that you use the SMS as your primary SNTP or NTP server. The SMS IP address is displayed at the bottom of the timekeeping panel.
Table 101. Device configuration (time settings)

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manual/Internal Device Time</td>
<td>The internal time for the device. You can set this time manually.</td>
</tr>
<tr>
<td>NTP Server</td>
<td>An NTP server is configured that optionally authenticates all time messages before they can be accepted as a time source.</td>
</tr>
<tr>
<td>Remote SNTP Server</td>
<td>A remote SNTP server for accessing the time for the device. Includes options for the primary and secondary server, duration in minutes, offset in seconds, port, timeout in seconds, and number of retries.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This feature is not supported on TPS devices or NGFW appliances.</td>
</tr>
<tr>
<td>Time Localization/Time Zone</td>
<td>Indicates the time zone for the device, including an option for daylight savings time.</td>
</tr>
</tbody>
</table>

**Configure the time options for TPS devices**

1. In the Device Configuration wizard, select **Time Settings** from the navigation pane. The Device Configuration (Time Settings) screen displays.

2. In the **Clock Source** section, select one of the following:
   - **Manual/Internal Device Time** — Sets the TPS to use its internal CMOS clock.
   - **NTP Server (one server required when selected)** — Sets the TPS to use an NTP server.

3. If you select **NTP Server (one server required when selected)**, do the following:
   a. Adjust the polling period as necessary (32 seconds is the default).
   b. You can optionally add authentication keys by clicking the **Auth Keys...** button and clicking **New** in the Authentication Keys window.
      A Key ID can be a number between 1 and 655535 that corresponds to a Key ID on a server. The Authentication Key value corresponds to an authentication key on an NTP server.
   c. To set up NTP Servers on the device, click **New** on the Time Settings page.
   d. Specify the hostname or IP address, version (1–3 for IPS devices), authentication preferences (optional), and whether the configured NTP sever is the preferred NTP server.
4. From the **Time Zone** section, select a location and respective city from the drop-down menus. 
5. Click **OK**.

**Configure the time options – IPS (N-Platform and NX-Platform)**

1. In the Device Configuration wizard, select **Time Settings** from the navigation pane. The Device Configuration (Time Settings) screen displays.
2. In the **Clock Source** section, select one of the following:
   - **Manual/Internal Device Time** — Sets the IPS to use its internal CMOS clock.
   - **NTP Server (one server required when selected)** — Sets the IPS to use an NTP server.
   - **Remote SNTP Server** — Sets the IPS to use an Simple Network Time Protocol (SNTP) server.
3. If you select **NTP Server (one server required when selected)**, do the following:
   a. Adjust the polling period as necessary. 
      The default is 16 seconds.
   b. You can optionally add authentication keys by clicking the **Auth Keys...** button and clicking **New** in the Authentication Keys window.
      A Key ID can be a number between 1 and 65535 that corresponds to a Key ID on a server. The Authentication Key value corresponds to an authentication key on an NTP server.
   c. Click **OK** to close the Authentication Keys window.
   d. To set up NTP Servers on the device, click **New** on the Time Settings page.
   e. Specify the hostname or IP address, version (1–3 for IPS devices), authentication preferences (optional), and whether the configured NTP server is the preferred NTP server.
   f. Click **OK**.
4. If you select **Remote SNTP Server**, do the following:
   a. To **Use the SMS as the Primary SNTP Server**, select the check box.
   b. Enter the **Primary SNTP Server Address**.
   c. Enter the **Secondary SNTP Server Address**.
   d. Enter a **Duration** amount in minutes.
   e. Enter an **Offset** amount in seconds.
   f. Enter a **Port**.
   g. Enter a **Timeout** amount in seconds.
   h. Enter the amount of **Retries**.
5. To enable daylight saving time, select the **Automatically adjust clock for daylight saving changes** check box.
6. From the **Time Zone** drop-down menu, you can choose from the following time zones:

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Offset from UTC (hours)</th>
<th>Daylight savings time</th>
<th>Time zone name</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACST</td>
<td>+9.5</td>
<td>OFF</td>
<td>AU Central Standard Time</td>
</tr>
<tr>
<td>AEST</td>
<td>+10</td>
<td>OFF</td>
<td>AU Eastern Standard/Summer Time</td>
</tr>
<tr>
<td>AKST</td>
<td>-9</td>
<td>OFF</td>
<td>Alaska Standard Time</td>
</tr>
<tr>
<td>AST</td>
<td>-4</td>
<td>OFF</td>
<td>Atlantic Standard Time</td>
</tr>
<tr>
<td>AWST</td>
<td>+8</td>
<td>OFF</td>
<td>AU Western Standard Time</td>
</tr>
<tr>
<td>CET</td>
<td>+1</td>
<td>OFF</td>
<td>Central Europe Time</td>
</tr>
<tr>
<td>CST</td>
<td>-6</td>
<td>OFF</td>
<td>Central Standard Time</td>
</tr>
<tr>
<td>EET</td>
<td>+2</td>
<td>OFF</td>
<td>Eastern Europe Time</td>
</tr>
<tr>
<td>EST</td>
<td>-5</td>
<td>OFF</td>
<td>Eastern Standard Time</td>
</tr>
<tr>
<td>GMT</td>
<td>0</td>
<td>OFF</td>
<td>Greenwich Mean Time</td>
</tr>
<tr>
<td>HST</td>
<td>-10</td>
<td>OFF</td>
<td>Hawaiian Standard Time</td>
</tr>
<tr>
<td>JST</td>
<td>+9</td>
<td>OFF</td>
<td>Japan Standard Time</td>
</tr>
<tr>
<td>KST</td>
<td>+9</td>
<td>OFF</td>
<td>Korea Standard Time</td>
</tr>
<tr>
<td>MSK</td>
<td>+3</td>
<td>OFF</td>
<td>Moscow Time</td>
</tr>
<tr>
<td>MST</td>
<td>-7</td>
<td>OFF</td>
<td>Mountain Standard Time</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Offset from UTC (hours)</td>
<td>Daylight savings time</td>
<td>Time zone name</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------------------</td>
<td>-----------------------</td>
<td>-------------------------------------</td>
</tr>
<tr>
<td>NZST</td>
<td>+12</td>
<td>ON</td>
<td>New Zealand Standard Time</td>
</tr>
<tr>
<td>PST</td>
<td>-8</td>
<td>OFF</td>
<td>Pacific Standard Time</td>
</tr>
<tr>
<td>WET</td>
<td>0</td>
<td>OFF</td>
<td>Western Europe Time</td>
</tr>
<tr>
<td>GMT-12</td>
<td>-12</td>
<td>OFF</td>
<td>Time zone GMT-12</td>
</tr>
<tr>
<td>GMT-11</td>
<td>-11</td>
<td>OFF</td>
<td>Time zone GMT-11</td>
</tr>
<tr>
<td>GMT-10</td>
<td>-10</td>
<td>OFF</td>
<td>Time zone GMT-10</td>
</tr>
<tr>
<td>GMT-9</td>
<td>-9</td>
<td>OFF</td>
<td>Time zone GMT-9</td>
</tr>
<tr>
<td>GMT-8</td>
<td>-8</td>
<td>OFF</td>
<td>Time zone GMT-8</td>
</tr>
<tr>
<td>GMT-7</td>
<td>-7</td>
<td>OFF</td>
<td>Time zone GMT-7</td>
</tr>
<tr>
<td>GMT-6</td>
<td>-6</td>
<td>OFF</td>
<td>Time zone GMT-6</td>
</tr>
<tr>
<td>GMT-5</td>
<td>-5</td>
<td>OFF</td>
<td>Time zone GMT-5</td>
</tr>
<tr>
<td>GMT-4</td>
<td>-4</td>
<td>OFF</td>
<td>Time zone GMT-4</td>
</tr>
<tr>
<td>GMT-3</td>
<td>-3</td>
<td>OFF</td>
<td>Time zone GMT-3</td>
</tr>
<tr>
<td>GMT-2</td>
<td>-2</td>
<td>OFF</td>
<td>Time zone GMT-2</td>
</tr>
<tr>
<td>GMT-1</td>
<td>-1</td>
<td>OFF</td>
<td>Time zone GMT-1</td>
</tr>
<tr>
<td>GMT+1</td>
<td>+1</td>
<td>OFF</td>
<td>Time zone GMT+1</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Offset from UTC (hours)</td>
<td>Daylight savings time</td>
<td>Time zone name</td>
</tr>
<tr>
<td>--------------</td>
<td>------------------------</td>
<td>-----------------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>GMT+2</td>
<td>+2</td>
<td>OFF</td>
<td>Time zone GMT+2</td>
</tr>
<tr>
<td>GMT+3</td>
<td>+3</td>
<td>OFF</td>
<td>Time zone GMT+3</td>
</tr>
<tr>
<td>GMT+4</td>
<td>+4</td>
<td>OFF</td>
<td>Time zone GMT+4</td>
</tr>
<tr>
<td>GMT+5</td>
<td>+5</td>
<td>OFF</td>
<td>Time zone GMT+5</td>
</tr>
<tr>
<td>GMT+6</td>
<td>+6</td>
<td>OFF</td>
<td>Time zone GMT+6</td>
</tr>
<tr>
<td>GMT+7</td>
<td>+7</td>
<td>OFF</td>
<td>Time zone GMT+7</td>
</tr>
<tr>
<td>GMT+8</td>
<td>+8</td>
<td>OFF</td>
<td>Time zone GMT+8</td>
</tr>
<tr>
<td>GMT+9</td>
<td>+9</td>
<td>OFF</td>
<td>Time zone GMT+9</td>
</tr>
<tr>
<td>GMT+10</td>
<td>+10</td>
<td>OFF</td>
<td>Time zone GMT+10</td>
</tr>
<tr>
<td>GMT+11</td>
<td>+11</td>
<td>OFF</td>
<td>Time zone GMT+11</td>
</tr>
<tr>
<td>GMT+12</td>
<td>+12</td>
<td>OFF</td>
<td>Time zone GMT+12</td>
</tr>
</tbody>
</table>

**Note:** The device keeps internal time information in Coordinated Universal Time (UTC) format. Log messages and other timestamp information is translated from UTC to the local time zone that you configure using timekeeping options.

7. Click **OK**.

**TSE settings**

The Device Configuration (TSE Settings) screen allows you to configure the global settings for the Threat Suppression Engine (TSE).

For information on monitoring TSE events, see *Events summary* on page 295.
You can configure the global settings for the Threat Suppression Engine (TSE). These options include the following:

- **Connection Table Timeout** — The value for the global connection table timeout. This value is 30-1800 seconds. This value applies to all blocked streams in the connection table, and determines the amount of time that elapses before that connection is cleared from the connection table. Before that period of time elapses, any incoming packets for that stream are blocked at the box. After the connection is cleared, the incoming connection is allowed (if its action set has changed) or re-added to the blocked list. Separate settings are available for TCP and non-TCP traffic.

- **Trusted Streams** — Specifies the global timeout interval for the trust table. This value determines the time interval that elapses before the trusted connection is cleared from the trust table.

- **Asymmetric Network** — The dynamic sharing and use of bandwidth for increased network traffic performance. If you configure the device through the TSE configuration for an asymmetric network, the SYN flood detection, or DDoS filters, will be disabled. In effect, the TSE will not see both sides of a TCP connection.

- **Quarantine** — Specifies the global timeout for the quarantine table. For quarantined hosts in the quarantine table, this value determines the time interval that elapses before the quarantined host is cleared from the quarantine table. After the quarantined host is cleared (the timeout interval expires), quarantined addresses can be automatically released, if that option is selected.

  **Note:** If you unmanage and then remanage a device, the quarantine settings are reset to the default values.

- **GZIP Decompression** — When enabled, permits decompression of GZIP HTTP responses.

- **IDS Mode** — When enabled, automatically configures the device to operate in a manner similar to an Intrusion Detection System (IDS).
  - Performance protection is disabled.
  - Adaptive Filtering mode is set to Manual.
  - Filters currently set to Block are not switched to Permit, and Block filters can be still be set.

  **Note:** You must reboot the device for the change to take effect.

- **HTTP Response Processing** — Specifies inspection of encoded HTTP responses.
  - **Accelerated inspection of responses**: Hardware acceleration is used to detect and decode encoded HTTP responses.
  - **Inspection of responses**: Enables strict detection and decoding of encoded HTTP responses.
  - **Ignore responses**: The device does not detect or decode encoded HTTP responses.

  **Note:** Some of these options are only available on TPS devices and IPS devices running specific TOS 3.2.x versions.
• DNS Reputation

Note: Some of these options are only available on TPS devices and IPS devices running specific TOS 3.2.x versions.

HTTP Mode

Note: Some of these options are only available on TPS devices and IPS devices running specific TOS 3.2.x versions.

Authentication preferences

For managed TPS devices and IPS devices running TOS v.3.3 and later, the SMS supports user authentication for individual devices.

From the Device Configuration screen for a managed device, you can set the following user authentication preferences:

• **Security Level** — None (level 0), Low (level 1), Medium (level 2), or High (level 3).
• **Maximum Login Attempts** — Login attempts from 1 to 10.
• **Failed Login Action** — Disable account and/or lockout IP address, lockout account and/or IP address account (default setting), or audit event.
• **Lockout Time** — Lockout time from 1 to 1440 minutes.

Local Authentication Only

The SMS stores a hashed password for the user account and authenticates against a user database stored locally on the TPS device.

Note: This option only appears on TPS devices. For IPS devices, see Authentication preferences on page 377.

The following password expiration options apply to accounts that are configured for local authentication only:

• **Password Expiration** — The minimum expiration period is 10 days, and the maximum expiration period is one year.
• **Password Expiration Action** — Force user to change password; notify user of expiration; or deny login, SuperUser must reset password.

Note: You cannot disable the password expiration for a Threat Protection System (TPS) device; therefore, Disabled is not available as an option.
Configure administrative login privileges

You can assign administrative login privileges to any remote authentication group. Users within that group can then change configuration settings. The Administrative login group can be chosen from one of the following remote authentication groups:

- RADIUS Groups
- LDAP Groups
- TACACS+ Groups

1. Select Devices > All Devices > device-name > Authentication.
2. In the Remote Authentication panel, click Edit.
3. In the Remote Authentication dialog, select the Administrative Login check box.
4. Select the group that you want to assign administrative privileges to and click OK.

Remote authentication configuration

Use the Remote Authentication page to configure remote authentication groups, servers, and administrative login privileges.

Specify one or more RADIUS groups and servers for TPS

For TPS devices, you can create and edit up to two RADIUS groups composed of six servers each for remote authentication.

1. Select Devices > All Devices > device-name > Authentication.
2. In the RADIUS Groups panel, click New.

   The Edit RADIUS Group dialog is displayed.

3. Configure the RADIUS Group Settings options described in the following table.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Group Name</td>
<td>Name of the RADIUS group.</td>
</tr>
<tr>
<td><strong>Note:</strong> 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.</td>
<td></td>
</tr>
<tr>
<td>Default User Group</td>
<td>Select between administrator, operator, or superuser.</td>
</tr>
</tbody>
</table>
### Setting | Description
--- | ---
Server Retries | Number of times between 0–3 that communication with the RADIUS server is attempted. The default is 1 (no retries after first unsuccessful attempt to contact RADIUS server).

Authentication Protocol | Authentication method used on the RADIUS server:
- PAP
- MD5
- PEAP/EAP-MSCHAPv2

**Note:** To use the PEAP/EAP-MSCHAPv2 protocol, you must first import an X509 certificate for the RADIUS server.

Security Certificates | Click **Manage Certificates** to specify a CA certificate. You can import a certificate or choose a previously imported one from the SMS certificate repository. For more information about certificate management, see Viewing certificates on page 568.

4. In the RADIUS Servers panel, click **New** to configure the RADIUS server options described in the following table.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname/IP Address</td>
<td>IP address or hostname of the RADIUS server. The IP Address field can contain an IPv4, IPv6, or named IP address. The Hostname field can contain an unqualified hostname or a fully qualified hostname (hostname+domain name).</td>
</tr>
<tr>
<td>Server Port</td>
<td>Port on the RADIUS server that listens for authentication requests; the default is port 1812.</td>
</tr>
<tr>
<td>Shared Secret/Confirm Secret</td>
<td>String used to encrypt and sign packets between RADIUS clients and the RADIUS server, set in the RADIUS client configuration file.</td>
</tr>
<tr>
<td>Server Timeout</td>
<td>Timeout, in seconds, for communication with the RADIUS server. Default is 2.</td>
</tr>
</tbody>
</table>
Setting | Description
---|---
NAS Id | Network access server identifier. This attribute of the RADIUS server is composed of a string that identifies the NAS that originated the Access-Request packet.

5. Test the RADIUS configuration by entering a valid User Name and Password for the server and then clicking Test.

6. Click OK to save the server configuration as an authentication preference.

**Note:** An X509 certificate is required for validating PEAP/EAP-MSCHAPv2 authentication responses. The certificate is generated on the RADIUS server, and must be imported to the SMS. The SMS server accepts DER (binary) or PEM (Base64) encoded X509 certificates. Invalid certificates, including expired and revoked certificates, can still be used according to the administrator’s discretion.

The configured server is displayed in the RADIUS Servers panel of the dialog. Click Move Up or Move Down to change the priority of the servers.

You can also change the configuration of RADIUS servers by selecting Admin > Authentication and Authorization > Authentication > Authentication Configuration > RADIUS.

**Specify one or more LDAP groups and servers for TPS**

For TPS devices, you can create and edit up to two Lightweight Directory Access Protocol (LDAP) groups composed of six servers each for remote authentication.

1. Select Devices > All Devices > device-name > Authentication.

2. In the LDAP Groups panel, click New.

   The Edit LDAP Group dialog is displayed.

3. Configure the LDAP Group Settings options.
   a. Under the General tab, configure the general LDAP properties described in the following table.
### Setting | Description
---|---
LDAP Version | Select between Version 2 or Version 3.
**Note:** Although an LDAP 2 client can connect to an LDAP 3 server, communication between the two might not occur if LDAP 3 features are required by the server.

LDAP Schema | Select from industry-standard schema for your directory server or click **Edit** to customize your own schema.

Bind DN for Authentication/Password/Confirm | The bind user on the directory server that enables the SMS to query the LDAP directory.

Base DN of tree to search | Distinguished name tree to search for directory entries.

Optionally configure TLS, encryption, and X.509 certificate validation by selecting those checkboxes.

b. Under the Servers tab, configure the LDAP server properties described in the following table.

### Setting | Description
---|---
Server Port | Port on the LDAP server that listens for authentication requests; the default is port 389, or 636 if SSL is enabled.

Server Retries | Number of times between 0–3 that communication with the LDAP server is attempted. The default is 1 (no retries after first unsuccessful attempt to contact LDAP server).

Server Timeout | Timeout, in seconds, for communication with the LDAP server; the default value is 2 seconds.

In the LDAP Servers panel, click **New** to configure the hostname and IP address of a LDAP server that you want to add. The configured server is displayed in the LDAP Servers panel of the dialog. Click **Move Up** or **Move Down** to change the priority of the servers.
Specify one or more TACACS+ groups and servers for TPS

For TPS devices, you can create and edit up to two TACACS+ groups composed of six servers each for remote authentication.

1. Select Devices > All Devices > device-name > Authentication.
2. In the TACACS+ Groups panel, click New.

   The Edit TACACS+ Group dialog is displayed.

3. Configure the TACACS+ Group Settings options described in the following table.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Group Name</td>
<td>Name of the TACACS+ group.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The name you provide for each group cannot be changed. To give a</td>
</tr>
<tr>
<td></td>
<td>group a new name, you must delete the group and re-create it with the new</td>
</tr>
<tr>
<td></td>
<td>name.</td>
</tr>
<tr>
<td>Default User Group</td>
<td>Select between administrator, operator, or superuser. The default is operator.</td>
</tr>
<tr>
<td>Server Retires</td>
<td>Number of times between 0–3 that communication with the TACACS+ server is</td>
</tr>
<tr>
<td></td>
<td>attempted. The default is 1 (no retries after first unsuccessful attempt to</td>
</tr>
<tr>
<td></td>
<td>contact TACACS+ server).</td>
</tr>
<tr>
<td>Authentication</td>
<td>Authentication method used on the TACACS+ server:</td>
</tr>
<tr>
<td>Protocol</td>
<td>• ASCII</td>
</tr>
<tr>
<td></td>
<td>• PAP (default)</td>
</tr>
<tr>
<td></td>
<td>• CHAP</td>
</tr>
</tbody>
</table>

4. In the TACACS+ Servers panel, click New to configure the TACACS+ server options described in the following table.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname/IP Address</td>
<td>IP address or hostname of the TACACS+ server. The IP Address field can contain an IPv4, IPv6, or named IP address. The Hostname field can</td>
</tr>
<tr>
<td></td>
<td>contain an unqualified hostname or a fully qualified hostname (hostname+domain name).</td>
</tr>
<tr>
<td>Setting</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Server Port</td>
<td>Port, between 1 and 65535, on the TACACS+ server that listens for authentication requests; the default is port 49.</td>
</tr>
<tr>
<td>Shared Secret/Confirm</td>
<td>Case-sensitive string used to encrypt and sign packets between TACACS+ clients and the TACACS+ server, set in the TACACS+ client configuration file. Maximum is 64 characters.</td>
</tr>
<tr>
<td>Shared Secret/Confirm</td>
<td>Case-sensitive string used to encrypt and sign packets between TACACS+ clients and the TACACS+ server, set in the TACACS+ client configuration file. Maximum is 64 characters.</td>
</tr>
<tr>
<td>Server Timeout</td>
<td>Timeout, between 1 and 15 seconds, for communication with the TACACS+ server. Default is 15.</td>
</tr>
</tbody>
</table>

5. Test the TACACS+ configuration by entering a valid User Name and Password for the server and then clicking Test.

6. Click OK to save the server configuration as an authentication preference.

The configured server is displayed in the TACACS+Servers panel of the dialog. Click Move Up or Move Down to change the priority of the servers.

You can also change the configuration of TACACS+ servers by selecting Admin > Authentication and Authorization > Authentication > Authentication Configuration > TACACS+.

**Remote Authentication**

**Note:** This page is only available on IPS devices running specific TOS 3.2.x versions.

In the Remote Authentication page, you can specify the source that the managed device uses to authenticate users.

- **Local** — The SMS stores a hashed password for the user account and authenticates against a user database stored locally on the IPS device.

- **SMS as Authentication Source** — The SMS is responsible for user authentication. If you choose to use SMS as the authentication source, specify the **Time Out Interval** (in number of seconds).

- **RADIUS as Authentication Source** — Authentication is performed on the RADIUS server; user role and access rights are maintained on the SMS server. You can specify up to three RADIUS servers. Note that user management remains on the device.

- **TACACS+ as Authentication Source** — Authentication is performed on the TACACS+ server; user role and access rights are maintained on the SMS server. You can specify up to three TACACS+ servers. Note that user management remains on the device.

**Note:** RADIUS authentication is supported on N-Platform and NX-platform devices running TOS v3.7.0 or later and all TPS and vTPS devices. If the device does not support RADIUS authentication, the
RADIUS options are disabled. TACACS+ authentication is supported only on TPS and vTPS devices running TOS v5.0.0 or later, and N-Platform and NX-platform devices running TOS v3.8.0 or later. If the device does not support TACACS+ authentication, this option is disabled.

Specify one or more RADIUS servers for IPS

1. On the Device Configuration Authentication Preferences screen, select the RADIUS as Authentication Source option in the Remote Authentication section.

2. In the RADIUS Servers section, click Edit next to the Primary, Secondary, or Tertiary Server IP.

3. In the RADIUS Server Configuration dialog, configure the RADIUS server options described in the following table.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>IP address of the RADIUS server.</td>
</tr>
<tr>
<td>Port</td>
<td>Port on the RADIUS server that listens for authentication requests; the default is port 1812.</td>
</tr>
<tr>
<td>Authentication Protocol</td>
<td>Authentication method used on the RADIUS server:</td>
</tr>
<tr>
<td></td>
<td>• PAP (default)</td>
</tr>
<tr>
<td></td>
<td>• MD5</td>
</tr>
<tr>
<td></td>
<td>• PEAP/EAP-MSCHAPv2</td>
</tr>
<tr>
<td></td>
<td>To use the PEAP/EAP-MSCHAPv2 protocol, you must first import an X509 certificate for the RADIUS server.</td>
</tr>
<tr>
<td></td>
<td>You can import a certificate now, or if you have already imported a certificate into the SMS certificate repository, simply choose the one you want. For more information about certificate management, see Viewing certificates on page 568.</td>
</tr>
<tr>
<td>Secret/Confirm Secret</td>
<td>String used to encrypt and sign packets between RADIUS clients and the RADIUS server, set in the RADIUS client configuration file.</td>
</tr>
<tr>
<td>Timeout</td>
<td>Timeout, in seconds, for communication with the RADIUS server. Default is 3.</td>
</tr>
<tr>
<td>Attempts</td>
<td>Number of times communication with the RADIUS server is attempted. The default is 1 (no retries after first unsuccessful attempt to contact RADIUS server).</td>
</tr>
</tbody>
</table>
Note: An IPS device that is managed by the SMS cannot have more than one RADIUS server configured with duplicate IP address, port, and authentication protocol settings.

4. Test the RADIUS configuration by entering a valid User Name and Password for the server (and confirming), and then clicking Test.

5. Click OK to save the server configuration as an authentication preference.

Note: To save the server configuration to the SMS and to the device, you must click OK on the Device Configuration wizard.

An X509 certificate is required for validating PEAP/EAP-MSCHAPv2 authentication responses. The certificate is generated on the RADIUS server, and must be imported to the SMS. The SMS server accepts DER (binary) or PEM (Base64) encoded X509 certificates.

Note: Invalid certificates, including expired and revoked certificates, can still be used according to the administrator’s discretion.

Import an X509 certificate

1. On the RADIUS tab, click Import to the right of the Primary RADIUS Certificate panel.
2. Select the X509 certificate file from your local drive or storage media, and click Import.

To clear the current certificate, click Reset.

Important: A certificate import or reset does not get saved until the entire device configuration is saved by clicking OK on the Device Configuration wizard.

Specify one or more TACACS+ servers for IPS

1. On the Device Configuration Authentication Preferences screen, select the TACACS+ as Authentication Source option in the Remote Authentication section.
2. In the TACACS+ Servers section, click Edit next to the Primary, Secondary, or Tertiary Server IP to configure a TACACS+ server.
3. In the TACACS+ Server Configuration dialog, configure the TACACS+ server options described in the following table.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address / Hostname</td>
<td>IP address or hostname of the TACACS+ server. The IP Address field can contain an IPv4, IPv6, or named IP address. The Hostname field can contain an unqualified hostname or a fully qualified hostname (hostname+domain name).</td>
</tr>
</tbody>
</table>
### Setting | Description
---|---
Port | Port, between 1 and 65535, on the TACACS+ server that listens for authentication requests; the default is port 49.
Authentication Protocol | Authentication method used on the TACACS+ server:
- ASCII
- **PAP** (default)
- **CHAP**
- **MSCHAP**
Secret/Confirm Secret | Case-sensitive string used to encrypt and sign packets between TACACS+ clients and the TACACS+ server, set in the TACACS+ client configuration file. Maximum is 63 characters.
Timeout | Timeout, between 1 and 15 seconds, for communication with the TACACS+ server. Default is 15.
Attempts | Number of times, between 1 and 10, communication with the TACACS+ server is attempted. Default is 3 attempts.

**Note:** An IPS device that is managed by the SMS cannot have more than one TACACS+ server configured with duplicate IP address, port, and authentication protocol settings.

4. Test the TACACS+ configuration by entering a valid User Name and Password for the server, and then clicking **Test**.
5. Click **OK**. This saves the server configuration changes to the Device Configuration dialog only.

**Important:** To save any of the device configuration changes you just made, you must click **OK** on the Device Configuration wizard.

### sFlow®
TPS devices running TOS v5.0.0 or later and NX-Platform devices support export of flow data statistics for visualization and analysis based on the sFlow technology standard. Statistics and flow data summaries can be viewed and analyzed by the SMS. The information can be used with external visualization and Network Behavior Anomaly Detection (NBAD) solutions to help identify compromised hosts and other suspicious and malicious network traffic.
When sFlow is enabled, it samples the packets on a segment and sends the data as a UDP packet to one or more servers. Port 6343 is the default sFlow collector port. You can send sFlow monitoring data from a device to one or more sFlow servers, including the SMS Collector. To start receiving sFlow data at a server, sFlow must also be enabled on one or more physical segments. The sampling rate is also set on each individual segment.

The SMS has the ability to auto-configure the sampling rate on the devices to maintain optimal SMS performance. When sFlow data is first collected, the SMS establishes a resource performance threshold by measuring the amount of disk space used by incoming sFlow data to be processed. If the threshold is exceeded and then increases again with a subsequent measurement, the sFlow sample rate gets cut in half on all segments. If another higher threshold is exceeded, the SMS automatically turns off the sFlow Collector. When performance stabilizes below the initial threshold, the sFlow Collector automatically turns back on. If necessary, the SMS Collector can be manually disabled and enabled using the `service sflowd stop` and `service sflowd start` commands, respectively.

**Note:** The option to use sFlow is available only when editing the configuration for an NX-Platform IPS system that is running TOS v3.6 or later and a TPS system running TOS v5.0.0 or later. vTPS devices do not support sFlow sampling. If there are no devices configured for sFlow sampling, the following warning message is displayed at the bottom of the Reports panel:

Currently there are no devices configured with the SMS as an sFlow® Collector. There may still be historical results.

### Create sFlow® collector

1. In the Device Configuration wizard, select **sFlow** from the navigation pane.

   The Device Configuration (sFlow) screen displays.

2. Check the **Enabled** checkbox to enable an sFlow data report to be sent to a collector.

   You must enable sFlow on at least one physical segment before sFlow data can be received at a collector.

3. Specify up to two sFlow collector servers for report analysis:

   - **SMS Collector.** Selecting this collector automatically populates the IP address of the SMS and the default collector port (6343). The generated sFlow reports are displayed on the Dashboard.

     **Note:** The SMS Collector server automatically adjusts the device sampling rate as required to maintain optimal SMS performance.

   - **External collector.** Specify the IP address and the port (default is 6343). Use this option if you require visualization and Network Behavior Anomaly Detection (NBAD), which is useful in identifying compromised hosts and suspicious network traffic.

   The SMS prompts you if an sFlow report is attempted without a configured collector server.

4. Click **OK** to return to the Device Configuration wizard.

5. Click **OK** to save your settings.
Device settings

Configure appliance-specific global settings, such as IDS and quarantine settings, timeout settings, asymmetric routing (DDoS filters cannot work if this feature is enabled), adaptive filter properties, and auto-reboot enablement.

You can configure the global settings for the following items:

- **Adaptive Filtering** — Set Adaptive Filtering Configuration (AFC) options that automatically manage your appliance under extreme load conditions and protect against the potential adverse effects of a defective filter. On rare occurrences, the system can experience extreme load conditions due to filter failure and traffic congestion, causing a device to enter High Availability (HA) mode. Adaptive filtering disables the filters that are likely causing traffic congestion.

- **Connection Table** — The value for the global connection table timeout. This value is 30-1800 seconds. This value applies to all blocked streams in the connection table, and determines the amount of time that elapses before that connection is cleared from the connection table. Before that period of time elapses, any incoming packets for that stream are blocked at the box. After the connection is cleared, the incoming connection is allowed (if its action set has changed) or re-added to the blocked list. Separate settings are available for TCP and non-TCP traffic.

- **Asymmetric Network** — The dynamic sharing and use of bandwidth for increased network traffic performance. If you configure the appliance through the TSE configuration for an asymmetric network, the SYN flood detection, or DDoS filters, will be disabled. In effect, the TSE will not see both sides of a TCP connection.

- **Quarantine** — Specifies the global timeout for the quarantine table. For quarantined hosts in the quarantine table, this value determines the time interval that elapses before the quarantined host is cleared from the quarantine table. After the quarantined host is cleared (the timeout interval expires), quarantined addresses can be automatically released, if that option is selected.

**Note:** If you unmanage an appliance and then remanage the appliance, the quarantine settings are reset to the default value.

- **IDS Mode** — When enabled, automatically configures the device to operate in a manner similar to an Intrusion Detection System (IDS).
  - Performance protection is disabled.
  - Adaptive Filtering mode is set to Manual.
  - Filters currently set to Block are not switched to Permit, and Block filters can be still be set.

Reboot your system for this setting to take effect.

- **Auto Reboot** — Specifies whether automatic reboots can be determined by the appliance.
Application visibility

Application visibility can be enabled or disabled. This feature allows you to see what applications are being used on your network using SMS. For more information on how the Application Visibility setting affects security zones, refer to the TippingPoint Next Generation Firewall Local Security Manager User Guide.

FIPS settings

If your device supports FIPS mode, you can allow management services for the device installed into a Federal Information Processing Standard (FIPS) Security Level 2 tamper-resistant hardware security module. When enabling FIPS mode on the device, review all the warning messages that display on the SMS.

FIPS settings for IPS devices

Table 102. FIPS settings for IPS devices

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>No FIPS compliance actions or restrictions are activated on the device.</td>
</tr>
<tr>
<td>Crypto</td>
<td>The device uses cryptographic libraries certified by the National Institute of Standards and Technology to be compliant with FIPS 140-2 publication. You must reboot the device for the system to operate in FIPS Cryptography mode.</td>
</tr>
<tr>
<td>Full</td>
<td>The SMS displays the Changing FIPS Mode wizard. Complete this wizard to enable full FIPS mode on the device. The SMS will delete all existing users on the device and will replace it with user defined in the wizard. The SMS will also rekey the device with a FIPS compliant key. For more information, see Enable FIPS on IPS device using SMS on page 390.</td>
</tr>
</tbody>
</table>

Note: You must reboot the device to completely enable or disable this service.
FIPS settings for TPS devices

Table 103. FIPS settings for TPS devices

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>No FIPS compliance actions or restrictions are activated on the device.</td>
</tr>
</tbody>
</table>
| FIPS Enabled| The device uses cryptographic libraries certified by the National Institute of Standards and Technology to be compliant with FIPS 140-2 publication. For more information, see *Enable FIPS on TPS device using SMS* on page 392. Important: You must factory reset the TPS device before you enable FIPS mode. To disable FIPS mode, you must factory reset the device. The following authentication settings are not supported on the TPS device:  
  • RADIUS  
  • TACACS+  
SNMP settings do not support MD5 and DES protocols when the TPS device is in FIPS mode. Important: The SMS must have a 2K key installed to communicate with the TPS device in FIPS mode. |

Enable FIPS on IPS device using SMS

Important: Before you can enable FIPS on a managed IPS device, you must make sure that FIPS mode is disabled on the SMS. If the SMS does have FIPS mode enabled, enable FIPS on the IPS device using the IPS CLI. Refer to the product document for your IPS device.

1. Manage the device from the SMS.
2. Right-click on the device from the All Devices page and select Edit > Device Configuration.
4. For FIPS Mode, select the Full radio button, and then click OK.
5. Click Next when the Changing FIPS Mode wizard is displayed.
6. Enter a username, enter and confirm your password, and then click Next.
7. Review your choices and click Finish.
   • If the SMS can communicate with the TMC, it will download and install the FIPS key package.
when it does, skip to Step 11.

• If the SMS cannot communicate with the TMC, the following error message instructs you to manually rekey the device:

![Error Message Image]

8. Close the message and download the FIPS key package from the TMC to your computer.

9. After the device completes rebooting, navigate to System > Update > Install Package in your device's LSM.

10. In Step 4 of the Install Package page, browse to your FIPS key package and click Install Package.

   If you receive the following error message, click OK, manually reboot the device, and repeat the previous two steps. The IPS should accept this second attempt to install the FIPS key package.
11. Verify that the device is in Full FIPS mode by doing any of the following:

- Enter `sh fips` in the CLI.
- From the SMS client, click the Device Configuration page for your device and view the **FIPS Mode** status under **Management Services**.

**Note:** If you see a **Socket Closed** SMS error message when trying to add an IPS in FIPS mode, run the `fips restore-ssl` command from the IPS CLI. After running this command, navigate to the **System > Update > Install Package** page of your device's LSM to reinstall the FIPS key package. This ensures that the IPS will use keys that meet FIPS strength requirements.

### Enable FIPS on TPS device using SMS

1. Manage the device from the SMS.
2. Right-click on the device from the All Devices page and select **Edit > Device Configuration**.
3. On the Device Configuration page, select **FIPS Settings**.
4. For **FIPS Mode**, select the **Enabled** check box.
5. Click **OK**.

### SSL Inspection

SSL inspection requires an SSL license update to be installed on the TPS or vTPS security device. If the device is not licensed for SSL inspection, the SMS displays a notification. Once you install a license that allows SSL inspection, you must reboot the device for it to take effect.

- **SSL License Status** — View the current SSL License status. If the checkbox is grayed, verify the license package allows SSL inspection. Click **View Installed License** to view a list of licensed capabilities for the device including the expiration date and details.
- **SSL Inspection** — Select this check box to enable the TPS or vTPS device to inspect SSL sessions.
- **Persist Private Keys** — Select this check box to store private keys for SSL server certificates on the device.
Packet trace – TPS and IPS (S-Series, N-Platform, and NX-Platform)

Packet trace is a useful tool that captures all or part of a suspicious packet for analysis. You can set the packet trace priority and packet trace verbosity for action sets.

You can perform the following tasks:

- Save all packet trace information for a device on page 393
- Download all packet trace files for a device to the SMS on page 393

Through the Devices screen, the SMS has the following right-click packet trace option for a selected device:

- **Save** — Opens a file chooser dialog where you can provide a location on the client system for saving all the packet trace information for the selected device. Packet trace files are merged into one PCAP file.
- **Download to SMS** — Downloads all the packet trace information for the selected device into the Exports and Archives section of the SMS client. When the download is complete, a popup message displays the location where the PCAP file was downloaded and provides an active HTML link to the files.

Packet trace options are available for devices that support the packet trace feature. Devices, such as the Core Controller and the SSL do not support packet trace. See *Save all packet trace information for a device* on page 393.

**Save all packet trace information for a device**

1. On the Devices (All Devices) screen, right-click a device in the graphics pane or right-click a device listing the table.
2. Select **Packet Traces (all)** and then the **Save** option to save all the packet trace information for the selected device.
3. Browse to the area where you want to save the packet trace information, and then click **Save**.

**Download all packet trace files for a device to the SMS**

1. On the Devices (All Devices) screen, right-click a device in the graphics pane or right-click a device listing the table.
2. Select **Packet Traces (all)** and then the **Download to the SMS** option to download all the packet trace information for the selected device.

**Replacing a device**

The SMS provides a convenient option that allows you to replace an existing device and have the new device function exactly the same as the old device. There are certain limitations based on the device features. For
example, if you replace an IPS device that supports DDoS with an IPS device that does not support DDoS, data might be lost or if the replacement IPS device has less segments than the original IPS device.

For a listing of device replacement models see Device replace table on page 420.

⚠️ Caution: Using the Device Replace option could result in data loss. Before using this feature, review all of the topics in this section and see Device replace table on page 420.

⚠️ Note: When you replace a device, the events from the previous device are preserved. However, previous installed TOS versions, rollback versions, and snapshots are reset using the new (replaced) device as a starting point.

This section contains the following topics:

- Device replacement limitations on page 394
- IPS device replacement considerations on page 396

Device replacement limitations

The device replace feature has the following limitation:

- TPS Devices:
  - A replacement device does not inherit device users. All device users must be added back manually.
  - You cannot replace FIPS Settings on the device.
- IPS N-Platform or NX-Platform Devices:
  - N-Platform or NX-Platform devices can replace any device, but might have data loss.
  - Only N-Platform or NX-Platform devices can replace other N-Platform or NX-Platform devices.
  - RADIUS authentication settings and servers remain only if the replacement devices support RADIUS authentication (N-Platform or NX-Platform devices running TOS v3.7.0 or later).
  - A replacement device does not inherit device users. All device users must be added back manually.
  - You cannot replace FIPS Settings on the device.
- Profile Distribution
  - Auto redistribution profiles is NOT supported.

Port configuration considerations

When you replace a device with another device that has a different port configuration, the SMS may attempt to push the port configuration for the old device to the new device. If this happens, unmanage the device, use the CLI or LSM to disable auto-negotiate for each port, and then remanage the device. You will need to redistribute any profile that was distributed to the device after you remanage it.
Table 104. Port configuration considerations

<table>
<thead>
<tr>
<th>Old Device</th>
<th>New Device</th>
<th>Device Replace Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPS (non-N-Platform)</td>
<td>IPS (non-NX-Platform)</td>
<td>No Change</td>
</tr>
<tr>
<td>IPS (non-NX-Platform)</td>
<td>IPS (NX-Platform)</td>
<td>All of the device configurations except for port configuration will be copied to the new device. The NX-Platform device I/O modules are very different from previous IPS devices.</td>
</tr>
<tr>
<td>IPS (NX-Platform)</td>
<td>IPS (NX-Platform)</td>
<td>All of the device configurations are copied to the new device if the I/O module types are the same. If the I/O module types are different, then the port configuration will not be copied.</td>
</tr>
<tr>
<td>IPS (NX-Platform)</td>
<td>TPS (TX Series)</td>
<td>All of the device configurations are copied to the new device if the I/O module types are the same. If the I/O module types are different, then the port configuration will not be copied.</td>
</tr>
<tr>
<td>IPS (NX-Platform)</td>
<td>TPS (TX Series)</td>
<td>All of the device configurations are copied to the new device if the I/O module types are the same. If the I/O module types are different, then the port configuration will not be copied.</td>
</tr>
<tr>
<td>TPS (TX Series)</td>
<td>TPS (TX Series)</td>
<td>All of the device configurations are copied to the new device if the I/O module types are the same. If the I/O module types are different, then the port configuration will not be copied.</td>
</tr>
</tbody>
</table>
IPS device replacement considerations

If you are replacing the same model with another model and both devices have the same TOS, the one-to-one replacement is straightforward. The following replacement options have specific issues to take into consideration:

- **Segments** on page 396
- **DDoS** on page 396
- **Different models** on page 396

See **Device replace table** on page 420.

Segments

Data loss occurs if the new device has fewer segments than the old device. For example, when a device with four segments is replaced by a device with two segments, events and settings related to the additional segments, if configured on the original device, are lost.

DDoS

Possible data loss occurs if the new device does not support DDoS and the old device is configured for DDoS.

Different models

- **New model cannot use same IP address as old model** If the old model is still online, you cannot use the same IP address and must choose a different one for the new model. If the TOS versions are not the same, you must upgrade to the newer version.

- After you upgrade your IPS device, you can give the old device and new IP Address and place it in another area of the network.

- **New model has more segments** Because the models are not the same and the new device has extra segments, the new segments are not configured. Extra segments are placed in the Default segment group.

- **New model has fewer segments** Because the models are not the same and the new device has fewer segments, the SMS cannot copy all segment/port setting to the new device. Therefore, the configuration of the common segments is copied and the remaining segment are dropped or removed from the SMS.

<table>
<thead>
<tr>
<th>Old Device</th>
<th>New Device</th>
<th>Device Replace Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>the same. If the I/O module types are different, then the port configuration will not be copied.</td>
</tr>
</tbody>
</table>

**Replace a device**

1. Review all of the topics in this section and the *Device replace table* on page 420.
2. Remove the new replacement IPS from the box and complete the Out of Box Experience (OBE) instructions using the old IPS address for the new one.

   **Tip:** If you name the IPS, use a similar name as the old IPS, such as MarketWest2 as the replacement for MarketWest1.

3. If the old model and new model are not the same and/or the TOS versions are different, refer to *IPS device replacement considerations* on page 396.
4. Log in to the SMS from the client.
5. On the All Devices screen, select the device to be replaced, and select **Edit > Details > Replace Device**.
6. After Devices - Replace Device dialog displays, enter the information for the new IPS device, and then click **OK**.

   If all of the supplied information is correct, the models are the same and the TOS versions are the same, a progress dialog appears. If the models or TOS versions are not the same, refer to the *IPS device replacement considerations* on page 396.

   When the replacement process is complete, a dialog appears and directs you to redistribute the appropriate versions of the IPS profiles.

**Advanced DDoS tasks**

This section includes the following topics:

- *Advanced DDoS supported models* on page 397
- *Advanced DDoS filter configuration* on page 398
- *DDoS preferences* on page 399

**Advanced DDoS supported models**

The SMS supports DDoS for the following devices:

- 660N/1200N/1400N/2500N/5100N (TOS 3.1.x through 3.6 and later)
- 5200NX/7100NX (TOS 3.5 and later)
- 2600NX/7500NX (TOS 3.6 and later)
Go to Devices to configure the following DDoS filter options:

- SYN Proxy Filter — Enable
- CPS Flood Filter — Enable, Threshold Settings
- Connection Flood Filter — Enable, Threshold Settings

The SYN Proxy Threshold setting for these devices is configured in the Profiles.

**Note:** The Advanced DDoS configuration options are set in the Profiles.

You can access this directly through the Devices, or when creating and editing filters through the Profiles. See *Advanced DDoS* on page 173.

### Advanced DDoS filter configuration

To view supported advanced DDoS filter configuration settings for devices, see *Table* on page 173.

#### Edit Advanced DDoS filters

1. On the *Devices navigation* pane, select the *Adv. DDoS Configuration* option for a TippingPoint Advanced DDoS supported models on page 397. The Advanced DDoS Device Settings screen displays and lists the current settings and any exceptions.
2. Click *Edit*.
3. The Edit Advanced DDoS Settings dialog displays.
   - For SYN Proxy, click the *Enable* check box. To configure the SYN Proxy Threshold, see *Create/edit a DDoS filter exception* on page 398.
   - For CPS Flood, click the *Enable* check box and enter a *Threshold* setting (1.0 to 100.0 range).
   - For Connection Flood, click the *Enable* check box and enter a *Threshold* setting (1 to 65536).
4. Click *OK*.

#### Create/edit a DDoS filter exception

1. In the *Devices navigation* pane, select the *Adv. DDoS Configuration* option for a TippingPoint Advanced DDoS supported models on page 397. The Advanced DDoS Device Settings screen displays and lists the current settings and any exceptions.
2. In the Exceptions area:
   - Click *Create* to create a new filter exception.
   - Select an exception from the list and click *Edit* to edit an existing exception.
The Filter - DDoS Create/Edit Exception dialog displays.

3. In the Filter - DDoS Create/Edit Exception dialog:
   a. Enter/edit a Name.
   b. Enter/edit a Source Address, and then select a format.

   **Note:** These instructions create hardware-based exceptions for *Advanced DDoS supported models* on page 397. To create software-based exceptions, see *Advanced DDoS* on page 173.

4. Click OK.

**DDoS preferences**

In the Device Configuration (TSE Settings) screen, the following DDoS setting are supported:

- Aggregate CPS alerts during attacks
- Aggregate connection flood alerts during attacks

When selected, these options cause the IPS to create a single log message for an attack of the corresponding type, rather than a log message for each packet that is blocked.

See *Advanced DDoS supported models* on page 397.

**Set DDoS preferences**

1. On the Devices > All Devices screen, select a device in the navigation pane.
2. On the Devices screen, click **Device Configuration**.
3. From the Device Configuration wizard panel menu, select **TSE Settings**.
4. On the Device configuration (TSE Settings) screen, make the desires changes. Available options include:
   - **Connection Table:** Timeout in seconds
   - **Asymmetric Network:** Enabled/Disabled
   - **Quarantine:** Release quarantine addresses automatically, Timeout in minutes
   - **DDoS:** Aggregate CPS and/or connection flood alerts during attacks
5. Click OK.

**SMS managed devices**

The SMS client supports the following TippingPoint devices:

*Threat Protection System devices* on page 400 — Protects your network with the Threat Suppression Engine (TSE) by scanning, detecting, and responding to network traffic according to the filters, action sets, and global settings maintained on each device by a client.
**V Series Threat Protection System** on page 403 — Software appliance designed to provide the same level of functionality available in the TippingPoint Threat Protection System (TPS), but virtually rather than physically.

**Intrusion Prevention System devices** on page 406 — Protect your network by scanning, detecting, and responding to network traffic according to filters, action sets, and global settings maintained on each device.

**Next Generation Firewall appliances** on page 412 — Monitor and control incoming and outgoing traffic.

**Core Controller** on page 413 — Controls traffic across its three 10GbE network segment pairs and across multiple TippingPoint devices.

**SSL appliance** on page 430 — Decrypts SSL traffic between clients and site servers and sends the decrypted traffic to an TippingPoint IPS device for analysis.

**TippingPoint vController** on page 414 — Secures network traffic in virtualized environments and is part of the TippingPoint Secure Virtualization Framework (SVF).

**Note:** For device specifications and rate limits, see the product hardware guide for your device.

### Threat Protection System devices

The TippingPoint Threat Protection System (TPS) is the latest offering in the comprehensive security suite of TippingPoint products.

The TPS family includes:

- **440T devices** on page 401
- **2200T devices** on page 401
- **TX Series devices** on page 401

Inspection throughput rates for TPS devices are determined by the inspection throughput license that is installed on the device. For more information, see **Licensing** on page 653.

For information about tier statistics for TPS devices, see **Tier statistics for the vTPS, TPS, and IPS (NX-Platform) devices** on page 409.

### Jumbo frame support

The TippingPoint Operating System supports inspection of jumbo frames up to 9050 bytes. This includes the 14-byte Ethernet header, 9032 bytes of payload data, and the 4-byte Ethernet checksum.

**Device support:** 440T, 2200T, 8200TX, and 8400TX

**Note:** This feature is not supported on vTPS devices.
440T devices

The 440T device protects your network with the Threat Suppression Engine (TSE) by scanning, detecting, and responding to network traffic according to the filters, action sets, and global settings maintained on each device. The TPS solution is optimized for high resiliency, high availability, and network segment protection from both external and internal attacks.

In addition, the 440T device includes:

- Built-in intrinsic high-availability features, guaranteeing continuity in the event of system failure
- Up to 1 Gbps aggregate across all four segments
- Device management through the Local Security Manager (LSM) or centralized management through the SMS

For additional information on the 440T device, refer to the TMC.

2200T devices

The 2200T device includes:

- Threat Suppression Engine (TSE) which scans, detects, and responds to network traffic according to the filters, action sets, and global settings maintained on each device
- Built-in bypass and intrinsic High Availability (HA) features, guaranteeing continuity in the event of system failure
- Up to 2 Gbps aggregate across all ten segments
- Onbox SSL decryption
- Device management through the Local Security Manager (LSM) or centralized management through the SMS

For additional information on the 2200T device, refer to the TMC.

TX Series devices

The TippingPoint TX Series TPS devices include:

- Threat Suppression Engine (TSE) which scans, detects, and responds to network traffic according to the filters, action sets, and global settings maintained on each device
- Built-in bypass and intrinsic High Availability (HA) features, guaranteeing continuity in the event of system failure
- Onbox SSL decryption
- Device management through the Local Security Manager (LSM) or centralized management through the SMS
- Support for up to four I/O modules enabling you to customize the device

For the 8200TX device, each installed module has an associated slot number from 1 to 2. Ports are organized by slots. For the 8400TX device, each installed module has an associated slot number from 1 to 4.

The following standard I/O modules are supported for the 8200TX and 8400TX security devices and are hot-swappable:

- TippingPoint 6-Segment Gig-T I/O module
- TippingPoint 6-Segment GbE SFP I/O module
- TippingPoint 4-Segment 10 GbE SFP+ I/O module
- TippingPoint 1-Segment 40 GbE QSFP+ I/O module

The following bypass I/O modules are supported for the 8200TX and 8400TX security devices and are hot-swappable:

- TippingPoint 4-Segment Gig-T Bypass module
- TippingPoint 2-Segment 1G Fiber SR Bypass module
- TippingPoint 2-Segment 1G Fiber LR Bypass module
- TippingPoint 2-Segment 10G Fiber SR Bypass module
- TippingPoint 2-Segment 10G Fiber LR Bypass module

**Note:** The 10G Fiber BIOMs have internal dual-rate SFP+ transceivers that can operate at either 10 Gbps (the default) or 1 Gbps speeds.

For the 10G Fiber bypass modules and 10 GbE I/O modules to operate at 1 Gbps speeds, explicitly set the line speed to 1 Gbps by using the CLI, LSM, or SMS. Auto-negotiation can also be selected at 1 Gbps, to match the link partner. To operate at 10 Gbps, auto-negotiation must be disabled on the 10G fiber bypass modules and 10 GbE I/O modules.

**Note:** A 40 Gigabit I/O module is hot-swappable with an existing 40 Gigabit I/O module. However, 40 Gigabit modules are not hot-swappable with a different module type. For example, a 10 Gigabit or 1 Gigabit I/O module cannot replace a 40 Gigabit I/O module without a performing a full reboot.

When the slot is empty, the ports or segments are not displayed. When a module is inserted, the SMS uses the current device configuration for the module. When a module is removed, the slot shows empty.

**Note:** Performing a hot-swap of I/O modules during system initialization is not supported.

The SMS supports TippingPoint Bypass I/O Modules (BIOM) which are designed for use with TX Series TPS devices. The bypass modules determine whether network traffic from a network system should be routed into the device or “looped back” to the module front panel and sent back out to the network system through the external port. System software determines if the module is in bypass or normal mode.
For information on installing and configuring BIOMs, see the TippingPoint Bypass Input/Output Module documentation.

**Note:** Network traffic is NOT scanned or blocked when the bypass I/O modules are used to bypass an IPS device.

To configure the bypass mode on a bypass I/O module, see *Enable and disable the bypass mode on an installed bypass module – TPS (TX Series) and IPS (NX-Platform)* on page 364.

**Virtual Threat Protection System**

The Virtual Threat Protection System (vTPS) is a software device designed to provide the same level of functionality available in the TippingPoint Threat Protection System (TPS), but virtually rather than physically.

TOS v4.0.1 and later of the vTPS supports the majority of features that were introduced with the 4.0.0 release of the 440T TPS device. For a list of TPS features that are not supported on vTPS devices, refer to the *Virtual Threat Protection System Functional Differences Addendum*.

For additional information on the vTPS device, refer to the TMC.

**Unsupported features**

All available features can be configured using the Local Security Manager (LSM) on each device, the device command line interface (CLI), or the SMS.

The following features that are supported in the physical TPS are not supported in the vTPS Standard device:

- **Port configuration** - The vTPS contains one management port and two data ports. The ports are not configurable and do not have the characteristics of a physical port, such as speed, duplex, or auto-negotiation.

- **High Availability (HA) deployments** - The vTPS does not support transparent HA (TRHA) or zero power HA (ZPHA). However, the vTPS does support Layer 2 Fallback.

- **Certain device information** - The Devices > All Devices screen does not display statuses or values for power supplies, fans, ZPHA, TRHA, or temperatures.

For more information, refer to the *Virtual Threat Protection System Functional Differences Addendum*.

**vTPS deployment and licensing**

In addition to the device license entitlement package (see *Licensing* on page 653 for more information), you must also install a license certificate package on a vTPS device before it deploys with the functionality that you purchased with your license package.
The vTPS device remains in Trial Mode until a valid license certificate is installed. The Trial Mode vTPS comes with limited feature capabilities. After a certificate is installed, the vTPS device deploys in Standard Mode, and the capabilities purchased with the license package are activated.

For more details on deploying a vTPS device, refer to the *vTPS Deployment Guide*.

vTPS certificate installation prerequisites

Before you assign a vTPS certificate to a vTPS device, complete the following items:

- Purchase an inspection throughput license through your regular sales channel. An inspection throughput license determines the processing speed of a device; it does not expire and can be attached or removed from any TPS device, including a vTPS device.
- Create the vTPS certificate using the Trend Micro TippingPoint License Manager. See *Create and download vTPS device license certificates* on page 404 for more information.

Create and download vTPS device license certificates

Use the following information to create a vTPS license certificate using the license manager. The license certificate package assigns a purchased inspection throughput license to a vTPS device. After you create a vTPS license certificate, install the certificate on the vTPS.

**To create a vTPS device license certificate**

1. Open the license manager.
   
   To access the license manager, go to the TMC, and navigate to *My Account > License Manager*.

2. From the License Management page of the license manager, click *Create vTPS Licenses*.
   
   The *Create vTPS Licenses* dialog opens.

3. (Optional) If you want to add SSL inspection to a vTPS device, but SSL is disabled, apply for SSL compliance.
   
   There are four states of SSL compliancy; Unknown, Pending, Compliant, and Non-Compliant. Before SSL is enabled, the SSL compliance state is set at Unknown.

   Complete the following steps to apply for SSL compliance:

   a. Next to *Your SSL is disabled*, click *Apply Now*.
   b. Fill out the Apply for SSL Compliance page.
   c. Click *Apply*.

   After you click *Apply*, the SSL compliance state changes to Pending. When the application process is completed, the state will either change to Compliant if SSL is approved or Non-Compliant if SSL is not approved.

   If you are SSL Compliant, SSL inspection is enabled on all of your vTPS devices.
4. Under **Action**, select the number of vTPS certificates that you want to create.

5. Click **Create**.

After the vTPS certificate is created, use the SMS or LSM to install the certificate to a vTPS device.

**Important:** If you do not use an SMS or if your SMS is not connected to the TMC, you must manually download and install the vTPS certificate package. After you download the vTPS certificate package, you can manually install the package from the SMS or LSM.

**To download the vTPS certificate package**

1. In the license manager, click **Download Cert**.
2. Select **vTPS Cert** from the drop down options.

   The vTPS Certificate Package page displays on the TMC.

3. Click **Download**.
4. Accept the EULA Agreement.
5. Save the vTPS certificate file to a local folder.

**To install the vTPS license certificate using the SMS**

Complete the following steps to install a vTPS certificate on a vTPS device using the SMS.

1. Ensure that the vTPS device is managed by the SMS.
2. In the SMS client, navigate to the Devices workspace.
3. Right-click on the appropriate vTPS device in **All Devices**, and then click **Edit > Install Certificate**.

   The **vTPS License Installation Wizard** is displayed.

4. Select an available vTPS certificate from the drop-down list to install on your vTPS device.

   The certificates are grouped by type (speed, capabilities, expiration date) and quantity. After you select a certificate, the certificate ID is displayed.

5. Select one of the following options:
   - **Download from TMC** — The SMS automatically downloads the selected certificate from the TMC. The SMS must be connected to the TMC to use this option.
   - **Import file** — Import a locally saved certificate file to the SMS. If you select this option, you must first manually create and download the appropriate certificate file from the license manager.

6. After you select either **Download from TMC** or **Import file**, click **Next**.

   - If you selected **Download from TMC**, and if the certificate file successfully downloads, the **Certificate Validated** page appears. Proceed to step 9.
Note: If the automatic download from the TMC fails, the Manual Certificate Import page appears with an error message. Retry the automatic TMC download or click Next to import the certificate file manually.

- If you selected Import file, the Import Certificate File page appears. Proceed to step 7.


8. Select the appropriate certificate file that you created and downloaded in the license manager, and then click Import.

Note: If you select the incorrect certificate file, the Certificate Validation Failed page appears. Click Previous to go back to the Import Certificate File page, and then upload a different certificate file.

When the certificate file successfully imports, the Certificate Validated page appears.


The SMS installs the license certificate package on the vTPS device. You can view the progress of the installation on the Distribute to Device dialog.

The vTPS device automatically reboots after the license certificate successfully installs on the device. When the reboot sequence completes, the new license certificate capabilities activate on the vTPS device.

Intrusion Prevention System devices

Intrusion Prevention System (IPS) devices protect your network by scanning, detecting, and responding to network traffic according to the filters, action sets, and global settings maintained on each device by a client. Each device provides intrusion prevention for your network according to the number of network connections and hardware capabilities.

TippingPoint IPS devices are designed to handle the extremely high demands of carriers and high-density data centers. Even while under attack, TippingPoint Intrusion Prevention Systems are extremely low-latency network infrastructure ensuring switch-like network performance. TippingPoint also has built-in intrinsic high-availability features, guaranteeing that the network keeps running in the event of system failure.

The SMS supports the following IPS devices:

S-Series devices on page 406

N-Platform devices on page 407

NX-Platform devices on page 407

S-Series devices

TippingPoint S-Series 10/110/330 devices that are new or that are upgraded to TippingPoint Operating System version 3.1.4 or above have increased functionality and include many of the same features that are included in N-Platform and NX-Platform devices. To manage these new or upgraded devices, the SMS must be version 3.2 or later.
• **TP 10 Devices** — provide access to two 10/100/1000 segments with 20 megabits/second and is designed as a smaller form factor for remote networks.

• **TP 110/330 Devices** — provide access to four 10/100/1000 segments with 100 megabits/second (TP 110) and 300 megabits/second (TP 330).

**N-Platform devices**

The TippingPoint N-Platform IPS devices are hardware-based IPS devices that support IPv6, tunneling (including GRE and multi-layer tunnels), and inspection bypass rules for trusted traffic. N-platform devices have the option to install ZPHA modules to support the 10GbE segments. These modules can be configured to block or permit traffic in the event of a power failure.

The 660N and 1400N models have five copper segments and five fiber segments. The 2500N, 5100N, and 6100N models have five copper segments and five fiber segments, and also include a 10GbE fiber segment.

**NX-Platform devices**

The TippingPoint NX-Platform IPS devices are built upon the same feature set as the N-Platform devices. Instead of ZPHA modules, NX-Platform devices add support for up to four I/O modules enabling users to customize the device.

The SMS supports TippingPoint Bypass Input/Output Modules (BIOM) which are designed for use with NX-Platform IPS devices.

For NX-Platform devices, each installed module has an associated slot number from 1 to 4. Ports are organized by slots.

The following standard I/O modules are supported for NX Platform security devices and are hot-swappable:

• TippingPoint 6-Segment Gig-T I/O module
• TippingPoint 6-Segment GbE SFP I/O module
• TippingPoint 4-Segment 10 GbE SFP+ I/O module
• TippingPoint 1-Segment 40 GbE QSFP+ I/O module

The following bypass I/O modules are supported for NX Platform security devices and are hot-swappable:

• TippingPoint 4-Segment Gig-T Bypass module
• TippingPoint 2-Segment 1G Fiber SR Bypass module
• TippingPoint 2-Segment 1G Fiber LR Bypass module
• TippingPoint 2-Segment 10G Fiber SR Bypass module
• TippingPoint 2-Segment 10G Fiber LR Bypass module

**Note:** The 10G Fiber BIOMs have internal dual-rate SFP+ transceivers that can operate at either 10 Gbps (the default) or 1 Gbps speeds.

For the 10G fiber bypass modules and 10 GbE I/O modules to operate at 1 Gbps speeds, explicitly set the line speed to 1 Gbps by using the CLI, LSM, or SMS. Auto-negotiation can also be selected at 1 Gbps, to match the link partner. To operate at 10 Gbps, auto-negotiation must be disabled on the 10G fiber bypass modules and 10 GbE I/O modules.

**Note:** A 40 Gigabit I/O module is hot-swappable with an existing 40 Gigabit I/O module. However, 40 Gigabit modules are not hot-swappable with a different module type. For example, a 10 Gigabit or 1 Gigabit I/O module cannot replace a 40 Gigabit I/O module without a performing a full reboot.

When the slot is empty, the ports or segments are not displayed. When a module is inserted, the SMS uses the current device configuration for the module. When a module is removed, the slot shows empty.

**Note:** Performing a hot-swap of I/O modules during system initialization is not supported.

The SMS supports TippingPoint Bypass I/O Modules (BIOM) which are designed for use with NX-Platform IPS devices that do not have integrated ZPHA or the ability to use Smart ZPHA modules. The bypass modules determine whether network traffic from a network system should be routed into the IPS device or “looped back” to the module front panel and sent back out to the network system through the external port. System software determines if the module is in bypass or normal mode.

For information on installing and configuring BIOMs, see the TippingPoint Bypass Input/Output Module documentation.

**Note:** Network traffic is NOT scanned or blocked when the bypass I/O modules are used to bypass an IPS device.

To configure the bypass mode on a bypass I/O module, see *Enable and disable the bypass mode on an installed bypass module – TPS (TX Series) and IPS (NX-Platform)* on page 364.

The following NX-Platform models and their traffic throughputs are supported across multiple copper and fiber segments for each model:

- 7500NX manages up to 20 Gbps
- 7100NX manages up to 13 Gbps
- 6200NX manages up to 10 Gbps
- 5200NX manages up to 5 Gbps
- 2600NX manages up to 3 Gbps
Tier statistics for the vTPS, TPS, and IPS (NX-Platform) devices

Displays throughput and efficiency across the different inspection tiers of this device. Use this information to diagnose certain performance-related issues. On a stack device, the device's stacking statistics are displayed.

<table>
<thead>
<tr>
<th>Inspection Tier</th>
<th>Description</th>
</tr>
</thead>
</table>
| Stack : Segment Ports | For IPS (NX-Platform) and TPS (TX Series) devices, the following information is displayed when stacking is enabled:  
  - **Segment Rx Mbps** displays the aggregate received traffic from all network segments on this device.  
  - **Segment Tx Mbps** displays the aggregate traffic transmitted from all network segments on this device.  
  - **Stack Balance** displays the load balance percentage, in which 100% equates to perfect balance across the number of devices in the stack. Note this will include devices that are in Intrinsic HA L2FB which would be zero in the load balance calculation. This statistic is analogous to the XLR load balance percent in Tier 1.  
  - **<host n> Rx Mbps** displays the traffic balanced from this device's network segments to the other devices in the stack.  
  - **Segment ratio to tier 1** displays the percentage of traffic being inspected by this device as a ratio of the segment Rx traffic. |
| Stack : Stack Ports | For IPS (NX-Platform) and TPS (TX Series) devices, the following information is displayed when stacking is enabled:  
  - **Stack Rx Mbps** displays the aggregate received traffic from both stacking ports.  
  - **Stack Tx Mbps** displays the aggregate traffic that is transmitted from both stacking ports.  
  - **Stack Rx > Stack Tx** displays the total amount of transit or through traffic on the stacking ports, for example, traffic received on Stack port 1 which is forwarded by the switch to stack port 2.  
  - **Stack Rx > Seg Tx** displays the amount of return traffic coming in on a stacking port en route to a network segment. |
<table>
<thead>
<tr>
<th>Inspection Tier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tier 1</td>
<td>Inspection bypass and Intrinsic HA L2FB are handled here, preventing traffic from going to the next tier. It also handles the rate limiter, inspection bypass rules, jumbo packet shunting, and hardware watchdog timer.</td>
</tr>
<tr>
<td></td>
<td>• Stack ratio to tier 1 displays the percentage of traffic being inspected by this device as a ratio of the stack Rx traffic.</td>
</tr>
<tr>
<td></td>
<td>• Rx Mbps and Tx Mbps and Rx packet/sec and Tx packet/sec indicate how much traffic is entering the inspection engine from all the segments. A value in parentheses () represents the high-level watermark and a value in brackets [] represents the low-level watermark since the IPS was powered on or the tier statistics were reset.</td>
</tr>
<tr>
<td></td>
<td>• Note: Use the clear np tier-stats CLI command to clear out these statistics.</td>
</tr>
<tr>
<td></td>
<td>• Bypass Mbps displays the current and max throughput matching an Inspection Bypass rule. Traffic matching an Inspection Bypass rule does not count towards the IPS inspection limits.</td>
</tr>
<tr>
<td></td>
<td>• A/B/C Balance displays how well the flows are being balanced between the XLRs. 100% indicates even balance 33/33/33 split, which is ideal. 0% means that all traffic is going to a single XLR. Note that the number of packets going thru the each XLR is flow based, so it is not uncommon to see a slight difference between them.</td>
</tr>
<tr>
<td></td>
<td>• Utilization displays the percentage of rated system throughput and of traffic to next tier.</td>
</tr>
<tr>
<td></td>
<td>• Inspection bypass rules reduce the value of both Utilization and Ratio to next tier.</td>
</tr>
<tr>
<td>Tier 2</td>
<td>Load balances flows through the KS threads and handles traffic management trusts and block filters will prevent traffic from proceeding to the next tier.</td>
</tr>
<tr>
<td></td>
<td>Ratio to next tier accounts for Traffic Management Trust and Block rules and Traffic normalization filters. TCP ACKs are trusted by default, and reduces Tier 2 ratio to next tier.</td>
</tr>
<tr>
<td>Tier 3</td>
<td>This tier is designed to search for suspicious traffic that needs to undergo deep inspection. This section handles IPv6 + GRE and Mobile IPv4 tunnels. IP reassembly, maintaining connection table, and TCP state tracking is handled</td>
</tr>
</tbody>
</table>
Inspection Tier | Description
--- | ---
here. If triggers are found it determines what filters need to be checked against the packet or flow than it turns on soft-reroute for the flow, and, if necessary, sends it for deep packet inspection.

This section displays how much traffic KS threads and IP reassembly will inspect. Ratio to next tier shows what percentage of traffic needs TCP reassembly or is suspicious (matched a trigger).

Tier 4

This tier performs TCP reassembly and threat verification which includes header-based checks, protocol decoders, content search, and regular expression matching. Also, action handling occurs here whether the packet is dropped, rate limited, or rate limited in the connection table.

• Rx due to indicates why traffic is going deep:
  ◦ Trigger match. Displays the percentage of traffic that matched a trigger.
  ◦ Rx due to Reroute. When a packet matches a trigger the following packets which belong to the same flow are required for threat verification.
  ◦ TCP sequence. If traffic cannot be reordered by K threads using loopy packet, it must go to Tier 4 for reordering.

• Ratio to next tier. Displays the percentage of traffic that matched a filter, regardless of the Action Set.

Tuning is required if congestion is occurring or if an IPS is being operated close to its maximum rated throughput. The deeper a flow is inspected the more processing is required, so the most performance gains can be attained by optimizing the KS threads at this level (Tiers 3 and 4). The three most process intensive operations are:

1. IP reassembly
2. Threat verification
3. TCP packet reordering

Tier 5

For supported TPS devices, the following information is displayed when SSL inspection is enabled:
### Inspection Tier

<table>
<thead>
<tr>
<th>Inspection Tier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Rx Mbps and Tx Mbps indicate how much encrypted traffic is entering the inspection engine from all the segments. The numbers in the brackets represent the high-level water mark since the IPS was powered on or tier stats was reset.</td>
<td></td>
</tr>
</tbody>
</table>

**Note:** Use the `clear np tier-stats` CLI command to clear out these statistics.

|• Utilization displays the percentage of rated system throughput and of traffic to next tier. |

---

### Next Generation Firewall appliances

The TippingPoint Next Generation Firewall (NGFW) appliances consist of an enterprise stateful firewall, application- and user-based policy, and the TippingPoint Intrusion Prevention System. The NGFW appliances offer sophisticated and comprehensive defense against network invasion, proliferation of unauthorized application use, and business interruption at critical access points, including the network perimeter. In addition to providing a robust and scalable solution that includes auto-updating and policy-based controls, these appliances are designed for easy installation and maintenance.

The NGFW family includes the S1000 Series, S3000 Series, and the S8000 Series appliances. These robust, high-performance security appliances offer a scalable solution to support all types of organizations and network environments.

- The S1000 Series currently features the S1050F 1U form-factor appliance designed for smaller organizations, such as corporate branch offices. This appliance provides full next-generation firewall protection designed to meet the needs and budgets of small- to medium-sized organizations.
- The S3000 Series currently features the S3010F and S3020F 2U form-factor appliances designed for medium-sized deployments, such as on university campuses.
- The S8000 Series currently features the high-performance S8005F and S8010F 2U form-factor appliances. These high-end, robust models accommodate the heavier traffic flows of large enterprises.

NGFW appliances are quick to deploy and easily managed with fine-grained, policy-based controls, and deep-packet, application-layer inspection capabilities. The TippingPoint SMS system can provide central management of multiple NGFW appliances as well as other devices.

Before you can add an NGFW appliance to the SMS as a managed device, you must install and configure the components and run through the OBE Setup Wizard. For more information, refer to the *TippingPoint Next Generation Firewall Hardware Specification and Installation Guide*. To add an NGFW appliance to the SMS, see *Adding, editing, or deleting a device* on page 327.
Core Controller

The TippingPoint Core Controller is a hardware-based appliance that enables inspection of up to 20 Gbps of traffic by sending the traffic to as many as 24 IPS segments. The Core Controller can control traffic across its three 10GbE network segment pairs and across multiple TippingPoint IPS devices. IPS devices are connected by 1GbE uplinks. Each packet that is received on a 10GbE Core Controller interface uses a flow management method to determine the IPS connection to use for transmitting the packet.

The Core Controller receives incoming network traffic through one to three 10GbE segments and manages the traffic flow by distributing the traffic across IPS device segments. After the IPS devices inspect the packets, the Core Controller transmits the traffic through the original 10GbE segment and back into the network.

IPS devices recommended for use with the Core Controller include TippingPoint 2400E, 5000E, 2500N, and 5100N.

Core Controller segment (10G)

The Core Controller contains three 10GbE segments. Each segment has an A port (incoming traffic) and a B port (outgoing traffic) and can be configured full or half duplex, with a total bandwidth of 10 Gbps in either direction.

You have the option to install ZPHA modules to support the 10GbE segments. These modules can be configured to block or permit traffic in the event of a power failure.

Core Controller iLinks

The Core Controller contains 24 1GbE iLinks, which connect to IPS segments. Each iLink has an A port and a B port. The range of iLinks assigned to a 10GbE segment is referred to as an iLink group.

Flow management

The Core Controller distributes traffic from the 10GbE segments to the associated iLinks (port pairs on the Core Controller). Flow management guarantees traffic flow affinity, so that all traffic associated with a flow of packets is routed to the same IPS segment. The SMS allows you to configure up to four rules based on various types of traffic. You can select a combination of Ethernet Type, IP Protocol, Packet Size and (VLAN or MPLS).

The TippingPoint Core Controller provides:

- Ability to add IPS inspection power as bandwidth usage grows
- Traffic flow management by distributing the traffic across TippingPoint IPS device segments
- High Availability with built-in ZPHA

Before you can add the Core Controller to the SMS as a managed device, you must install and configure the components and run through the OBE Setup Wizard. For more information, refer to the TippingPoint Core
Controller Hardware Installation and Safety Guide. To add the Core Controller to the SMS, see Adding, editing, or deleting a device on page 327.

After you add the Core Controller to the SMS, the SMS client launches the Core Controller Mapping wizard to guide you through the process of mapping the SMS and connected device segments.

**TippingPoint vController**

The TippingPoint vController secures network traffic in virtualized environments and is part of the TippingPoint Secure Virtualization Framework (SVF). The vController enables network traffic between virtual machines to be redirected onto a physical network and to an IPS, where the traffic can be inspected. See the TippingPoint vController documentation available from the TippingPoint Threat Management Center at [https://tmc.tippingpoint.com](https://tmc.tippingpoint.com).

**Access the TippingPoint vController from the SMS**

To access the vController management interface with the SMS, you must have:

- TippingPoint vController v2.8 or later, including its management application, the Virtualization Management Center (VMC)
- TippingPoint SMS client 3.1.1 or later

**Note:** The SMS client and vController client can operate correctly when installed on independent hosts. However, the option to launch the vController client from the SMS menu is only available when both clients reside on the same host.

1. Log in to the SMS client.
2. From the top menu bar, go to Tools > TippingPoint VMC.

**TippingPoint Operating System**

When TippingPoint identifies new attacks or improves methods of detecting existing attacks, the TMC makes the updates available to customers in the form of Digital Vaccine filter packages and software packages. Software packages are upgrades to your IPS operating system. DV filter packages contain newly developed attack, peer-to-peer, and anomaly filters along with improvements to existing filters. See Profiles on page 122.

Through the Devices screen, you can check for update notifications for the TippingPoint Operating System (TOS). The SMS client allows you to download and store the TOS files on the system. The packages display on their own screens providing quick review of which devices have received the updates. You can also distribute the updates from each page. The TMC notifies you that new packages are available on the Dashboard. You can also click Download on the Devices (TippingPoint OS) screen.

The following table defines the TOS Inventory details.
When performing a distribution of the update, you can select a high or low priority. The priority aids in performance of the system. High priority updates distribute before low priority. Low priority updates are regulated to ensure the best performance of the system. You can select the priority on the distribute dialog boxes that display when performing a distribution in the SMS client.

When you select a high priority, it takes precedent over a low priority update. However, during the update, you might have dropped packets as traffic and performance are hampered during the update. If you do not
want this loss of packets, you can select a low priority. From a device perspective, unless the traffic through the device is low (or in Layer-2 Fallback), you should always do high priority updates from SMS. Selecting low priority updates can take hours to perform a full update without a loss in traffic packets depending on the level of traffic.

To download and distribute the TOS update, do the following:

- Download the TOS software on page 339
- Import TOS software from a file on page 339
- Managing TOS distribution on page 340
- Distribute the TOS on page 340

## Virtual segments

Virtual segment can be set up to define traffic using a VLAN ID, an endpoint pair (source and destination IP addresses of a packet), or both. One or more physical segments are then assigned to the virtual segment. Virtual segments are members of a segment group and the assigned devices are not exposed in segment group membership. You define the priority order for virtual segment so that any overlapping definitions are resolved. Attempting to define an overlapping virtual segment on a device which does not allow it will produce an error.

Virtual segments can be used as:

- A target for distribution
- Search criteria in events and reports

## Special notes

- Virtual segments appear only if the user has access to the segment group for the virtual segment.
- Virtual segments can be created that do not initially contain any physical segments.
- Physical segments tied to a TOS version 2.2 or earlier device which does not support virtual segments are disabled but displayed in the physical segment lists.
- Physical segments tied to a TOS version 3.0 or earlier device are disabled if the virtual segment is CIDR based.
- IPS devices with virtual segments that were configured locally on an IPS device and then added to the SMS are merged to the global virtual segment listing.
- A Virtual Segment must contain at least one VLAN ID, Source IP, or Destination IP traffic definition.

## Migration

For information on migrating from TOS version 3.0 or earlier, see the SMS Release Notes.
Limitations: 3.1 devices other than N-Platform or NX-Platform IPS devices

IPS devices with a TOS version less than 3.1 do not support overlapping virtual ports or virtual ports defined with src/dest address. Using these devices in an SMS Virtual Segment has certain limitations.

- The device does not support Virtual Segments defined with src/dest address.
- Virtual Segments which contain overlapping VLAN definitions on the same physical segment are invalid because this creates unresolved ambiguity for traffic flow within this device.
- The device does not support the mapping of a mixture of single direction and bi-directional segments. You must choose either both directions for all segments, or only one direction for each segment.
- An IPS device does not support changing the mapping of its physical segments from a set of single direction segments to a set of bi-directional segments or vice-versa.
- When using the opposite side of a directional segment being shared with another Virtual Segment, you must use the exact same VLAN ID for both Virtual Segments. If using Named Resources, the same Named Resource must be used.

In some cases, you might open the Virtual Segment editor and find that you cannot update anything about the segment. In this case, the Virtual Segment is frozen and cannot be updated. The device is sharing the opposite side of a directional segment. Updating the VLAN for one Virtual Segment would cause the other to be updated as well. For this reason, both Virtual Segments are frozen, and cannot be updated.

This section contains the following topics:

- Virtual Segment table on page 417
- Traffic flow analyzer on page 419

You can perform the following tasks:

- Create a virtual segment on page 340
- Delete a virtual segment on page 341
- Segment groups on page 419

Virtual Segment table

The Virtual Segment table is an inventory listing of the currently defined virtual segments and lists the following information:

- **Order** — Priority order that allows resolution for overlapping definitions. Keep in mind the following points:
  - You cannot have a virtual segment with an overlapping VLAN ID on the same physical segment.
  - A user-defined virtual segment with a specified VLAN ID takes precedence over a physical segment (any VLAN).
When you configure virtual segments, keep in mind the following points:

- The IPS (N-Platform or NX-Platform) provides a system-defined virtual segment named ANY-ANY to which the default security profile is assigned. The ANY-ANY segment protects any traffic that does not match another inspection profile on the device. The ANY-ANY segment is not configurable (and is not displayed in the virtual segment table), but you can distribute your own inspection profile to the virtual segment. The priority order for virtual segments on the IPS is:
  a. User-defined virtual segments with a specified VLAN-ID and source/destination IP address.
  b. Physical segments (any VLAN)
  c. ANY-ANY virtual segment
- Unlike the IPS, the TPS does not provide a system-defined ANY-ANY virtual segment. However, you can create a “catch all” virtual segment to distribute your own inspection profile and protect network traffic that does not match another inspection profile on the device. When you create a “catch all” virtual segment, be sure to assign all physical segments and to order the virtual segment lowest in priority. The priority order for virtual segments on the TPS is:
  a. User-defined virtual segments with a specified VLAN-ID and source/destination IP address.
  b. Physical segments (any VLAN)

From the Virtual Segments screen, you can choose the following options:

- **Reorder** — Reorders virtual segments.
- **New** — Creates a new virtual segment.
- **Edit** — Edits an existing virtual segment.
- **Delete** — Delete an existing virtual segment.

The initial view of certain segment and device tables are empty and have the option to customize the table listing by adding list items using the **Add** option.
Traffic flow analyzer

The traffic flow analyzer allows you to check which virtual segments match the supplied criteria for the traffic. If no matches are found of any virtual segment, the device physical segment is used. You can search using the following criteria:

- Source IP Address
- Destination IP Address
- Device Segment
- VLAN ID

Segment groups

Through the Devices screen, you can create and manage groups of device segments. These segment groups enable you to maintain settings and file distribution according to grouping of device segments. These groups provide greater management and distribution of profiles and updates for Digital Vaccine packages, TOS software, and SMS software. Depending on your network setting and architecture, you might need to have differing types and versions of filters and action sets running on particular segments. By creating segment groups, you can associate a particular profile of filters to the group.

In effect, segment groups enhances your network security by providing a deeper level of customization and intrusion protection.

**Note:** A segment can only be a member of one group and have only one distributed profile at any given time. You cannot add a segment to multiple groups. However, you can have many profiles point to the same segment. When you distribute a profile, the segment replaces the currently used profile.

The Segment Groups lists the segment groups with the following information:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Name</td>
<td>Name of the segment group.</td>
</tr>
<tr>
<td>Members</td>
<td>Total number of segment members.</td>
</tr>
<tr>
<td>Profile</td>
<td>Name of the associated profile of filters.</td>
</tr>
</tbody>
</table>
### Device replace table

Use the following tables to determine whether a device needs to be replaced.

**Note:** The devices listed across the top of the table are the new device models; the devices listed down the side of the table are the old device models.

<table>
<thead>
<tr>
<th>New Device</th>
<th>Old Device</th>
<th>vTPS</th>
<th>440T</th>
<th>2200T</th>
<th>110</th>
<th>330</th>
<th>660N</th>
<th>1400N</th>
</tr>
</thead>
<tbody>
<tr>
<td>vTPS</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>440T</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>2200T</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>110</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>330</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>660N</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>1400N</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>Y</td>
</tr>
</tbody>
</table>

For each comparison, note the following:

- **Y** = Yes
- **N** = No replacement
- PD (possible data loss) refers to DDoS settings
- DL (data loss) indicates events and settings for segments that have been removed, such as replacing a four-segment device with a two-segment device.
<table>
<thead>
<tr>
<th>New Device</th>
<th>Old Device</th>
<th>10*</th>
<th>110</th>
<th>330*</th>
<th>660N</th>
<th>1200N</th>
<th>1400N</th>
<th>2500N</th>
<th>5100N</th>
<th>6100N</th>
<th>2600NX</th>
<th>5200NX</th>
<th>6200NX</th>
<th>7100NX</th>
<th>7500NX</th>
</tr>
</thead>
<tbody>
<tr>
<td>10*</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>110</td>
<td>DL</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>330*</td>
<td>DL</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>660N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1200N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1400N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2500N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5100N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6100N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2600NX</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5200NX</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6200NX</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7100NX</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7500NX</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8200TX</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### New Device

<table>
<thead>
<tr>
<th>Old Device</th>
<th>10*</th>
<th>110</th>
<th>330*</th>
<th>660N</th>
<th>1200N</th>
<th>1400N</th>
<th>2500N</th>
<th>5100N</th>
<th>6100N</th>
<th>2600NX</th>
<th>5200NX</th>
<th>6200NX</th>
<th>7100NX</th>
<th>7500NX</th>
</tr>
</thead>
<tbody>
<tr>
<td>8400TX</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
</tbody>
</table>

* These devices must be running TOS v3.14 or later.

For more information, see [Replacing a previous IPS model with an NX model](#) on page 422 and [Replacing an existing NX model with another NX model](#) on page 422

### Replacing a previous IPS model with an NX model

- Port/segment info from the previous model is mapped to NX modules beginning with the module in the first NX slot.

- If the first NX slot does not contain a module, data from the previous model is lost.

- Data from the previous model is lost for any ports/segments that exceed the number of NX module ports/segments.

### Replacing an existing NX model with another NX model

- Port/segment info from the previous model is mapped to NX modules beginning with the module in the first NX slot.

- If either of the NX models has a different slot configuration, data may be lost.

- Data is not mapped to or from models with a blank slot and is lost.

### General clarifications

- N-Series devices can only be replaced by another N-Series or NX-Series device.

- NX-Series devices can only be replaced by another NX-Series device.

- X-Family devices are not supported as either device.

- Core Controller is not supported as either device.

- If the new model is not the same as the old model:
  - And the old model supports DDoS and the new model does not, then DDoS functionality is removed.
  - Virtual segments are removed.
- And the old model has more physical segments than the new model, information is lost.
- The old model cannot be running a newer TOS than the new model.
NGFW

NGFW routing

On the Routing screen, select the settings for various protocols, including the Border Gateway Protocol (BGP), Routing Information Protocol (RIP), and the Open Shortest Path First (OSPF) protocol. In addition, specify route table properties (unicast or multicast), IPv4 and IPv6 static routes, route maps, and static monitored routes.

**Note:** Whether or not static route entries are included in routing tables depends on several topology factors. These include network specificity, metrics, and whether the next hop IP is on the associated interface. Other routing types, redistributions, and firewall rules also impact static route entries in the routing tables.

For more information on routing, refer to the *TippingPoint Next Generation Firewall Local Security Manager User Guide.*

NGFW VPN configuration

A Virtual Private Network (VPN) is a means of establishing a secure connection between two points across a public network, such as the Internet. VPN initiation occurs when a remote user or network requests access to the company LAN. Tunnel initiation is usually accomplished using VPN client software on a PC, or through VPN support in an access router or firewall.

VPN termination is the point in the network at which the identity of the remote party is validated, the VPN tunnel is created, and the remote party enters the network.

From the VPN Configuration screen, you can enable or disable VPN, define the preshared keys to be used by IPsec VPN, select which device certificates are Trusted Certificate Authorities, configure Internet Exchange Key (IKE) settings and proposals, set up IPsec associations and policies, and establish IPsec VPN users. For more information about certificate management, see *Viewing certificates* on page 568 and *Viewing Certificate Authority (CA) certificates* on page 573.

NGFW authentication

Use the Authentication screen to configure user password and security parameter settings for the NGFW appliance.

The SMS supports user authentication for individual devices. From the Device Users screen for a managed device, you can set the following user authentication preferences:

**Security Level** — No security checking (default setting), base or maximum security checking.

**Expiry Time** — Disabled, 10 to 90 days (default setting), 6 months or 1 year.

**Expiry Action** — Force user to change password (default), notify user of expiration or disable the account.
**Maximum Login Attempts** — Login attempts from 1 to 10 (5 - default setting).

**Failed Login Action** — Disable account, lockout account (default setting), or audit event.

**Lockout Time** — Lockout time from 0 to 360 minutes (5 minutes - default setting).

**Login Group** — Indicate whether remote authentication is required for administrative and network/VPN logins, and select the method of authentication.

In addition, the Authentication screen enables you to add and configure RADIUS and LDAP groups, specify the authentication properties of appliance certificates, define the captive portal parameters, and edit the authentication preferences for users, groups, and roles.

For more information on managing authentication, refer to the *TippingPoint Next Generation Firewall Local Security Manager User Guide*.

**NGFW distribution queue**

From the Distribution Queue screen, you can specify the types of packages that can be distributed to an appliance, including:

- Tipping Point Operating System (TOS)
- Profiles
- Digital Vaccine (DV)
- Digital Vaccine Toolkit (DVT)

The queuing of distributions to an NGFW appliance allows you to start a distribution of different packages to the same appliance. See *Distribution queue configuration – TPS and IPS (S-Series, N-Platform, and NX-Platform)* on page 345.

**Create a device HA cluster**

The SMS enables you to configure two NGFW appliances into a two-node high availability (HA) cluster to prevent service interruptions and minimize network downtime due to device failure.

In this configuration, the two devices share state and configuration information, and the passive device monitors the state of the active device. If the active device fails, the passive device takes over, becoming the active device. The HA cluster provides failover protection in the event of a system failure.

Both devices in an HA cluster must be identical models and must be configured the same. Only the following items can be unique to each device:

- Management Interface
- Host Name
- Cluster Member ID
• HA Port IP Address

All remaining configuration must be identical, otherwise the secondary device cannot join the cluster if configuration consistency is enabled.

**Note:** The SMS does not copy the device configuration to the secondary device. If one device is configured, then create a device snapshot and restore the snapshot to the second device.

Before you create a cluster, add the NGFW devices separately to the SMS, and connect the devices using the HA ports. If the appliances have multiple HA ports, verify that you use the same HA port on each appliance.

**Create a device HA cluster**

1. On the All Devices screen, click **New Cluster**.
2. On the General Settings screen of the New Cluster wizard, configure the cluster name, the configuration sync method, and state synchronization options.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster Name</td>
<td>Name that is shared with both members of the cluster. Choose a name that makes sense for your organization.</td>
</tr>
<tr>
<td>Config Sync By</td>
<td>Method used to synchronize configuration information.</td>
</tr>
<tr>
<td>SMS</td>
<td>Shared configuration changes are sent to both cluster members at the same time to keep them in sync. This option is unavailable if the cluster configuration is not in sync.</td>
</tr>
<tr>
<td>Manual</td>
<td>You must configure each cluster member to get the device configurations in sync. Note that the devices will remain out-of-sync until they are configured identically. When the Manual option is enabled, the SMS does not sync any configuration changes to the cluster members, and there are no shared nodes displayed in the Devices navigation pane.</td>
</tr>
<tr>
<td>State Synchronization</td>
<td>Select the subsystems to include in state synchronization (Firewall, Routing, and IPS), and specify the log level for each subsystem.</td>
</tr>
</tbody>
</table>

3. Click **Next**, and select each Member Device included in the cluster.

   The SMS displays the following information for each cluster member:

   - **Member ID** — Identification number that the SMS automatically assigns to each cluster member (1 and 2). The Member ID is not editable.
- Name — Device name that the SMS initially provides for each cluster member. You can edit this field as needed.

- Member Device — Device selected as a cluster member.

**Note:** If you change the Member Device, the SMS does not automatically update the Name field. If you change the selection for Member Device for either cluster member, be sure to update the Name field as well.

- HA Port IP Address — IP address that the SMS automatically assigns to the device HA port. You can edit the HA Port IP Address as needed.

  **Note:** Do not select Standby unless you want to prevent the cluster member from passing traffic.

- Sync Configurations — Select the source member device to copy that device's configuration to the other member of the cluster. If None is selected (the default), the configuration copy operation is not performed when the cluster is formed.

4. Click **Next**, and accept or edit the Failover Group parameters for the cluster:

   - Group Name — Name of the Failover Group.
   - Base MAC Address — Address that all traffic and data interfaces in the cluster use to generate their MAC addresses. By default, the failover group is assigned a base MAC address from one of the member devices that has the “Local Admin” bit set.

5. Click **Next**, and configure cluster traffic parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encrypt Cluster Traffic</td>
<td>Option to encrypt traffic between the cluster devices using Advanced Encryption Standard (AES) 256-bit encryption. If you select this option, you must provide a passphrase.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If the HA port network traffic is physically secure, you do not need to encrypt the traffic. Leaving traffic unencrypted improves performance.</td>
</tr>
<tr>
<td>Use management Port for HA Link Failure</td>
<td>Enable the devices to use the management port to connect in the event that the HA port fails.</td>
</tr>
<tr>
<td>Auto Negotiation</td>
<td>Specifies if auto negotiation is enabled or disabled on the HA port. Auto-negotiation is enabled by default.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Link Speed</td>
<td>Speed of throughput on the port. Link Speed is uneditable if Auto Negotiation is enabled. Default Link Speed = 1 Gbps</td>
</tr>
<tr>
<td>Duplex</td>
<td>Specifies duplex mode on the port (half or full). Duplex mode is uneditable if Auto Negotiation is enabled. Default = Full Duplex</td>
</tr>
<tr>
<td>MTU</td>
<td>Maximum transmission unit. Largest data packet size (in bytes, 576–9,216) that is allowed. Default MTU = 9216 bytes</td>
</tr>
<tr>
<td>Multicast IP</td>
<td>IP address for multicast address transmission. Default IP address = 239.0.0.10</td>
</tr>
</tbody>
</table>

**Note:** Both devices in the cluster should use matching Multicast IPs and UDP ports. These should be unique to this cluster to avoid accidental collisions with other clusters on the same network.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UDP Port</td>
<td>UDP port number for multicast address transmission. Default port = 5404</td>
</tr>
<tr>
<td>TTL</td>
<td>TTL setting (in milliseconds, 1–255) for multicast address transmission. Default TTL = 1 ms</td>
</tr>
<tr>
<td>Timeout</td>
<td>Timeout (in milliseconds, 100—10,000) for multicast address transmission. Default Timeout = 1000 ms</td>
</tr>
<tr>
<td>Retransmission</td>
<td>Number of attempts (1–10) to retransmit multicast address transmission. Default Retransmission attempts = 4</td>
</tr>
</tbody>
</table>

6. Click **Finish**.
A message appears, warning you not to change any configuration before the update has completed. Click OK.

When the cluster is created, the Devices screen displays the cluster in the All Devices area.

If you selected the SMS configuration sync method, the cluster appears as one node in the navigation pane — expand the node to view shared settings information as well as separate nodes for device-specific information such as Device Configuration, Events, and the device Distribution Queue.

If you selected the Manual configuration sync method, the cluster members appear in the navigation pane as two distinct devices, with configuration information shown separately. Note that, if you change the configuration for one device, you must make the same change for the other device to keep both devices in sync.

In the navigation pane, you can select the device node to display an individual device shelf-level graphic for either cluster member. At the shelf-level graphic view, you can right-click on a device to unmanage and remanage a device in a cluster.

Note: If you delete a device form a cluster, the cluster is removed from the SMS and the SMS client shows the other cluster member as an individual device. If you add a deleted device back, the SMS recreates the cluster.

To remove devices from a cluster, you delete the cluster. The devices return to their original state prior to the cluster.

**Synchronize a cluster configuration**

This procedure describes how to synchronize the configuration between two NGFW devices that are members of a High Availability (HA) cluster. The cluster remains intact and the devices are not rebooted during the copy operation. However, you cannot make changes to either member of the cluster until the copy is complete.

Note: The Sync Configuration Now only appears when both cluster members are running on a release that supports the Sync Configuration feature.

1. Click **Devices** and the select the cluster.
2. Click **Sync Configuration Now**.

   The Sync Configuration Now dialog appears.

3. Select the device that contains the configuration that you want to copy to the other cluster member. This is the source device.

   Note: The configuration on the target device will be overwritten.

4. Click **OK** to start the copy.
The copy operation may take several minutes to complete and both devices are non-editable during this process. When the copy is complete, the SMS redisCOVERs both cluster members and updates the **Config Sync** status of each member.

**Force state change**

The Cluster Status table shows the current HA state for each NGFW appliance. You can force the active device to become the passive device, which in turn forces the passive device to become the active device.

1. Select **Devices > All Devices > HA Cluster**.
2. Click **Force State Change**.

   The HA State (in the Cluster Status table and the Member Status area changes to reflect the current state). The firewall synchronization may take a few minutes to display the HA state. Alternatively, you can click **Refresh** to update the HA state.

**Remove a cluster from the SMS**

1. On the All Devices screen, select the device cluster.
2. Click Edit in the menu bar, and then select **Delete**.
3. In the Delete Selected Cluster dialog, click **Delete**.

   Once a cluster is removed, the SMS disables all data ports on the passive device to prevent two devices with identical IP addresses from passing traffic on the network at the same time. When the devices are moved out of the cluster, the All Devices screen displays details for the individual devices again, and cluster information no longer appears on the screen.

**SSL appliance**

The SSL appliance is a hardware-based appliance with dedicated SSL processing. The SSL appliance decrypts SSL traffic between clients and site servers and sends the decrypted traffic to an IPS device for analysis. If the traffic is allowed by the IPS device, the SSL appliance then re-encrypts the traffic and sends it to the client or server.

SSL traffic analysis involves the following process:

- Incoming SSL traffic is routed to the SSL appliance.
- The SSL appliance decrypts the SSL traffic and sends it to the IPS.
- The IPS inspects the decrypted SSL traffic based on user-defined policy.
- Valid traffic is forwarded to the SSL appliance.
- Non-valid traffic is handled according to the user-defined policy.
• The SSL appliance re-encrypts the traffic, if re-encryption is enabled, and forwards it on to the original target device.

Note: Incoming non-SSL traffic is forwarded directly to IPS.

Setting up an SSL appliance

To use the SSL appliance with the SMS, you must have:

• TippingPoint SSL appliance 1500S with TOS version 2.4.2 or later
• SMS with TOS version 3.1.1 or later

In a typical deployment, the SSL appliance is placed in the data path between the clients and server(s), and is connected to the IPS device. Setting up an SSL appliance involves the following basic steps:

1. Install the SSL appliance.
2. Configure the SSL appliance.
3. Configure SNMP on the SSL appliance.
4. Add the SSL appliance to the SMS.

Install the SSL appliance

Follow the instructions listed in the TippingPoint SSL appliance documentation that shipped with the product.

Configure the SSL appliance

Follow the instructions listed in the TippingPoint SSL appliance documentation. This step sets up the basic SSL appliance configuration. These settings can be viewed in the SMS but cannot be edited in the SMS. In order to communicate with the SMS, you must also Configure SNMP on the SSL appliance on page 431.

Configure SNMP on the SSL appliance

Follow the instructions listed in the TippingPoint SSL Appliance GUI Reference Guide to set up SNMP. This step sets up SNMPv1 or v2.

Note: If you want to use SNMPv3, you must use the Command Line Interface (CLI) to configure SNMP on the SSL appliance.

Configure SNMPv3 on the SSL appliance

1. Use a terminal emulation application (such as Putty) to start a terminal session.
2. Log in to the SSL appliance with user name SuperUser.

1500S login: SuperUser
Password: ***** 
Type ? for Help
3. Enter the following commands:

   1500S>enable
   1500S#config
   1500S(config)#snmp-server view [your_view_name] 1.3.6.1 included
   1500S(config)#snmp-server group [your_group_name] v3 priv read
   [your_view_name]
   1500S(config)#snmp-server user [your_user_name] group [your_group_name] v3 auth sha [your_password] encrypted

4. Exit the CLI.

Add the SSL appliance to the SMS

1. On the All Devices screen, click New Device.

   The New Device (Device Information) screen displays.

2. Enter the following information:
   - **IP Address** of the device.
   - **Username** for an account with SuperUser rights, defined on the SSL appliance.
   - **Password** associated with the SuperUser account.

3. Select a **Device Group** to add the device to. You can select All Devices or a specific Device Group you have created.

4. For **Device Type**, select SSL from the drop-down box.

5. Select Options in the wizard navigation pane.

6. On the New Devices (Options) screen, choose the SNMP Version.
   - For SNMP v2, enter the **SNMP Community String**.
   - For SNMP v3, enter the **User Name** and **Authentication Key**.

7. Click OK.

   When the request is successful, the device name displays in the Devices screen.

SSL appliance configuration

The SMS provides configuration details for the SSL appliance.

**Note:** Configuration changes must be made directly through the Web-based interface on the SSL Appliance.

From the SMS, you can review the following configuration areas for the SSL Appliance:

- **Device configuration** on page 433
- **Network configuration** on page 433
• *Event monitoring (SSL appliance)* on page 434

• *System health* on page 434

• *Performance* on page 435

• *Port health* on page 435

• *Traffic* on page 436

• *System log* on page 438

**Device configuration**

The Device Configuration screen provides a summary of the device settings for the SSL Appliance and includes the information you entered when you set up the device.

**Network configuration**

The Network Configuration screen displays relevant network information for the SSL Appliance and includes a tabbed section that displays port information.

**Ports tab**

The Ports tab displays the following information:

• **Type** — Type of port, such as Management Port or Data Port

• **Port** — Port designation

• **Segment** — Segment associated with the port

• **Enabled** — Enabled/disabled status

• **Autonegotiation** — Check mark indicates the port auto-negotiates for line speed

• **Configured** — Speed and duplex configuration

• **Negotiated** — Negotiated setting

• **State** — Health status of the port

• **Qualifiers** — Health status information

• **Media** — Type of media for the port, such as copper or fiber
Event monitoring (SSL appliance)

Through the Events screen for an individual device, you can monitor system-specific information. The default displays data from the past 24 hours. Realtime data is available for most monitoring parameters. The data in the graphs can be printed or exported. To format, right-click on the graph.

**Note:** When first adding a device to the SMS, all of the graphs might not have 24-hours of data.

This section contains the following topics:

- *System health* on page 434
- *Performance* on page 435
- *Port health* on page 435
- *Traffic* on page 436
- *System log* on page 438

**System health**

The System Health monitoring for SSL Appliances tracks key health areas for managed devices and provides information in textual and graphical formats. Monitored statistics include temperature, CPU and memory of the selected managed device. To display current values, click **Refresh**.

**Health Stats** — Lists the current uptime for the SSL Appliance and includes a table with the following system data:

- **Name** — Name of the system component.
- **State** — Includes one of the following indicators:
  - Red square icon — Critical
  - Yellow square icon — Major
  - Green square icon — Normal
- **Current Value** — The amount of the component used.
- **Details** — Specific information about the monitored component.

**Health Graphs** — Provides a graphical representation for the following system data:

- **Temperature** — Temperature (measured in degrees C) of the SSL Appliance.
- **CPU** — How much of the CPU capacity is in use.
- **Memory** — How much memory the SSL Appliance is using.
Performance
Monitored performance data is displayed in textual and graphical formats for the following areas:

- Performance
- HTTP Proxy
- Health Check Summary

To display current values, click **Refresh**. To reset the counter, click **Reset**. To copy a device graph data to the clipboard, right-click on the graph.

The Performance Graphs area displays graphs for the following items:

- Throughput
- Current Connections
- New Connections
- L7 Request

To display current values, click **Refresh**. To view Realtime data, click **Realtime**.

Port health
Port health monitoring for an SSL Appliance tracks key port statistics for managed devices and provides information in textual and graphical formats.

Port statistics
The textual display provides data by segment and includes the following information:

- Total Received/Sent Bytes
- Total Received/Sent Errors

To display current values, click **Refresh**.

The graphical display tracks Input/Output by port and provides information about the following items:

- Bits — Bits per second
- Errors— Bits per second
- Other Errors— Bits per second

To display current values, click **Refresh**.
Traffic

The Traffic section tracks and compiles information on all traffic managed by the device. Traffic monitoring includes tabbed pages for the following areas:

- **Server tab** on page 436
- **Net tab** on page 436
- **SSL tab** on page 437
- **Switch tab** on page 437

Server tab

The Server screen displays textual and graphical information about current/total connections, received/sent packages, received/sent bytes for each listed server. The default view provides information for the first server in the server table listings. To view information for another server, highlight the server in the list.

To display current values, click **Refresh**. To view Real-time data, click **Realtime**. For additional information, check the help files on your SSL appliance.

Net tab

The Net screen displays textual information about the following items:

- **Connection Limit Drops/Resets** — Number of connections dropped/reset because the server connection limit was reached.
- **IP Out with No Route** — Number of IP packets that could not be routed.
- **Server Sel Failure** — Number of times selection of a real server failed.
- **Sessions Ages Out** — Number of sessions that aged out.
- **TCP No SLB** — Non-SLB packets.
- **TCP Out RST** — Number of TCP resets sent
- **TCP Out RST**:  
  - **ACK attack** — Number of TCP resets sent in response to a TCP ACK attack.
  - **No SYN** — Number of resets sent for which there were no SYN.
  - **Stale Sessions** — Number of TCP reset packets the SSL appliance sent due to stale TCP sessions.
  - **TCP Proxy** — Number of TCP reset packets the SSL appliance sent as a TCP proxy.
  - **TCP Received** — Number of TCP packets received.

To display current values, click **Refresh**. To view Realtime data, click **Realtime**. For additional information, check the help files on your SSL appliance.
SSL tab

The SSL screen displays textual information about the following items:

- Current/Failed/Total SSL Connections
- HW Ring Full
- No HW Context Memory
- Number of Available/enabled Crypto Engines
- Number of SSL Modules
- SSL Fail CA Verification
- SSL Memory Usage

To display current values, click Refresh. To view Realtime data, click Realtime. For additional information, check the help files on your SSL appliance.

Switch tab

The Switch screen displays textual information about the following items:

- ACL Denies
- Anomaly:
  - All Frag Drops
  - Any Drops
  - IP Option Drops
  - LAN Attack Drops
  - Ping-of-Death Drops
  - SYN Frag Drops
  - TCP No Flag Drops
  - TCP SYN Fin Drops
- Bad Packet Drop
- Forward Kernel
- IP Fragment
  - Overlap Drops
  - Exceed Drop
○ Overlap
○ Reasm Fail
○ Reasm OKs
○ Received

• IP (TCP) Received
• IPv4 No route Drop
• L2 Forward
• L3 IP Forward
• L4 Process
• Link down Drop
• Packet Error Drops
• Protocol Down Drop
• SRC Port Suppression
• SYN rate exceeded Drop
• TTL Exceeded Drop
• Unknown Protocol Drop
• VLAN Flood

To display current values, click Refresh. To view Real-time data, click Realtime. For additional information, check the help files on your SSL appliance.

**System log**

System log monitoring functions the same as an IPS device. For additional information, check the SMS help files.
Stacking

Stacking enables you to increase the overall inspection capacity of your TippingPoint Intrusion Prevention System (IPS) or TippingPoint Threat Protection System (TPS). See the following sections for more information.

Stacking for TPS

The information provided describes how to increase inspection capacity by implementing stacking for TippingPoint TX Series Threat Protection System (TPS) devices.

Overview

Stacking enables you to increase the overall inspection capacity of your TippingPoint Threat Protection System (TPS) by grouping multiple TX Series devices and pooling their resources.

You can configure up to five TX Series devices in a stack. The stack operates as a single device that you manage on the TippingPoint Security Management System (SMS). The devices in the stack can be all 8200TX or 8400TX TPS devices, or a mix of both 8400TX and 8200TX security devices. All devices in a stack should be licensed for the same inspection throughput.

In-line inspection capacity increases with each device that you add to the stack. For example, for each 8200TX or 8400TX added to a stack of devices, the inspection capacity increases according to the licensed inspection capacity of each device, up to a stacking maximum of 120 Gbps.

The following TippingPoint software is supported for stacking:

- **TippingPoint SMS v5.0.0, or later** - Centrally manages each stack of devices.
- **TippingPoint Operating System (TOS) v5.0.0, or later** - Must be installed on each security device.

**Note:** No additional licensing is required to implement stacking.

Not all TippingPoint TX Series TPS features are supported in a stack configuration. See *Limitations* on page 482.

Set up the stack

This information explains how to set up the stack of devices, including basic, resilient, and multiple network segment configurations.

You can customize the stack by adding the number of devices and enabling the features you need.

After you set up a basic stack, you can consider whether to configure it to be a resilient stack. For more information, see *Resilient stack configuration* on page 445.
For details about how to install your security device, see the *Install your security device* quick reference card.

**Stacking components**

You need the following components for each device that you add to the stack. Also, you need network I/O modules for the stack members that you connect to the network.

- TippingPoint 8200TX or 8400TX device.

- TippingPoint 40G QSFP+ Active Optical Cable (AOC).

**Basic stack configuration**

When you configure a basic stack, every member of the stack must be operational. If any member of a basic stack becomes unavailable, the entire stack becomes unavailable. Use the following information to configure a basic stack:

- *Install the stacking components* on page 440
- *Create the stack in the SMS* on page 442

Install the stacking components

A TX Series device stack consists of two or more devices. The *stacking bus* consists of a pair of SP ports on each stacking device that connect each device to its peer in a ring topology.
The I/O modules should be installed in the stacking device that you plan to use as the network segment device. A network segment device operates in-line in the network and distributes network traffic to each stack member for inspection. The other stack members do not need network I/O modules.

**Note:** If you have a mixed stack configuration with 8400TX and 8200TX devices, maximize the physical network I/O slots that are available to the stack by installing network I/O modules in any of the network I/O slots on the 8400TX security device.

**To install the stacking components**

1. Install the network I/O modules on the network segment device so that you can connect the device to the network.
   
   For information about how to install I/O modules, see the *TX Series Hardware Installation and Safety Guide*.

2. Install the AOC cables in the SP ports of both devices so that each device connects to its peer in a ring topology.

   **Note:** When you install the AOC cable, you should orient the QSFP+ transceiver with the tab on top. The AOC cable is keyed so that it can only be correctly inserted one way. If the cable does not slide in easily and click to latch, it may be upside down. See *Verify AOC cable installation* on page 454 for more information.

**Examples with the AOC cables installed**

The following example shows a mixed stack configuration with an 8400TX (bottom) and an 8200TX (top) security device. The AOC cables are properly installed in the SP ports.

**Figure 1. TippingPoint TX Series TPS – the AOC cables are installed properly**
The next example shows the network I/O modules are properly installed in slots 1 and 2 of the network segment device (bottom).

**Figure 2. TippingPoint TX Series TPS – stack with network I/O modules installed in slots 1 and 2**

Create the stack in the SMS

Use the SMS to create the stack and centrally manage the stacking devices online.

The process is:

1. **Add the stacking devices to the SMS**
2. **Create the stack**
3. **Distribute the inspection profile**

The following information provides more details:

- *Add the stacking devices to the SMS* on page 442
- *Create the stack* on page 443
- *Distribute the inspection profile* on page 444

**Note:** Before you can create the stack in the SMS, you need to set up the stacking components. See *Install the stacking components* on page 484.

**Add the stacking devices to the SMS**

After you install the stacking components, add each device in the stack to the SMS so that you can create and manage the stack online.
For each device, use the SMS to install the required TippingPoint Operating System (TOS) version, v5.0.0 or later. The TOS version must be the same on each TX Series device. For more information, see *Adding, editing, or deleting a device* on page 327.

If you are repurposing an existing device for use in the stack, reset the device to factory settings, and then install the required TOS version. For more information, see *Repurpose a device* on page 483.

Create the stack

After you add the stacking devices to the SMS, create the stack in the SMS so that the devices are in the stacking topology. Then, use the Devices options in the SMS to specify the stack configuration.

**Note:** You must have the Device Group/Stack Structure Manager capability assigned to your role to create a stack. See *Authentication and authorization* on page 542.

To create the basic stack in the SMS with two devices

1. In the SMS tools, click **Devices**.
2. In the **All Devices** workspace, right-click a stacking device and select **New Stack**.
3. In the **Choose Devices** options, specify the stack name.

   **Figure 3. Choose devices options – stacking devices selected**

   ![Choose Devices](image)

4. Choose **Normal** for the Stack Resilience option.
   
   For information about the **N+1 Redundancy** option, see *Resilient stack configuration* on page 445.
5. Select both devices.
- If a device is not displayed, validate the following items:
  - The device is not already a member of another stack.
  - The device is a TX Series (8200TX or 8400TX) TPS.
  - If either device does not have a **Ready for stacking** status, see *Resolve issues adding a device to the stack* on page 518 for troubleshooting information.

6. Click **Set as Segment Reference Device** and select the network segment device that the SMS uses as a template to create the corresponding segments on each stack member.

7. Click **OK**.

8. In the **All Devices** workspace, double-click the stack shelf-level image to view stack health.

9. In the **Summary** tab, verify the stack health is **Normal**.

   If the stack is not healthy, identify and resolve any issues. See *Verify stack health and synchronization* on page 459.

**Distribute the inspection profile**

Distribute the inspection profile to the stack by choosing from the segments on the segment reference device (SRD). After you do this, the inspection profile goes to the corresponding segments on each member of the stack.

**Note:** For more information, see *Distribute an inspection profile to inspection segments* on page 145.

After you distribute the inspection profile, use the **Sync Health** tab to identify and resolve any synchronization issues with the stack. See *Verify stack synchronization* on page 468.
The following example shows the profile distribution to the default segment group, which includes all the segments on the stack.

Figure 4. Distribute the inspection profile to all the segments on the stack

Resilient stack configuration

You can change the configuration of a basic stack to a resilient stack so that the stack continues to inspect network traffic if a single stack member is not ready to inspect (NRTI).

In a resilient stack, the network traffic continues to be inspected when a single stack member is NRTI by rebalancing network traffic between the remaining ready to inspect (RTI) devices. For information about how stacking determines whether a device is ready to inspect, see Enable or disable Intrinsic High Availability Layer-2 Fallback on page 478.

To enable a resilient stack configuration, follow the same process that is described in Create the stack on page 443, but select the N+1 Redundancy Stack Resiliency option.

When all the devices in the stack are RTI, the stack load balances network traffic across all the devices. If a single stack member is NRTI, the stack rebalances network traffic between the remaining RTI devices, reducing inspection capacity.

Important: When the stack is configured with a single network segment device, if the network segment device is NRTI, the entire stack is NRTI. To enable the stack to continue to inspect traffic
The following example shows a resilient stack:

- The network segment device (1) is at the bottom of the stack.
- The network segment device load-balances network traffic from each utilized segment to the other device in the stack.
- The stack continues to inspect if the top device is unavailable.

**Figure 5. TippingPoint TX Series TPS – resilient stack configuration**

**Multiple network segment device configuration**

You can change the device configuration of a resilient stack to include multiple network segment devices. With more than one network segment device, the stack continues to inspect network traffic if any stack member, including a network segment device, becomes unavailable. If any stack member becomes unavailable, the stack rebalances network traffic between the remaining available devices.

**To configure multiple network segment devices**

- Install network I/O modules on each network segment device.

  The same slot on each device must be configured with either the same network I/O module or no network I/O module. The following example shows the slot numbers for 8200TX and 8400TX devices.
Consider the following items when you configure multiple network segment devices:

- Connect the same networks to the same network segments on each network segment device.
- Traffic can come in both network segment devices as long as the corresponding segment ports of each device are connected to the same networks. For example, port 1–1A on IPS–A and IPS–B are connected to Network A and port 1–1B on IPS–A and IPS–B are connected to Network B.

**Example with multiple network segment devices**

The following example shows a valid two-device stack with both network segment devices connected to the same networks on the same segment ports. Either network segment device can be designated as the segment reference device. Each network segment device load-balances traffic from each utilized segment to the other member of the stack on a per flow basis.

**Figure 7. TippingPoint TX Series TPS – two-device stack with multiple network segment devices**
Update the stack configuration

In the SMS, update the stack configuration, for example, when you need to add another device to the stack.

Note: For information about the differences between configuring a stack of devices compared with configuring a standalone device, see *Differences between configuring a stack and a standalone device* on page 526.

The following information describes several ways that you can update the stack configuration:

- *Enable or disable stack resiliency* on page 448
- *Change the segment reference device* on page 449
- *Replace a device in the stack* on page 449
- *Remove a device from the stack* on page 450
- *Add a device to the stack* on page 450
- *Delete the stack* on page 452
- *Grant permissions to the stack* on page 452
- *Distribute a TOS update* on page 453

Enable or disable stack resiliency

Update the stack configuration in the SMS to enable stack resiliency so that the stack can continue to inspect traffic if a single stack member is not ready to inspect (NRTI) network traffic.

When you enable stack resiliency, make sure the stack is configured with enough devices to provide the required inspection capacity. See *Resilient stack configuration* on page 445.

To enable or disable stack resiliency

1. In the SMS tools, click **Devices**.
2. In the **All Devices** workspace, double-click the stack.
3. In the **Summary** tab, click **Edit**.
4. In **Edit Stack Configuration**, select a Stack Resilience option:
   - **N+1 Redundancy** – This option enables the stack to continue to inspect traffic if a single stack member is NRTI. If more than one device is NRTI, the stack automatically goes into Intrinsic HA L2FB. See also, *Enable or disable stack resiliency* on page 448.
   - **Normal** – This option automatically places the stack and all of its devices into Intrinsic HA L2FB if a single stack member is NRTI.
Change the segment reference device

Update the stack configuration in the SMS to select the network segment device that the SMS uses as a template to create the corresponding segments on each stack member.

Make sure that the device is configured with the correct network I/O modules, has the correct segment configuration, and has the associated inspection policy.

After you change the segment reference device, distribute the inspection profile to update the stack. For more information, see Distribute the inspection profile on page 444.

To change the segment reference device in the SMS

1. In the SMS tools, click Devices.
2. In the All Devices workspace, double-click the stack.
3. In the Summary tab, click Edit.
4. In Edit Stack Configuration options, select the network segment device from the Segment Reference Device list.

Replace a device in the stack

If a stacking device must be replaced, you can update the stack configuration in the SMS with the replacement device.

To replace a stack member in the SMS

1. Place the stack in Intrinsic HA L2FB. See Enable or disable Intrinsic HA L2FB on the stack on page 478.
2. Remove the stack member from the stack configuration. See Remove a device from the stack on page 450.
   If the device is designated as the segment reference device (SRD), update the stack configuration to designate a different device as the SRD, and then remove the stack member from the stack configuration. See Change the segment reference device on page 449.
3. Install the AOC cables to remove the old stacking device from the stacking bus and to add the new device. See Install the stacking components on page 440.
   If the device you want to replace is configured with network I/O modules, make sure that the replacement device has the same network I/O modules in the same slots.
4. Manage the new device with the SMS and then add the stacking device to the stack configuration.
   If necessary, update the stack configuration to designate the replacement device as the SRD. See Change the segment reference device on page 449.
5. Distribute the inspection profile to the stack. For more information, see Distribute the inspection profile on page 444.
6. Take the stack out of Intrinsic HA L2FB. See Enable or disable Intrinsic HA L2FB on the stack on page 478.
Remove a device from the stack

Remove a device from the stack when you need to decrease inspection capacity, or when you need to replace a device in the stack.

(Best Practice) To reuse a device after it is removed from the stack, either as a standalone device or as part of a different stack, use the `debug factory-reset` command to restore the device to its original settings. See `Repurpose a device` on page 483.

**Note:** A stack with a single stack member is supported on a temporary basis, for example, to replace a device in the stack with two devices. However, a single-device stack does not have a normal health status.

To remove a device from the stack configuration

1. Place the stack in Intrinsic HA L2FB. See `Enable or disable Intrinsic HA L2FB on the stack` on page 478.
2. Remove the device from the stack in the SMS (see the next procedure).
   - If the device is designated as the segment reference device (SRD), update the stack configuration to designate a different device as the SRD, then remove the device from the stack configuration. See `Change the segment reference device` on page 449.
3. Install the AOC cables to remove the old stacking device from the stacking bus. See `Install the stacking components` on page 440.
4. Take the stack out of Intrinsic HA L2FB. See `Enable or disable Intrinsic HA L2FB on the stack` on page 478.

To remove a device from the stack in the SMS

1. In the SMS tools, click **Devices**.
2. In the **All Devices** workspace, double-click the stack.
3. In the **Summary** tab, select a device from the Stack Member list.
4. Click **Remove**.
   - **Note:** You cannot remove a device from the stack while it is the SRD. If necessary, change the SRD to a different stacking device and then remove the device from the stack.
5. Click **OK**.
   - The stack health is updated. See `Verify stack health and synchronization` on page 459.

Add a device to the stack

Add a device to the stack when you need to increase the inspection capacity of the stack, or when you need to replace a device in the stack.

(Best Practice) If you are repurposing an existing device for use in the stack, reset the device to factory settings, and then install the required TOS version. See `Repurpose a device` on page 483.
When you add a device to the stack configuration, the SMS automatically enables stacking on the device. If necessary, remove the device from the stack configuration, and then add it again to enable stacking. See View overall health of the stack on page 460.

To add a device to the stack configuration

1. Place the stack in Intrinsic HA L2FB. See Enable or disable Intrinsic HA L2FB on the stack on page 478.
2. Install the AOC cables to add the device to the stacking bus. See Install the stacking components on page 440.
3. Add the stacking device to the SMS. See Add the stacking devices to the SMS on page 442.
4. Add the device to the stack in the SMS (see the next procedure).
5. Distribute the inspection profile to the stack. For more information, see Distribute the inspection profile on page 444.
6. Take the stack out of Intrinsic HA L2FB. See Enable or disable Intrinsic HA L2FB on the stack on page 478.

After you add a device to the stack, update any scheduled profile distributions to include the new stack member as a target for the distribution.

Note: For information about where the options are different for managing a stack of devices instead of a single device, see Differences between configuring a stack and a standalone device on page 526.

Note: You must have permission to manage a device in order to add the device to a stack. See Grant permissions to the stack on page 452.

To add a device to the stack in the SMS

1. In the SMS tools, click Devices.
2. In the All Devices workspace, double-click the stack.
3. In the Summary tab, click Add.
4. Select the device to add.
   
   If the device cannot be added to the stack, identify and resolve the issue. For troubleshooting information, see Create the stack on page 443.
5. Click OK.
   
   The stack health is updated. See Verify stack health and synchronization on page 459.
6. If the device you are adding is intended to be the segment reference device (SRD), update the stack configuration to designate the device as the SRD. See Change the segment reference device on page 449.
7. Distribute the inspection profile. See Distribute the inspection profile on page 444.
Delete the stack

Delete the stack to return the devices to the SMS as standalone devices.

After you delete the stack:

- The devices continue to be managed by the SMS.
- Stacking is disabled on each device.
- The inspection policies on all stacking devices are preserved.
- Any scheduled profile distributions continue to run on all the devices that were in the stack.

Note: For information about the differences between configuring a stack of devices compared with configuring a standalone device, see Differences between configuring a stack and a standalone device on page 526.

To delete the stack

1. In the SMS tools, click Devices.
2. In the All Devices workspace, right-click the stack and click Delete Stack.

   The stack is removed and its devices are displayed in All Devices.

Grant permissions to the stack

In the SMS, grant permissions to the stack so that an assigned user group can perform the following functions:

- Create, update, or delete the stack
- Add a device to or remove a device from the stack

The following information describes how to grant permissions to the stack:

- Add stack management to the user role on page 452
- Grant the user group access to the stack on page 453

Add stack management to the user role

In the SMS, grant permission to a user role to manage a stack.

This capability requires the user group to also have access to the stack. See Grant the user group access to the stack on page 453.

To update the user role

1. In the SMS tools, click Admin.
2. In the left navigation pane, expand Authentication and Authorization > Roles.
3. In the **User Roles** workspace, select the user role and click **Edit**.
4. In **Capabilities** options, click **Devices**.
5. Select the **Device Group/Stack Management** capability.

Grant the user group access to the stack

In the SMS, grant the user group access to the stack. With access to the stack, and permission to manage the stack, the user group can perform basic operations on the stack.

**To grant the user group access to the stack**

1. In the SMS tools, click **Admin**.
2. In the left navigation pane, expand **Authentication and Authorization > Groups**.
3. In the **User Groups** workspace, select the user group you want and click **Edit**.
4. In **Devices** options, select each stack you want from the list of devices.

**Distribute a TOS update**

Distribute a TOS update to the stack so that each stack member is updated with the same TOS version.

(Best Practice) Before you distribute a TOS update, enable Intrinsic HA L2FB on the stack. Installing a new software package forces a reboot of each stacking device, but Intrinsic HA L2FB remains enabled until the stack master confirms that there are enough devices in the stack that are ready to inspect (RTI). For more information, see *Enable or disable Intrinsic HA L2FB on the stack* on page 478.

Distribute a TOS update to the stack using the same steps you would follow for a standalone TippingPoint TX Series TPS. For more information, see *Distribute the TOS* on page 340.

Use the **Sync Health** tab to verify that the same TOS version is installed on each stacking device. For more information, see *Verify stack synchronization* on page 468.

**Note:** If the TOS update does not install properly on a stack member, distribute the TOS update to the stack again. If the stacking device has issues, remove it from the stack to make any updates, and then add the device to the stack. For more information, see *Remove a device from the stack* on page 450.

**Troubleshooting**

Use the following information to identify and resolve stacking issues:

- *Verify AOC cable installation* on page 454
- *View stacking status* on page 455
- *Verify stack health and synchronization* on page 459
- *Resolve issues adding a device to the stack* on page 475
- *View stacking tier statistics* on page 476
• *Enable or disable Intrinsic High Availability Layer-2 Fallback* on page 478
• *CLI commands for stacking* on page 480

**Verify AOC cable installation**

The following information describes how to verify the AOC cable installation. Also, you can use this information to verify the installation of a QSFP+ transceiver.

**Examples of an SP port with the AOC cable installed**

The following example shows an SP port with the AOC cable installed correctly.

**Figure 8. TippingPoint TX Series TPS – SP port with the AOC cable installed correctly**
The next example shows an SP port with the AOC cable installed incorrectly.

**Figure 9. TippingPoint TX Series TPS – SP port with the AOC cable partially inserted upside down**

View stacking status

In the SMS, use the Devices workspace to view and manage the stack and its devices.

See [Devices](#) on page 282.

Device details

In the SMS, the All Devices workspace provides a consolidated view of information and configuration settings for the stack and individual stack members. Click Stack State to view stacking details and verify stack health.

The following information describes the device detail states for a stack.
**Stack is normal**

The stack state is normal.

**Stack with a device in Intrinsic HA L2FB**

The 🔄 icon indicates that a device is in Intrinsic HA L2FB.
Stack with an unmanaged device

The ❌ icon indicates that the smstx1002 device is unmanaged by the SMS and another device could be in Intrinsic HA L2FB. The navigation pane indicates that the smstx1001 device is the segment reference device (SRD) for the stack.

Stack with an unmanaged device that is also in Intrinsic HA L2FB

The ⚠ icon and the ❌ icon indicate that a device is not managed by the SMS and another can be in Intrinsic HA L2FB.
Stack is in Intrinsic HA L2FB

The ⚠️ icon indicates the stack is in Intrinsic HA L2FB.

Front panel stacking LEDs

Use the front panel stacking LEDs to identify the stacking status on the device:

- **Stack**: Indicates whether stacking is enabled on the device. Stacking is automatically enabled when you use the SMS to add the device to the stack. If necessary, remove the device from the stack and then add it again to enable stacking. LED color indicates the following states:
  - **Solid green**: Indicates that the device is RTI and is inspecting network traffic.
  - **Off**: Indicates that stacking is not enabled on the device.

- **Stack Master**: Indicates whether the device is the stack master. The stack master is a device role that is responsible for managing stack configuration and states. The stack master is automatically elected by the devices in the stack. All stack members are eligible for election to stack master.
  - **Solid green**: Indicates that the device is the stack master.
  - **Off**: Indicates that the device is not the stack master.

The following example shows the stacking LEDs on the front of each device in the stack:
Device shelf-level graphic

In the SMS, use the device shelf-level graphic to identify the stacking status on the device:

- The **STK** LED indicates whether stacking is enabled. If the **STK** LED is green, stacking is enabled.

**Verify stack health and synchronization**

Use the SMS to identify and resolve stack health and synchronization issues. In the **All Devices** workspace, double-click the stack to view its status information:

- Use the **Summary** tab to verify the health of the stack. The icon on the **Summary** tab indicates the most severe status for the stack. If the stack is in a degraded state, use the Stack Members table to troubleshoot and resolve any issues.

  (Best Practice) Perform stack health troubleshooting steps in the following order:

  a. *View overall health of the stack* on page 460
  b. *Verify stacking bus state* on page 462
  c. *Verify stack member state* on page 465
  d. *Verify device state* on page 466
• Use the **Sync Health** tab to verify the synchronization status of each device in the stack. The icon on the **Sync Health** tab indicates the most severe synchronization status for the stack. If synchronization is in a degraded state, use the Issues table to troubleshoot and resolve any issues. For more information, see *Verify stack synchronization* on page 468.

**View overall health of the stack**

The **Summary** tab displays the current stack configuration, overall stack state, and the status of the stacking bus topology. If the status of the stack is not green (normal), identify and resolve any issues.

**To view overall health of the stack**

1. In the SMS tools, click **Devices**.
2. In the **All Devices** workspace, double-click the stack.
3. In the **Summary** tab, use the stack health summary information to identify the current health of the stack and its configuration.
   
   ◦ **Stack name** — Indicates the name of the stack. Click **Edit** to rename the stack.
   
   ◦ **Stack state** — Indicates the current state of the stack as reported by the segment reference device.

   **Note:** If the Stacking State is not normal, use the **Stack Port A** and **Stack Port B** columns, along with the **Status** column, to troubleshoot and resolve any issues.

   The following information provides SP port status information and suggested actions.

**Table 105. SP port status**

<table>
<thead>
<tr>
<th>Status</th>
<th>Information</th>
<th>Suggested action</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Ready to Inspect - Normal" /></td>
<td>Indicates that the stack is working correctly.</td>
<td>No action is required.</td>
</tr>
<tr>
<td><img src="image" alt="Not Ready to Inspect - Unknown" /></td>
<td>Indicates that the stack is not inspecting traffic for an unknown reason.</td>
<td>This is a transitory state and no action is required.</td>
</tr>
<tr>
<td><img src="image" alt="Not Ready to Inspect - Rebooting" /></td>
<td>Indicates that the stack is not inspecting traffic because one or more of the stack members is rebooting.</td>
<td>This is a transitory state and no action is required.</td>
</tr>
<tr>
<td>Status</td>
<td>Information</td>
<td>Suggested action</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
<td>-----------------</td>
</tr>
<tr>
<td><img src="image" alt="Not Ready to Inspect - Layer 2 Fallback" /></td>
<td>Indicates that the stack is not inspecting traffic because one or more of the devices is stuck in Intrinsic HA L2FB.</td>
<td>At a minimum, reboot the device. If the device returns to this state, a hardware-related issue is likely.</td>
</tr>
<tr>
<td><img src="image" alt="Not Ready to Inspect - Recoverable Layer 2 Fallback" /></td>
<td>Indicates that the stack is not inspecting traffic because one or more of the devices is waiting for you to disable Intrinsic HA L2FB.</td>
<td>Disable Intrinsic HA L2FB on the stack. See Enable or disable Intrinsic HA L2FB on the stack on page 478.</td>
</tr>
<tr>
<td><img src="image" alt="Not Ready to Inspect - Invalid" /></td>
<td>Indicates that the stack is not inspecting traffic because one or more devices has not completed the boot sequence.</td>
<td>Validate that each device has completed its boot sequence. To validate a particular device, log in to its serial interface and look for Run Level 12 in the boot sequence. If necessary, reboot the device.</td>
</tr>
<tr>
<td><img src="image" alt="Ready to Inspect - Layer 2 Fallback" /></td>
<td>Indicates that the stack is in Intrinsic HA L2FB but can return to Ready to Inspect - Normal when the stack master determines that the minimum number of devices are ready to inspect.</td>
<td>Depending on whether you configured the stack for resiliency, all but one of the stack members, or all of the stack members must declare they are Ready to Inspect - Normal before the stack master returns the stack to Ready to Inspect - Normal. See Enable or disable stack resiliency on page 448.</td>
</tr>
</tbody>
</table>

- **Stacking bus** — Indicates the current state of the stacking bus topology.
The following information provides stacking bus status information and suggested actions.

Table 106. Stacking bus topology state

<table>
<thead>
<tr>
<th>Status</th>
<th>Information</th>
<th>Suggested Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connected in a ring</td>
<td>Indicates that the AOC cables are installed correctly.</td>
<td>No action is required.</td>
</tr>
<tr>
<td>Not Connected in a ring</td>
<td>Indicates that the AOC cables are not installed correctly.</td>
<td>Verify the stacking bus health.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See Verify stacking bus state on page 462. See also, Install the stacking components on page 440.</td>
</tr>
</tbody>
</table>

- **Stack Resilience** — Indicates whether the stack goes into Intrinsic HA L2FB if a single device is not ready to inspect (NRTI). See Enable or disable Intrinsic High Availability Layer-2 Fallback on page 478.

- **Segment Reference Device** — Indicates the network segment device that the SMS uses as a reference to manage the inspection policy across each segment of the stack. Click **Edit** to change the segment reference device.

- **Stack Members (N)** — Indicates the number of TippingPoint IPS devices that belong to the stack configuration in the SMS.

  **Note:** For information about the devices that are linked together in the stacking bus, use the **Stack Port A** and **Stack Port B** columns. See Verify stacking bus state on page 462.

Verify stacking bus state

The **Summary** tab displays stacking bus health by checking the state of the SP ports and the state of the stack topology on each device. If the status of the stacking bus is not green (normal), identify and resolve any issues.

**To verify stacking bus state**

1. In the SMS tools, click **Devices**.
2. In the **All Devices** workspace, double-click the stack.
3. In the **Summary** tab, verify stacking is enabled on each device and the status of SP port connectivity:

   - **Enabled** — Indicates whether stacking is enabled or disabled.

      Stacking is automatically enabled when you add a device to the stack. If necessary, remove the device from the stack and then add it to the stack to enable stacking.
Stack Port A and Stack Port B — Indicate the SP port connectivity. See also, Device shelf-level graphic on page 459.

The following information provides SP port status information and suggested actions.

<table>
<thead>
<tr>
<th>Status</th>
<th>Information</th>
<th>Suggested action</th>
</tr>
</thead>
<tbody>
<tr>
<td>devicename</td>
<td>Indicates the device to which the SP port is resolved.</td>
<td>No action is required.</td>
</tr>
<tr>
<td>&lt;No Peer&gt;</td>
<td>Indicates a peer device is not connected to the SP port.</td>
<td>Validate that the SP port is connected to a SP port on a peer device. See Install the stacking components on page 440.</td>
</tr>
<tr>
<td></td>
<td>Indicates the peer device that is connected to the SP port does not have stacking enabled.</td>
<td>Validate that stacking is enabled on the peer device. See View overall health of the stack on page 460.</td>
</tr>
<tr>
<td>&lt;Unknown&gt; (mac-address-hex)</td>
<td>Indicates the peer device that is connected to the SP port is not managed by the SMS.</td>
<td>Add the peer device to the SMS. See Add the stacking devices to the SMS on page 442.</td>
</tr>
<tr>
<td>No peer information is available</td>
<td>Indicates no stacking information was returned from a peer device.</td>
<td>Verify that the SP port is connected to the same stacking bus as the segment reference device.</td>
</tr>
</tbody>
</table>

4. Use the Status column to verify the stack topology state.

The following information provides stack topology status information and suggested actions.
Table 108. Stack topology status

<table>
<thead>
<tr>
<th>Status</th>
<th>Information</th>
<th>Suggested action</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Segment Reference" /></td>
<td>Indicates that the device has been designated as the segment reference device and is ready for stacking.</td>
<td>No action is required.</td>
</tr>
<tr>
<td><img src="image" alt="Normal" /></td>
<td>Indicates that the device is functioning normally.</td>
<td>No action is required.</td>
</tr>
<tr>
<td><img src="image" alt="Missing peer" /></td>
<td>Indicates a peer device is not connected to the SP port.</td>
<td>Validate that the SP port is connected to a peer device. See Install the stacking components on page 440.</td>
</tr>
<tr>
<td><img src="image" alt="Peer {device-name} is not a stack member" /></td>
<td>Indicates that a device SP port references a device that is not actually a part of the stack. This message appears once for each SP port.</td>
<td>Validate that stacking is enabled on the peer device.</td>
</tr>
<tr>
<td><img src="image" alt="Not in stack" /></td>
<td>Indicates that the device is not in the stack topology.</td>
<td>Validate that the SP port is connected to a peer device that is a member of the stack. See Install the stacking components on page 440.</td>
</tr>
<tr>
<td><img src="image" alt="Wrong I/O Modules in slot(s) {slot numbers}" /></td>
<td>Indicates that there is an I/O module on the device that does not match the I/O module in the segment reference device.</td>
<td>Verify that the slot on the device is configured with the same network I/O module or no network I/O module</td>
</tr>
</tbody>
</table>
Verify stack member state

The **Summary** tab displays the state of each stack member as reported by the device. If the status of a stack member is not green (normal), identify and resolve any issues.

**To verify stack member state**

1. In the SMS tools, click **Devices**.
2. In the **All Devices** workspace, double-click the stack.
3. In the **Summary** tab, use the **Stack Member State** column to verify the stack member status.

The following information provides stack member status information and suggested actions.

### Table 109. Stack member status

<table>
<thead>
<tr>
<th>Status</th>
<th>Information</th>
<th>Suggested action</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="Image" alt="RTI - Normal" /></td>
<td>Indicates that the stack member is working correctly.</td>
<td>No action is required.</td>
</tr>
<tr>
<td><img src="Image" alt="NRTI - Unknown" /></td>
<td>Indicates that the stack member is not inspecting traffic for an unknown reason.</td>
<td>This is a transitory state and no action is required.</td>
</tr>
<tr>
<td>Status</td>
<td>Information</td>
<td>Suggested action</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>NRTI - Rebooting</td>
<td>Indicates that the stack member is not inspecting traffic because it is rebooting.</td>
<td>This is a transitory state and no action is required.</td>
</tr>
<tr>
<td>NRTI - L2FB</td>
<td>Indicates that the stack member is not inspecting traffic because it is stuck in Intrinsic HA L2FB.</td>
<td>At a minimum, reboot the device. If the device returns to this state, a hardware-related issue is likely.</td>
</tr>
<tr>
<td>NRTI - L2FB, Recoverable</td>
<td>Indicates that the stack member is not inspecting traffic because it is waiting for you to disable Intrinsic HA L2FB.</td>
<td>Disable Intrinsic HA L2FB on the stack. See <em>Intrinsic HA</em> on page 478.</td>
</tr>
<tr>
<td>RTI - L2FB</td>
<td>Indicates that the stack member is in Intrinsic HA L2FB but can return to Ready to Inspect - Normal when the stack master determines that the minimum number of devices are ready to inspect.</td>
<td>Depending on whether you configured the stack for resiliency, all but one of the stack members, or all of the stack members must declare they are Ready to Inspect - Normal before the stack master returns the stack to Ready to Inspect - Normal. See <em>Enable or disable stack resiliency</em> on page 448.</td>
</tr>
</tbody>
</table>

**Verify device state**

The **Summary** tab displays the state of each device. If the status of a device is not green (normal), identify and resolve any issues.

**To verify device state**

1. In the SMS tools, click **Devices**.
2. In the **All Devices** workspace, double-click the stack.
3. In the **Summary** tab, use the **Device State** column to verify the device status.

   The following information provides device status information and suggested actions.
### Table 110. Device status

<table>
<thead>
<tr>
<th>Status</th>
<th>Information</th>
<th>Suggested action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Normal</td>
<td>Indicates that the device is working normally.</td>
<td>No action is required.</td>
</tr>
<tr>
<td>Updating</td>
<td>Indicates that the device is updating its status.</td>
<td>This is a transitory state and no action is required.</td>
</tr>
<tr>
<td>Unmanaged</td>
<td>Indicates the device is not managed by the SMS.</td>
<td>In the SMS, manage the device:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>a. In SMS tools, click Devices.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>b. Right-click the unmanaged device and click Edit &gt; Manage Device.</td>
</tr>
<tr>
<td>Not Communicating</td>
<td>Indicates that the device is not communicating across the management network with the SMS.</td>
<td>Verify network connectivity between the SMS and the device. Also, verify the required ports are not blocked.</td>
</tr>
<tr>
<td>Layer 2 Fallback</td>
<td>Indicates that the device is not inspecting traffic because Intrinsic HA L2FB is enabled.</td>
<td>If you enabled Intrinsic HA L2FB on the device, disable Intrinsic HA L2FB. See Intrinsic HA on page 479.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If you cannot disable Intrinsic HA L2FB, determine whether stacking has put the device into Intrinsic HA L2FB. See Verify stack member state on page 465.</td>
</tr>
<tr>
<td>Rebooting</td>
<td>Indicates that the device has started a reboot based on a request from the SMS.</td>
<td>This is a transitory state and no action is required.</td>
</tr>
</tbody>
</table>
Verify stack synchronization

The **Sync Health** tab displays stack synchronization status. For example, synchronization status indicates whether the same TippingPoint Operating System (TOS) version is installed on each device. If the status of the synchronization health is not green (normal), identify and resolve any issues.

There are configuration items that should match across each segment of the stack. For example, virtual segments and segment group membership should be the same. Profiles must be the same on corresponding segments. If they do not match, the SMS indicates the mismatch and shows the stack health degraded.

**To verify stack synchronization**

1. In the SMS tools, click **Devices**.
2. In the **All Devices** workspace, double-click the stack.
3. Click the **Sync Health** tab.
4. Use the **Status For** and **Issue** columns to identify synchronization issues.

The following information provides synchronization status information and suggested actions.

**Table 111. Stack synchronization status**

<table>
<thead>
<tr>
<th>Stack information</th>
<th>Information</th>
<th>Suggested Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>TOS</td>
<td>Indicates the TippingPoint Operating System (TOS) version for each of the devices.</td>
<td>Distribute the TOS version to the stack.</td>
</tr>
<tr>
<td></td>
<td>Critical indicator: Mismatch in versions or distribution.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Tip:</strong> To filter synchronization information by this type of issue, use the Type column to filter by TOS Versions.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> For information about where the options are different for managing a stack of devices instead of a single device, see <em>Differences between configuring a stack and a standalone device</em> on page 526.</td>
<td></td>
</tr>
<tr>
<td>Digital Vaccine</td>
<td>Indicates the Digital Vaccine (DV) version for each of the devices.</td>
<td>Distribute the DV package to the stack.</td>
</tr>
<tr>
<td></td>
<td>Major indicator: Mismatch in versions or distribution.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> For information about where the options are different for managing a stack of devices instead of a single device, see <em>Differences between configuring a stack and a standalone device</em> on page 526.</td>
<td></td>
</tr>
<tr>
<td>Stack information</td>
<td>Information</td>
<td>Suggested Action</td>
</tr>
<tr>
<td>-------------------</td>
<td>-------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>Tip: To filter synchronization information by this type of issue, use the Type column to filter by Digital Vaccines.</td>
<td>Indicates the ThreatDV version of a specific ThreatDV subtype for each of the devices. If a ThreatDV subtype has not been distributed to a device, the cell value is &lt;None&gt;. Major indicator: Mismatch in versions or distribution. If a ThreatDV subtype is not distributed to any devices, it is not displayed. Tip: To filter synchronization information by this type of issue, use the Type column to filter by ThreatDV Versions.</td>
<td>Distribute the ThreatDV package to the stack.</td>
</tr>
<tr>
<td>![aux-dv-sub type-name] ThreatDV Versions</td>
<td></td>
<td>Note: For information about where the options are different for managing a stack of devices instead of a single device, see Differences between configuring a stack and a standalone device on page 526.</td>
</tr>
<tr>
<td>![dvt-name] Digital Vaccine Toolkit (DVT) version of a specific DVT for each of the devices. If a DVT has not been distributed to a device, the cell value is &lt;None&gt;. Major indicator: Mismatch in distributions (not versions). If a DVT is not distributed to any devices, it is not displayed.</td>
<td>Distribute the DVToolkit package to the stack.</td>
<td></td>
</tr>
<tr>
<td>Note: For information about where the options are different for managing a stack of devices instead of a single device, see Differences between configuring a stack and a standalone device on page 526.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Stack information</td>
<td>Information</td>
<td>Suggested Action</td>
</tr>
<tr>
<td>-------------------</td>
<td>-------------</td>
<td>-----------------</td>
</tr>
<tr>
<td><strong>Tip:</strong> To filter synchronization information by this type of issue, use the Type column to filter by DVToolkit Versions.</td>
<td><strong>Tip:</strong> To filter synchronization information by this type of issue, use the Type column to filter by DVToolkit Versions.</td>
<td>Distribute the profile to the physical segment.</td>
</tr>
<tr>
<td><strong>Indicates the</strong> {profile name} {profile-version} <strong>was distributed to a physical segment on each of the devices.</strong></td>
<td><strong>Indicates the</strong> {profile-name} {profile-version} <strong>was distributed to a physical segment on each of the devices.</strong></td>
<td><strong>Note:</strong> For information about where the options are different for managing a stack of devices instead of a single device, see <em>Differences between configuring a stack and a standalone device</em> on page 526.</td>
</tr>
<tr>
<td><strong>Major indicator:</strong> Mismatch between profile name, profile version, or distribution.</td>
<td><strong>Major indicator:</strong> Mismatch between profile name, profile version, or distribution.</td>
<td><strong>Note:</strong> For information about where the options are different for managing a stack of devices instead of a single device, see <em>Differences between configuring a stack and a standalone device</em> on page 526.</td>
</tr>
<tr>
<td><strong>Major indicator:</strong> <em>unknown</em></td>
<td><strong>Major indicator:</strong> <em>unknown</em></td>
<td><strong>Note:</strong> For information about where the options are different for managing a stack of devices instead of a single device, see <em>Differences between configuring a stack and a standalone device</em> on page 526.</td>
</tr>
<tr>
<td><strong>Tip:</strong> To filter synchronization information by this type of issue, use the Type column to filter by Physical Segment's Profiles.</td>
<td><strong>Tip:</strong> To filter synchronization information by this type of issue, use the Type column to filter by Physical Segment's Profiles.</td>
<td></td>
</tr>
<tr>
<td><strong>Indicates the</strong> {profile-name} {profile-version} <strong>was distributed to a virtual segment on each of the devices.</strong></td>
<td><strong>Indicates the</strong> {profile-name} {profile-version} <strong>was distributed to a virtual segment on each of the devices.</strong></td>
<td>Distribute the profile to the virtual segment.</td>
</tr>
<tr>
<td><strong>Major indicator:</strong> Mismatch between profile name, profile version, or distribution.</td>
<td><strong>Major indicator:</strong> Mismatch between profile name, profile version, or distribution.</td>
<td><strong>Note:</strong> For information about where the options are different for managing a stack of devices instead of a single device, see <em>Differences between configuring a stack and a standalone device</em> on page 526.</td>
</tr>
<tr>
<td><strong>Major indicator:</strong> <em>unknown</em></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Indicates the</strong> {profile-name} {profile-version} <strong>was distributed to a virtual segment on each of the devices.</strong></td>
<td><strong>Indicates the</strong> {profile-name} {profile-version} <strong>was distributed to a virtual segment on each of the devices.</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Major indicator:</strong> Mismatch between profile name, profile version, or distribution.</td>
<td><strong>Major indicator:</strong> Mismatch between profile name, profile version, or distribution.</td>
<td></td>
</tr>
<tr>
<td><strong>Major indicator:</strong> <em>unknown</em></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Indicates the</strong> {profile-name} {profile-version} <strong>was distributed to a virtual segment on each of the devices.</strong></td>
<td><strong>Indicates the</strong> {profile-name} {profile-version} <strong>was distributed to a virtual segment on each of the devices.</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Major indicator:</strong> Mismatch between profile name, profile version, or distribution.</td>
<td><strong>Major indicator:</strong> Mismatch between profile name, profile version, or distribution.</td>
<td></td>
</tr>
<tr>
<td><strong>Major indicator:</strong> <em>unknown</em></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Stack information</td>
<td>Information</td>
<td>Suggested Action</td>
</tr>
<tr>
<td>-------------------</td>
<td>-------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>Major indicator <img src="image" alt="Mismatch" /> Mismatch between profile name, profile version, or distribution is displayed. There is one row for each virtual segment. <strong>Tip:</strong> To filter synchronization information by this type of issue, use the Type column to filter by Virtual Segment's Profiles.</td>
<td>Edit and save the virtual segment to update the stack. <strong>Note:</strong> For information about where the options are different for managing a stack of devices instead of a single device, see <a href="#">Differences between configuring a stack and a standalone device</a> on page 526.</td>
<td></td>
</tr>
<tr>
<td><img src="image" alt="Missing" /> {virtual-segment-name}</td>
<td>Indicates a virtual segment exists on the SRD but is missing from all the other stack members. Critical indicator <img src="image" alt="Missing" />: There is one missing virtual segment row for each virtual segment on the SRD that is not on any of the other member devices. <strong>Tip:</strong> To filter synchronization information by this type of issue, use the Type column to filter by Missing Virtual Segment.</td>
<td>Edit and save the virtual segment to update the stack. <strong>Note:</strong> For information about where the options are different for managing a stack of devices instead of a single device, see <a href="#">Differences between configuring a stack and a standalone device</a> on page 526.</td>
</tr>
<tr>
<td><img src="image" alt="Extra" /> {virtual-segment-name}</td>
<td>Indicates an extra virtual segment exists on one of the stack members but is missing from the SRD. Critical indicator <img src="image" alt="Extra" />: There is one extra virtual segment row for each virtual segment that is not in the segment reference device but is in one of the other devices in the stack.</td>
<td>Delete the extra virtual segment if it is not applicable. Or, edit and save the virtual segment to update the stack. <strong>Note:</strong> For information about where the options are different for managing a stack of devices instead of a single device, see <a href="#">Differences between configuring a stack and a standalone device</a> on page 526.</td>
</tr>
<tr>
<td>Stack information</td>
<td>Information</td>
<td>Suggested Action</td>
</tr>
<tr>
<td>-------------------</td>
<td>-------------</td>
<td>-----------------</td>
</tr>
<tr>
<td><strong>Mismatched group for</strong> (\text{virtual-segment-name})</td>
<td>Indicates the (\text{Mismatch}) (\text{group-name}) to which a virtual segment belongs for each of the devices. Critical indicator (\text{Mismatch}) displayed. There is one row for each virtual segment that has a mismatch in segment groups. <strong>Tip:</strong> To filter synchronization information by this type of issue, use the Type column to filter by (\text{Virtual Segment's Group}).</td>
<td>Edit and save the segment group (without making any changes) to update the segment group with all of its segments. <strong>Note:</strong> For information about where the options are different for managing a stack of devices instead of a single device, see <em>Differences between configuring a stack and a standalone device</em> on page 526.</td>
</tr>
<tr>
<td><strong>Mismatched group for</strong> (\text{physical-segment-name})</td>
<td>Indicates the (\text{Mismatch}) (\text{group-name}) to which a physical segment belongs for each of the devices. Critical indicator (\text{Mismatch}) displayed. There is one row for each physical segment that has a mismatch in segment groups. <strong>Tip:</strong> To filter synchronization information by this type of issue, use the Type column to filter by (\text{Physical Segment's Group}).</td>
<td>Edit and save the segment group (without making any changes) to update the segment group with all of its segments. <strong>Note:</strong> For information about where the options are different for managing a stack of devices instead of a single device, see <em>Differences between configuring a stack and a standalone device</em> on page 526.</td>
</tr>
<tr>
<td>Stack information</td>
<td>Information</td>
<td>Suggested Action</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Extra rule {inspection-bypass-rule-name}</td>
<td>Indicates that there is an inspection bypass rule on a stacking device that is not on the SRD.</td>
<td>Edit and save the inspection bypass rule (without making any changes) to update the stack.</td>
</tr>
<tr>
<td></td>
<td>Critical indicator [Mismatch displayed.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>There is one row for each inspection bypass rule.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Tip:</strong> To filter synchronization information by this type of issue, use the Type column to filter by Extra Rule.</td>
<td></td>
</tr>
<tr>
<td>Missing {inspection-bypass-rule-name}</td>
<td>Indicates that there is an inspection bypass rule on the SRD that is missing from a device in the stack.</td>
<td>Edit and save the inspection bypass rule (without making any changes) to update the stack.</td>
</tr>
<tr>
<td></td>
<td>Critical indicator [Mismatch displayed.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>There is one row for each inspection bypass rule.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Tip:</strong> To filter synchronization information by this type of issue, use the Type column to filter by Missing Rule.</td>
<td></td>
</tr>
<tr>
<td>Stack Resilience {stack-resilience-value}</td>
<td>Indicates that there is at least one device that has a different Stack Resilience option than what is configured for the stack in the SMS.</td>
<td>Edit and save the stack configuration (without making any changes) to update all of the stacking devices.</td>
</tr>
<tr>
<td>Stack information</td>
<td>Information</td>
<td>Suggested Action</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Tip:</strong></td>
<td>To filter synchronization information by this type of issue, use the Type column to filter by Device Resilience Mismatch.</td>
<td></td>
</tr>
<tr>
<td>SSL Enabled</td>
<td>Indicates that SSL inspection is enabled on some of the devices in the stack but not all of them.</td>
<td>Edit the device configuration on each stacking device to verify that SSL inspection is enabled (<a href="#">Devices &gt; All Devices &gt; device-name &gt; Device Configuration</a>). For more information, see the <a href="#">Security Management System User Guide</a>.</td>
</tr>
<tr>
<td>SSL Licensed</td>
<td>Indicates that some of your devices have a license that allows SSL inspection and others that do not allow SSL inspection.</td>
<td>Update your license package to assign a product capability that you have purchased, such as SSL inspection, to each stacking device. When you install the license package on the device, be sure to reboot the device and apply the license update for SSL inspection. Go the TMC at <a href="https://tmc.tippingpoint.com">https://tmc.tippingpoint.com</a> to review and manage the capabilities in your license package.</td>
</tr>
<tr>
<td>License Throughput</td>
<td>Indicates that some of your devices have a license for a different inspection throughput rate than the other devices.</td>
<td>Update your license package to assign a product capability that you have purchased, such as inspection throughput, to a particular security device. Go the TMC at <a href="https://tmc.tippingpoint.com">https://tmc.tippingpoint.com</a> to review and manage the capabilities in your license package.</td>
</tr>
<tr>
<td>Extra VLAN</td>
<td>Indicates that there is a VLAN translation rule on a stacking device that is not on the SRD.</td>
<td>Remove the device from the stack, restore the device to its original settings, and then add the device to the stack.</td>
</tr>
</tbody>
</table>
There is one row for each VLAN translation rule.

**Tip:** To filter synchronization information by this type of issue, use the Type column to filter by Extra VLAN.

There is one row for each VLAN translation rule.

**Tip:** To filter synchronization information by this type of issue, use the Type column to filter by Missing VLAN.

Indicates that there is a VLAN translation on the SRD that is missing from a device in the stack.

If necessary, edit the VLAN translation mappings for the SRD to include the VLAN translation mapping from the stacking device.

Edit and save the VLAN translation mapping on the SRD (without making any changes) to update all of the stacking devices.

---

### Resolve issues adding a device to the stack

The following information describes how to identify and resolve issues with adding a device to the stack configuration in the SMS.

The following information provides device status and suggested actions for adding a device to the stack.

#### Table 112. Device status – adding a device to the stack

<table>
<thead>
<tr>
<th>Status</th>
<th>Information</th>
<th>Suggested action</th>
</tr>
</thead>
<tbody>
<tr>
<td>🟢 Ready for stacking</td>
<td>Indicates that there is no issue with adding the device to the stack.</td>
<td>No action is required.</td>
</tr>
<tr>
<td>🟥 This device's TOS version doesn't match the TOS version for the selected devices.</td>
<td>Indicates that there is a TOS version mismatch.</td>
<td>The TippingPoint Operating System (TOS) version must be the same on each device in the stack. If necessary, install a</td>
</tr>
<tr>
<td>Status</td>
<td>Information</td>
<td>Suggested action</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
<td>------------------</td>
</tr>
<tr>
<td><img src="image" alt="This device does not support stack sizes of more than ## devices." /></td>
<td>Indicates a device is valid for stacking, but that the maximum number of devices in the stack has been reached.</td>
<td>Remove a device from the stack so that you can add the device. See <a href="#">Remove a device from the stack</a> on page 450.</td>
</tr>
<tr>
<td><img src="image" alt="Device is not communicating" /></td>
<td>Indicates that the device is not communicating with the SMS.</td>
<td>Verify network connectivity between the SMS and the device. Also, verify the required ports are not being blocked.</td>
</tr>
<tr>
<td><img src="image" alt="Device is unmanaged" /></td>
<td>Indicates that the device is no longer managed by the SMS.</td>
<td>In the SMS, manage the device: 1. In SMS tools, click <strong>Devices</strong>. 2. Right-click the unmanaged device and click <strong>Edit &gt; Manage Device</strong>.</td>
</tr>
</tbody>
</table>

### View stacking tier statistics

In the SMS, use the stacking tier statistics to view stacking (Tier S) data for a stacking device in addition to device tiers 1–4. Tier S data includes stacking data from the SP ports.

The tier statistics area provides information on packets and speed as measured in Mbps by tier.

<table>
<thead>
<tr>
<th>Inspection Tier</th>
<th>Information</th>
</tr>
</thead>
</table>
| Stack : Segment Ports | This inspection tier presents the total I/O module throughput for the network segment device as well as the receive rates from the I/O module to each stack member.  
When stacking is enabled, the following information is displayed:  
• **Segment Rx Mbps** displays the aggregate received traffic from all network segments on this device. |
## Inspection Tier

<table>
<thead>
<tr>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>• <strong>Segment Tx Mbps</strong> displays the aggregate traffic transmitted from all</td>
</tr>
<tr>
<td>network segments on this device.</td>
</tr>
<tr>
<td>• <strong>Stack Balance (A/B/C)</strong> displays the load balance percentage, in which</td>
</tr>
<tr>
<td>100% equates to perfect balance across the number of devices in the</td>
</tr>
<tr>
<td>stack. For devices that are in Intrinsic HA L2FB, the Rx rate is zero, and</td>
</tr>
<tr>
<td>this zero value is included in the load balance calculation. This statistic</td>
</tr>
<tr>
<td>is similar to the <strong>A/B/C Balance</strong> percentage in Tier 1.</td>
</tr>
<tr>
<td>◦ <strong>&lt;host n&gt; Rx Mbps</strong> displays the traffic balanced from this device's</td>
</tr>
<tr>
<td>network segments to the other devices in the stack.</td>
</tr>
<tr>
<td>Note that the number of packets going through each host is flow-based,</td>
</tr>
<tr>
<td>so it is not uncommon to see a slight difference between them.</td>
</tr>
<tr>
<td>• <strong>Segment ratio to tier 1</strong> displays the percentage of traffic being</td>
</tr>
<tr>
<td>inspected by this device as a ratio of the segment Rx traffic.</td>
</tr>
</tbody>
</table>

## Stack : Stack Ports

This inspection tier presents SP port throughput, including through traffic and return traffic rates.

When stacking is enabled, the following information is displayed:

<table>
<thead>
<tr>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>• <strong>Stack Rx Mbps</strong> displays the aggregate received traffic from both SP</td>
</tr>
<tr>
<td>ports.</td>
</tr>
<tr>
<td>• <strong>Stack Tx Mbps</strong> displays the aggregate traffic that is transmitted from</td>
</tr>
<tr>
<td>both SP ports.</td>
</tr>
<tr>
<td>• <strong>Stack Rx &gt; Stack Tx</strong> displays the total amount of transit or through</td>
</tr>
<tr>
<td>traffic on the SP ports; for example, traffic received on SP 1, which</td>
</tr>
<tr>
<td>is forwarded by the switch to SP 2.</td>
</tr>
<tr>
<td>• <strong>Stack Rx &gt; Seg Tx</strong> displays the amount of return traffic coming in on</td>
</tr>
<tr>
<td>a SP port that is returning to the outbound network segment.</td>
</tr>
<tr>
<td>• <strong>Stack ratio to tier 1</strong> displays the percentage of traffic being</td>
</tr>
<tr>
<td>inspected by this device as a ratio of the stack Rx traffic.</td>
</tr>
</tbody>
</table>

See *Tier statistics for the vTPS, TPS, and IPS (NX-Platform) devices* on page 409.
Enable or disable Intrinsic High Availability Layer-2 Fallback

Intrinsic High Availability (Intrinsic HA) determines how the device manages traffic on each segment in the event of a system failure. Layer-2 Fallback (L2FB) mode either permits or blocks all traffic on each segment, depending on the Intrinsic HA L2FB action setting for the segment. Any permitted traffic is not inspected.

In the SMS, you can enable Intrinsic HA L2FB on a stack member or the entire stack, for example, to perform scheduled maintenance. When you finish, disable Intrinsic HA L2FB to resume normal operation.

Stacking automatically enables and disables Intrinsic HA L2FB on a stack member or the stack as needed, depending on the inspection state of the stack or the devices.

- **Ready to Inspect (RTI)** indicates that a device or the stack is ready to inspect traffic. If enough devices are RTI, the stack master takes the stack out of Intrinsic HA L2FB. See *Enable or disable stack resiliency* on page 448.

- **Not Ready to Inspect (NRTI)** indicates that a device or the stack is not ready to inspect traffic.

  When a device or stack is NRTI, Intrinsic HA L2FB remains enabled until the NRTI cause is resolved. In some cases, NRTI is a temporary recoverable condition and in other cases, NRTI recovery requires manual intervention. See *Verify stack member state* on page 465.

**Tip:** If a device or the stack is in Intrinsic HA L2FB, disable Intrinsic HA L2FB on the stack to restore the stack to Normal mode. If the stack does not return to Normal mode, verify the stack health to determine why the stack is in Intrinsic HA L2FB and resolve any issues. See *Verify stack health and synchronization* on page 459.

Enable or disable Intrinsic HA L2FB on the stack

In the SMS, enable Intrinsic HA L2FB mode on the stack to either permit or block all traffic on each segment of the devices in the stack, depending on the Intrinsic HA L2FB action setting for the segment. When you disable Intrinsic HA L2FB on the stack, any devices in Intrinsic HA L2FB are restored to Normal mode.

To resume normal operation, the stack must validate:

- The minimum number of devices are RTI - Normal. See *Verify stack health and synchronization* on page 459.

- The stack members communicate regularly with the stack master.

  If the number of missed heartbeats exceeds a threshold value, or if the device does not send a heartbeat message within 15 minutes of rebooting, the device is NRTI.

- The same TippingPoint Operating System (TOS) version is installed on each device. See *Verify stack synchronization* on page 468.

If you manually enable Intrinsic HA L2FB on the stack, you must also disable it to resume inspection. If necessary, resolve Intrinsic HA L2FB issues on a device to bring the stack out of Intrinsic HA L2FB.
To enable or disable Intrinsic HA L2FB on the stack

1. In the SMS tools, click **Devices**.

2. In the **All Devices** workspace, right-click the stack and click **Edit > Intrinsic HA**, then choose an option:
   - **Fallback** puts the stack in Intrinsic HA L2FB.
   - **Normal** takes the stack out of Intrinsic HA L2FB.

Enable or disable Intrinsic HA L2FB on a stacking device

In the SMS, enable Intrinsic HA L2FB mode on a stacking device to either permit or block all traffic on each segment, depending on the Intrinsic HA L2FB action setting for the segment. When you disable Intrinsic HA L2FB on the device, Intrinsic HA L2FB is restored to Normal mode.

Before you enable Intrinsic HA L2FB on a stacking device, verify whether the loss of the device would place the entire stack into Intrinsic HA L2FB. See *Enable or disable stack resiliency* on page 448.

To enable or disable Intrinsic HA L2FB on the stacking device

1. In the SMS tools, click **Devices**.

2. In the **All Devices** workspace, double-click the stack.

3. In the left navigation pane, expand the stack.

   If a stacking device is in Intrinsic HA L2FB, the name of the device is appended by **(fallback)**. In the following example, **MyStack** and its stack members are in Intrinsic HA L2FB.
4. Click the device that is in Intrinsic HA L2FB.

The stacking device shelf-level graphic is displayed.

5. In the Device workspace, right-click the shelf-level graphic and click Edit > Intrinsic HA, then choose an option:

- **Fallback** puts the device in Intrinsic HA L2FB.
- **Normal** takes the device out of Intrinsic HA L2FB.

**CLI commands for stacking**

On the IPS, use the Command Line Interface (CLI) to display stacking status information from the device. For more information about stacking-related commands, see the IPS Command Line Interface Reference.

**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>
</tbody>
</table>
### Limitations

When you consider stacking, keep these points in mind:

- The following options, which require state information to be shared across multiple devices, are not supported in a stacking configuration:
  - Transparent HA
  - IPS Quarantine. As a workaround, use SMS Responder to propagate IPS Quarantine to stack members.

  **Note:** For information about the differences between configuring a stack of devices compared with configuring a standalone device, see * Differences between configuring a stack and a standalone device * on page 526.
  - Scan/sweep filters
  - Policy-based rate limits

- The SMS is required to manage the stack and any stack members. You cannot manage the stack from the Local Security Manager (LSM) or CLI on the device.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Information</th>
</tr>
</thead>
<tbody>
<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>
• All stack members must use consistent sets of inspection profiles to ensure inspection policies are applied consistently, regardless of which device inspects the traffic.

**Repurpose a device**

If you have existing TippingPoint 8200TX or 8400TX devices that are not currently deployed in your network, you can repurpose the devices for use in a stack. Also, if you remove a device from a stack, you can repurpose it for use in another stack or as a standalone device.

For information about adding a device to the stack, see *Add a device to the stack* on page 450.

**To repurpose a device**

• Use the `debug factory-reset` command to restore the device to its original settings.

Keep the following items in mind when you repurpose a device for use in a stack:

• The same TippingPoint Operating System (TOS) version, v5.0.0 or later, must be installed on each TX Series device in the stack.

• The same slot on each device must be configured with either the same network I/O module or no network I/O module as compared to the network segment device. For more information, see *Multiple network segment device configuration* on page 446.

**Stacking for IPS**

The information provided describes how to increase inspection capacity by implementing stacking for TippingPoint NX Series Intrusion Prevention System (IPS) devices.

**Overview**

Stacking enables you to increase the overall inspection capacity of your TippingPoint Intrusion Prevention System (IPS) by grouping multiple NX Series devices and pooling their resources.

You can configure up to five NX Series devices in a stack. The stack operates as a single device that you manage on the TippingPoint Security Management System (SMS). All devices in the stack must be the same model, either 7100NX or 7500NX.

In-line inspection capacity increases with each device that you add to the stack. For example, for each 7500NX added to a stack of 7500NX devices, the inspection capacity increases by 20 Gbps.

The following TippingPoint software is supported for stacking:

• **TippingPoint SMS v4.5.0, or later** - Centrally manages each stack of devices.

• **TippingPoint Operating System (TOS) v3.9.0, or later** - Must be installed on each security device.

**Note:** No additional licensing is required to implement stacking.
Not all TippingPoint NX Series IPS features are supported in a stack configuration. See Limitations on page 524.

**Set up the stack**

This information explains how to set up the stack of devices, including basic, resilient, and multiple network segment configurations.

You can customize the stack by adding the number of devices and enabling the features you need.

After you set up a basic stack, you can consider whether to configure it to be a resilient stack. For more information, see Resilient stack configuration on page 488.

For details about how to install your security device, see the Install your security device quick reference card.

**Basic stack configuration**

When you configure a basic stack, every member of the stack must be operational. If any member of a basic stack becomes unavailable, the entire stack becomes unavailable. Use the following information to configure a basic stack:

- Install the stacking components on page 484
- Create the stack in the SMS on page 486

Install the stacking components

An NX Series device stack requires the 40 GbE QSFP+ I/O module to always be installed in slot 4 of each device. You can use slots 1–3 for network I/O modules.

The I/O modules should be installed in the stacking device that you plan to use as the network segment device. A network segment device operates in-line in the network and distributes network traffic to each stack member for inspection. The other stack members do not need network I/O modules.

When you connect the AOC cables, use a ring topology so that each device connects to its peer.

**To install the stacking components**

1. Install the network I/O modules on the network segment device in slots 1–3 so that you can connect the device to the network.
2. Install the 40 GbE QSFP+ I/O module in slot 4 of both devices so that you can connect the devices to the stacking bus.

    The stacking bus consists of a 40 GbE QSFP+ I/O module on each stacking device that connects the stack in a ring topology.

    For more information about how to install I/O modules, see the NX-Platform Hardware Installation and Safety Guide.
3. Install the AOC cables in slot 4 of both devices so that each device connects to its peer in a ring topology.

**Note:** When you install the AOC cable, you should orient the QSFP+ transceiver with the tab on top. The AOC cable is keyed so that it can only be correctly inserted one way. If the cable does not slide in easily and click to latch, it may be upside down. See *Verify AOC cable installation* on page 497 for more information.

Examples with the 40 GbE QSFP+ I/O modules and the AOC cables installed

The following example shows the 40 GbE QSFP+ I/O modules are installed in slot 4 and the AOC cables are installed.

**Figure 13. TippingPoint NX Series IPS – 40 GbE QSFP+ I/O modules are installed in slot 4 and the AOC cables are installed properly**

The next example shows the network I/O modules are installed in slots 1, 2, and 3 of the network segment device (1).

**Figure 14. TippingPoint NX Series IPS – stack with network I/O modules installed in slots 1–3**
Create the stack in the SMS

Use the SMS to create the stack and centrally manage the stacking devices online.

The process is:

Add the stacking devices to the SMS

Create the stack

Distribute the inspection profile

The following information provides more details:

- **Add the stacking devices to the SMS** on page 486
- **Create the stack** on page 486
- **Distribute the inspection profile** on page 488

**Note:** Before you can create the stack in the SMS, you need to set up the stacking components. See *Install the stacking components* on page 484.

**Add the stacking devices to the SMS**

After you install the stacking components, add each device in the stack to the SMS so that you can create and manage the stack online.

For each device, use the SMS to install the required TippingPoint Operating System (TOS) version, v3.9.0 or later. The TOS version must be the same on each NX Series device. For more information, see *Adding, editing, or deleting a device* on page 327.

If you are repurposing an existing device for use in the stack, reset the device to factory settings, and then install the required TOS version. For more information, see *Repurpose a device* on page 525.

**Create the stack**

After you add the stacking devices to the SMS, create the stack in the SMS so that the devices are in the stacking topology. Then, use the Devices options in the SMS to specify the stack configuration.

**Note:** You must have the Device Group/Stack Structure Manager capability assigned to your role to create a stack. See *Authentication and authorization* on page 542.

**To create the basic stack in the SMS with two devices**

1. In the SMS tools, click **Devices**.
2. In the **All Devices** workspace, right-click a stacking device and select **New Stack**.

3. In the **Choose Devices** options, specify the stack name.

   **Figure 15. Choose devices options – stacking devices selected**

4. Choose **Normal** for the Stack Resilience option.

   For information about the **N+1 Redundancy** option, see *Resilient stack configuration* on page 488.

5. Select the checkbox for both devices.

   ◦ If a device is not displayed, validate the following items:
     ◦ The device is not already a member of another stack.
     ◦ The device is the same model as the other selected devices.

   ◦ If either device does not have a **Ready for stacking** status, see *Resolve issues adding a device to the stack* on page 518 for troubleshooting information.

6. Select a network segment device that the SMS uses as a template to create the corresponding segments on each stack member and click **Set as Segment Reference Device**.

7. Click **OK**.

8. In the **All Devices** workspace, double-click the stack shelf-level image to view stack health.

9. In the **Summary** tab, verify the stack health is **Normal**.

   If the stack is not healthy, identify and resolve any issues. See *Verify stack health and synchronization* on page 502.
Distribute the inspection profile

Distribute the inspection profile to the stack by choosing from the segments on the segment reference device (SRD). After you do this, the inspection profile goes to the corresponding segments on each member of the stack.

**Note:** For more information, see *Distribute an inspection profile to inspection segments* on page 145.

After you distribute the inspection profile, use the **Sync Health** tab to identify and resolve any synchronization issues with the stack. See *Verify stack synchronization* on page 511.

The following example shows the profile distribution to the default segment group, which includes all the segments on the stack.

**Figure 16. Distribute the inspection profile to all the segments on the stack**

![Profile Distribution Interface](image)

**Resilient stack configuration**

You can change the configuration of a basic stack to a resilient stack so that the stack continues to inspect network traffic if a single stack member is not ready to inspect (NRTI).

In a **resilient stack**, the network traffic continues to be inspected when a single stack member is NRTI by rebalancing network traffic between the remaining ready to inspect (RTI) devices. For information about how stacking determines whether a device is ready to inspect, see *Enable or disable Intrinsic High Availability Layer-2 Fallback* on page 520.
To enable a resilient stack configuration, follow the same process that is described in Create the stack on page 486, but select the **N+1 Redundancy** Stack Resiliency option.

When all the devices in the stack are RTI, the stack load balances network traffic across all the devices. If a single stack member is NRTI, the stack rebalances network traffic between the remaining RTI devices, reducing inspection capacity.

**Important:** When the stack is configured with a single network segment device, if the network segment device is NRTI, the entire stack is NRTI. To enable the stack to continue to inspect traffic when the network segment device is NRTI, configure multiple network segment devices. See Multiple network segment device configuration on page 489.

The following example shows a resilient stack:

- The network segment device (1) is at the bottom of the stack.
- The network segment device load-balances network traffic from each utilized segment to the other device in the stack.
- The stack continues to inspect if the top device is unavailable.

**Figure 17. TippingPoint NX Series IPS – resilient stack configuration**

**Multiple network segment device configuration**

You can change the device configuration of a resilient stack to include multiple network segment devices. With more than one network segment device, the stack continues to inspect network traffic if any stack member, including a network segment device, becomes unavailable. If any stack member becomes unavailable, the stack rebalances network traffic between the remaining available devices.

**To configure multiple network segment devices**

- Install network I/O modules on each network segment device.
  
  The same slot on each device must be configured with either the **same** network I/O module or **no** network I/O module.
Consider the following items when you configure multiple network segment devices:

- Connect the same networks to the same network segments on each network segment device.
- Traffic can come in both network segment devices as long as the corresponding segment ports of each device are connected to the same networks. For example, port 1–1A on IPS–A and IPS–B are connected to Network A and port 1–1B on IPS–A and IPS–B are connected to Network B.

**Example with multiple network segment devices**

The following example shows a valid two-device stack with both network segment devices connected to the same networks on the same segment ports. Either network segment device can be designated as the segment reference device. Each network segment device load-balances traffic from each utilized segment to the other member of the stack on a per flow basis.

**Figure 18. TippingPoint NX Series IPS – two-device stack with multiple network segment devices**

---

**Update the stack configuration**

In the SMS, update the stack configuration, for example, when you need to add another device to the stack.

**Note:** For information about the differences between configuring a stack of devices compared with configuring a standalone device, see *Differences between configuring a stack and a standalone device* on page 526.

The following information describes several ways that you can update the stack configuration:

- *Enable or disable stack resiliency* on page 491
- *Change the segment reference device* on page 491
- *Replace a device in the stack* on page 492
- *Remove a device from the stack* on page 492
- *Add a device to the stack* on page 493
Enable or disable stack resiliency

Update the stack configuration in the SMS to enable stack resiliency so that the stack can continue to inspect traffic if a single stack member is not ready to inspect (NRTI) network traffic.

When you enable stack resiliency, make sure the stack is configured with enough devices to provide the required inspection capacity. See Resilient stack configuration on page 488.

To enable or disable stack resiliency

1. In the SMS tools, click Devices.
2. In the All Devices workspace, double-click the stack.
3. In the Summary tab, click Edit.
4. In Edit Stack Configuration, select a Stack Resilience option:
   - N+1 Redundancy – This option enables the stack to continue to inspect traffic if a single stack member is NRTI. If more than one device is NRTI, the stack automatically goes into Intrinsic HA L2FB. See also, Enable or disable Intrinsic High Availability Layer-2 Fallback on page 520.
   - Normal – This option automatically places the stack and all of its devices into Intrinsic HA L2FB if a single stack member is NRTI.

Change the segment reference device

Update the stack configuration in the SMS to select the network segment device that the SMS uses as a template to create the corresponding segments on each stack member.

Make sure that the device is configured with the correct network I/O modules, has the correct segment configuration, and has the associated inspection policy.

After you change the segment reference device, distribute the inspection profile to update the stack. For more information, see Distribute the inspection profile on page 488.

To change the segment reference device in the SMS

1. In the SMS tools, click Devices.
2. In the All Devices workspace, double-click the stack.
3. In the Summary tab, click Edit.
4. In Edit Stack Configuration options, select the network segment device from the Segment Reference Device list.
Replace a device in the stack

If a stacking device must be replaced, you can update the stack configuration in the SMS with the replacement device.

If any of the physical segments on the stacking device were renamed, rename the segments on the replacement device. For more information, see Rename segments on page 495.

**To replace a stack member in the SMS**

1. Place the stack in Intrinsic HA L2FB. See Enable or disable Intrinsic HA L2FB on the stack on page 521.
2. Remove the stack member from the stack configuration. See Remove a device from the stack on page 492.

   If the device is designated as the segment reference device (SRD), update the stack configuration to designate a different device as the SRD, and then remove the stack member from the stack configuration. See Change the segment reference device on page 491.

3. Install the AOC cables to remove the old stacking device from the stacking bus and to add the new device. See Install the stacking components on page 484.

   If the device you want to replace is configured with network I/O modules, make sure that the replacement device has the same network I/O modules in the same slots.

4. Manage the new device with the SMS and then add the stacking device to the stack configuration. See Add a device to the stack on page 493.

   If necessary, update the stack configuration to designate the replacement device as the SRD. See Change the segment reference device on page 491.

5. Distribute the inspection profile to the stack. For more information, see Distribute the inspection profile on page 488.

6. Take the stack out of Intrinsic HA L2FB. See Enable or disable Intrinsic HA L2FB on the stack on page 521.

Remove a device from the stack

Remove a device from the stack when you need to decrease inspection capacity, or when you need to replace a device in the stack.

(Best Practice) To reuse a device after it is removed from the stack, either as a standalone device or as part of a different stack, use the debug factory-reset command to restore the device to its original settings. See Repurpose a device on page 525.

**Note:** A stack with a single stack member is supported on a temporary basis, for example, to replace a device in the stack with two devices. However, a single-device stack does not have a normal health status.

**To remove a device from the stack configuration**
1. Place the stack in Intrinsic HA L2FB. See *Enable or disable Intrinsic HA L2FB on the stack* on page 521.
2. Remove the device from the stack in the SMS (see the next procedure).
   
   If the device is designated as the segment reference device (SRD), update the stack configuration to designate a different device as the SRD, then remove the device from the stack configuration. See *Change the segment reference device* on page 491.
3. Install the AOC cables to remove the old stacking device from the stacking bus. See *Install the stacking components* on page 484.
4. Take the stack out of Intrinsic HA L2FB. See *Enable or disable Intrinsic HA L2FB on the stack* on page 521.

**To remove a device from the stack in the SMS**

1. In the SMS tools, click **Devices**.
2. In the **All Devices** workspace, double-click the stack.
3. In the **Summary** tab, select a device from the Stack Member list.
4. Click **Remove**.
5. Click **OK**.
   
   The stack health is updated. See *Verify stack health and synchronization* on page 502.

**Add a device to the stack**

Add a device to the stack when you need to increase the inspection capacity of the stack, or when you need to replace a device in the stack.

(Best Practice) If you are repurposing an existing device for use in the stack, reset the device to factory settings, and then install the required TOS version. See *Repurpose a device* on page 525.

When you add a device to the stack configuration, the SMS automatically enables stacking on the device. If necessary, remove the device from the stack configuration, and then add it again to enable stacking. See *View overall health of the stack* on page 503.

If any of the physical segments on the stack were renamed, if necessary, rename the segments on the new device. For more information, see *Rename segments* on page 495.

**To add a device to the stack configuration**

1. Place the stack in Intrinsic HA L2FB. See *Enable or disable Intrinsic HA L2FB on the stack* on page 521.
2. Install the AOC cables to add the device to the stacking bus. See *Install the stacking components* on page 484.
3. Add the stacking device to the SMS. See *Add the stacking devices to the SMS* on page 486.
4. Add the device to the stack in the SMS (see the next procedure).
5. Distribute the inspection profile to the stack. For more information, see *Distribute the inspection profile* on page 488.
6. Take the stack out of Intrinsic HA L2FB. See *Enable or disable Intrinsic HA L2FB on the stack* on page 521.

After you add a device to the stack, update any scheduled profile distributions to include the new stack member as a target for the distribution.

**Note:** For information about where the options are different for managing a stack of devices instead of a single device, see *Differences between configuring a stack and a standalone device* on page 526.

**Note:** You must have permission to manage a device in order to add the device to a stack. See *Grant permissions to the stack* on page 495.

**To add a device to the stack in the SMS**

1. In the SMS tools, click **Devices**.
2. In the **All Devices** workspace, double-click the stack.
3. In the **Summary** tab, click **Add**.
4. Select the device to add.
   
   If the device cannot be added to the stack, identify and resolve the issue. For troubleshooting information, see *Create the stack* on page 486.
5. Click **OK**.
   
   The stack health is updated. See *Verify stack health and synchronization* on page 502.
6. If the device you are adding is intended to be the segment reference device (SRD), update the stack configuration to designate the device as the SRD. See *Change the segment reference device* on page 491.
7. Distribute the inspection profile

**Delete the stack**

Delete the stack to return the devices to the SMS as standalone devices.

After you delete the stack:

- The devices continue to be managed by the SMS.
- Stacking is **disabled** on each device.
- The inspection policies on all stacking devices are preserved.
- Any scheduled profile distributions continue to run on all the devices that were in the stack.

**Note:** For information about the differences between configuring a stack of devices compared with configuring a standalone device, see *Differences between configuring a stack and a standalone device* on page 526.

**To delete the stack**
1. In the SMS tools, click Devices.
2. In the All Devices workspace, right-click the stack and click Delete Stack.

   The stack is removed and its devices are displayed in All Devices.

**Rename segments**

On slots 1–3, you can rename a physical segment and optionally, propagate that segment name to the corresponding segment on each member of the stack. Slot 4 is reserved for the stacking bus.

(Best Practice) Do not modify segment details other than the segment name. Across the stack, each segment must have the same configuration.

**Tip:** Use the Rename across stacked device segments option to propagate physical segment names across the stack, including any segment that does not have a network I/O module installed.

If you add or replace a stack member, if necessary, update any segment names on the new device. For example, if the new device does not have a network I/O module installed, use the Rename across stacked device segments option to propagate physical segment names across the updated stack configuration.

See Edit TPS/IPS segment details on page 289.

**Grant permissions to the stack**

In the SMS, grant permissions to the stack so that an assigned user group can perform the following functions:

- Create, update, or delete the stack
- Add a device to or remove a device from the stack

The following information describes how to grant permissions to the stack:

- Add stack management to the user role on page 495
- Grant the user group access to the stack on page 496

**Add stack management to the user role**

In the SMS, grant permission to a user role to manage a stack.

This capability requires the user group to also have access to the stack. See Grant the user group access to the stack on page 496.

**To update the user role**

1. In the SMS tools, click Admin.
2. In the left navigation pane, expand Authentication and Authorization > Roles.
3. In the User Roles workspace, select the user role and click Edit.
5. Select the **Device Group/Stack Management** capability.

Grant the user group access to the stack

In the SMS, grant the user group access to the stack. With access to the stack, the user group can perform basic operations on the stack.

**To grant the user group access to the stack**

1. In the SMS tools, click **Admin**.
2. In the left navigation pane, expand **Authentication and Authorization > Groups**.
3. In the **User Groups** workspace, select the user group you want and click **Edit**.
4. In **Devices** options, select each stack you want from the list of devices.

**Distribute a TOS update**

Distribute a TOS update to the stack so that each stack member is updated with the same TOS version.

(Best Practice) Before you distribute a TOS update, enable Intrinsic HA L2FB on the stack. Installing a new software package forces a reboot of each stacking device, but Intrinsic HA L2FB remains enabled until the stack master confirms that there are enough devices in the stack that are ready to inspect (RTI). For more information, see **Enable or disable Intrinsic HA L2FB on the stack** on page 521.

Distribute a TOS update to the stack using the same steps you would follow for a standalone TippingPoint NX Series IPS. For more information, see **Distribute the TOS** on page 340.

Use the **Sync Health** tab to verify that the same TOS version is installed on each stacking device. For more information, see **Verify stack synchronization** on page 511.

**Note:** If the TOS update does not install properly on a stack member, distribute the TOS update to the stack again. If the stacking device has issues, remove it from the stack to make any updates, and then add the device to the stack. For more information, see **Remove a device from the stack** on page 492.

**Troubleshooting**

Use the following information to identify and resolve stacking issues:

- **Verify AOC cable installation** on page 497
- **View stacking status** on page 498
- **Verify stack health and synchronization** on page 502
- **Resolve issues adding a device to the stack** on page 518
- **View stacking tier statistics** on page 519
- **Enable or disable Intrinsic High Availability Layer-2 Fallback** on page 520
Verify AOC cable installation

The following information describes how to verify the AOC cable installation. Also, you can use this information to verify the installation of a QSFP+ transceiver.

Examples of a stacking port with the AOC cable installed

The following example shows a stacking port with the AOC cable installed correctly.

Figure 19. TippingPoint NX Series IPS – stacking port with the AOC cable installed correctly
The next example shows a stacking port with the AOC cable installed incorrectly.

**Figure 20. TippingPoint NX Series IPS – stacking port with the AOC cable partially inserted upside down**

---

**View stacking status**

In the SMS, use the **Devices** workspace to view and manage the stack and its devices.

See *Devices* on page 282.

**Device details**

In the SMS, the **All Devices** workspace provides a consolidated view of information and configuration settings for the stack and individual stack members. Click **Stack State** to view stacking details and verify stack health.

The following information describes the device detail states for a stack.
Stack is normal

The stack state is normal.

Stack with a device in Intrinsic HA L2FB

The 🔄 icon indicates that a device is in Intrinsic HA L2FB.
Stack with an unmanaged device

The icon indicates that the smsnx1002 device is unmanaged by the SMS and another device could be in Intrinsic HA L2FB. The navigation pane indicates that the smsnx1001 device is the segment reference device (SRD) for the stack.

Stack with an unmanaged device that is also in Intrinsic HA L2FB

The icon and the icon indicate that a device is not managed by the SMS and another can be in Intrinsic HA L2FB.
Stack is in Intrinsic HA L2FB

The ![danger] icon indicates the stack is in Intrinsic HA L2FB.

Front panel stacking LEDs

Use the front panel stacking LEDs to identify the stacking status on the device:

- **Stack**: When lit, indicates that stacking is enabled on the device. Stacking is automatically enabled when you use the SMS to add the device to the stack. If necessary, remove the device from the stack and then add it again to enable stacking. LED color indicates the following states:
  - **Flashing green**: Indicates that the device is ready to inspect (RTI) and is waiting for the stack master to allow the device to begin inspecting network traffic.
  - **Solid amber**: Indicates that the device is not ready to inspect (NRTI).
  - **Solid green**: Indicates that the device is RTI and inspecting network traffic. This is the normal operating mode.

- **Stack Master**: When lit (solid green), indicates that the device is the stack master.

  The stack master is a device role that is responsible for managing stack configuration and states. The stack master is automatically elected by the devices in the stack. All stack members are eligible for election to stack master.

The following example shows the stacking LEDs on the front of each device in the stack:
Device shelf-level graphic

In the SMS, use the device shelf-level graphic to identify the stacking status on the device:

• **STK LED** indicates whether stacking is enabled. In the following example, the **STK LED** is green to indicate stacking is enabled.

• In slot 4, the 40 GbE QSFP+ I/O module is installed.

• The Stack **A** and **B** ports indicate whether the AOC cables are installed. The following example shows the stacking ports are yellow to indicate the AOC cables are not installed.

**Verify stack health and synchronization**

Use the SMS to identify and resolve stack health and synchronization issues. In the All Devices workspace, double-click the stack to view its status information:
• Use the **Summary** tab to verify the health of the stack. The icon on the **Summary** tab indicates the most severe status for the stack. If the stack is in a degraded state, use the Stack Members table to troubleshoot and resolve any issues.

(Best Practice) Perform stack health troubleshooting steps in the following order:

a. **View overall health of the stack** on page 503
b. **Verify stacking bus state** on page 506
c. **Verify stack member state** on page 508
d. **Verify device state** on page 510

• Use the **Sync Health** tab to verify the synchronization status of each device in the stack. The icon on the **Sync Health** tab indicates the most severe synchronization status for the stack. If synchronization is in a degraded state, use the Issues table to troubleshoot and resolve any issues. For more information, see **Verify stack synchronization** on page 511.

View overall health of the stack

The **Summary** tab displays the current stack configuration, overall stack state, and the status of the stacking bus topology. If the status of the stack is not green (normal), identify and resolve any issues.

**To view overall health of the stack**

1. In the SMS tools, click **Devices**.
2. In the **All Devices** workspace, double-click the stack.
3. In the **Summary** tab, use the stack health summary information to identify the current health of the stack and its configuration.
   - **Stack name** — Indicates the name of the stack. Click **Edit** to rename the stack.
   - **Stack state** — Indicates the current state of the stack as reported by the segment reference device.

   **Note:** If the Stacking State is not normal, use the **Stack Port A** and **Stack Port B** columns, along with the **Status** column, to troubleshoot and resolve any issues.

   The following information provides stacking port status information and suggested actions.

**Table 113. Stacking port status**

<table>
<thead>
<tr>
<th>Status</th>
<th>Information</th>
<th>Suggested action</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Ready to Inspect - Normal]</td>
<td>Indicates that the stack is working correctly.</td>
<td>No action is required.</td>
</tr>
<tr>
<td>Status</td>
<td>Information</td>
<td>Suggested action</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>----------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Not Ready to Inspect - Unknown</td>
<td>Indicates that the stack is not inspecting traffic for an unknown reason.</td>
<td>This is a transitory state and no action is required.</td>
</tr>
<tr>
<td>Not Ready to Inspect - Rebooting</td>
<td>Indicates that the stack is not inspecting traffic because one or more of the stack members is rebooting.</td>
<td>This is a transitory state and no action is required.</td>
</tr>
<tr>
<td>Not Ready to Inspect - Layer 2 Fallback</td>
<td>Indicates that the stack is not inspecting traffic because one or more of the devices is stuck in Intrinsic HA L2FB.</td>
<td>At a minimum, reboot the device. If the device returns to this state, a hardware-related issue is likely.</td>
</tr>
<tr>
<td>Not Ready to Inspect - Recoverable Layer 2 Fallback</td>
<td>Indicates that the stack is not inspecting traffic because one or more of the devices is waiting for you to disable Intrinsic HA L2FB.</td>
<td>Disable Intrinsic HA L2FB on the stack. See Enable or disable Intrinsic HA L2FB on the stack on page 521.</td>
</tr>
<tr>
<td>Not Ready to Inspect - Invalid</td>
<td>Indicates that the stack is not inspecting traffic because one or more devices has not completed the boot sequence.</td>
<td>Validate that each device has completed its boot sequence. To validate a particular device, log in to its serial interface and look for Run Level 12 in the boot sequence. If necessary, reboot the device.</td>
</tr>
<tr>
<td></td>
<td>Indicates that the number of devices in the stack does not match the SMS stack configuration.</td>
<td>Validate that the number of devices that are cabled together in the stacking bus correspond to the stack configuration in the SMS.</td>
</tr>
<tr>
<td>Ready to Inspect - Layer 2 Fallback</td>
<td>Indicates that the stack is in Intrinsic HA L2FB but can return to Ready to Inspect - Normal when depending on whether you configured the stack for resiliency, all but one of the stack members, or all of the stack.</td>
<td></td>
</tr>
<tr>
<td>Status</td>
<td>Information</td>
<td>Suggested action</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
<td>------------------</td>
</tr>
<tr>
<td>Connected in a ring</td>
<td>Indicates that the AOC cables are installed correctly.</td>
<td>No action is required.</td>
</tr>
<tr>
<td>Not Connected in a ring</td>
<td>Indicates that the AOC cables are not installed correctly.</td>
<td>Verify the stacking bus health. See Verify stacking bus state on page 506. See also, Install the stacking components on page 484.</td>
</tr>
</tbody>
</table>

- **Stacking bus** — Indicates the current state of the stacking bus topology.
  
The following information provides stacking bus status information and suggested actions.

Table 114. Stacking bus topology state

- **Stack Resilience** — Indicates whether the stack goes into Intrinsic HA L2FB if a single device is not ready to inspect (NRTI). See Enable or disable Intrinsic High Availability Layer-2 Fallback on page 520.

- **Segment Reference Device** — Indicates the network segment device that the SMS uses as a reference to manage the inspection policy across each segment of the stack. Click **Edit** to change the segment reference device.

- **Stack Members (N)** — Indicates the number of TippingPoint IPS devices that belong to the stack configuration in the SMS.

*Note:* For information about the devices that are linked together in the stacking bus, use the **Stack Port A** and **Stack Port B** columns. See Verify stacking bus state on page 506.
Verify stacking bus state

The Summary tab displays stacking bus health by checking the state of the stacking ports and the state of the stack topology on each device. If the status of the stacking bus is not green (normal), identify and resolve any issues.

To verify stacking bus state

1. In the SMS tools, click Devices.
2. In the All Devices workspace, double-click the stack.
3. In the Summary tab, verify stacking is enabled on each device and the status of stacking port connectivity:
   - **Enabled** — Indicates whether stacking is enabled or disabled.
     Stacking is automatically enabled when you add a device to the stack. If necessary, remove the device from the stack and then add it to the stack to enable stacking.
   - **Stack Port A and Stack Port B** — Indicate the stacking port connectivity. See also, Device shelf-level graphic on page 502.

The following information provides stacking port status information and suggested actions.

Table 115. Stacking port status

<table>
<thead>
<tr>
<th>Status</th>
<th>Information</th>
<th>Suggested action</th>
</tr>
</thead>
<tbody>
<tr>
<td>![devicename]</td>
<td>Indicates the device to which the stacking port is resolved.</td>
<td>No action is required.</td>
</tr>
<tr>
<td>![&lt;No Peer&gt;]</td>
<td>Indicates a peer device is not connected to the stacking port.</td>
<td>Validate that the stacking port is connected to a stacking port on a peer device. See Install the stacking components on page 484.</td>
</tr>
<tr>
<td></td>
<td>Indicates the peer device that is connected to the stacking port does not have stacking enabled.</td>
<td>Validate that stacking is enabled on the peer device. See View overall health of the stack on page 503.</td>
</tr>
<tr>
<td>Status</td>
<td>Information</td>
<td>Suggested action</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>&lt;Unknown&gt; (mac-address-hex)</td>
<td>Indicates the peer device that is connected to the stacking port is not managed by the SMS.</td>
<td>Add the peer device to the SMS. See Add the stacking devices to the SMS on page 486.</td>
</tr>
<tr>
<td>No peer information is available</td>
<td>Indicates no stacking information was returned from a peer device.</td>
<td>Verify that the stacking port is connected to the same stacking bus as the segment reference device.</td>
</tr>
</tbody>
</table>

4. Use the Status column to verify the stack topology state.

The following information provides stack topology status information and suggested actions.

**Table 116. Stack topology status**

<table>
<thead>
<tr>
<th>Status</th>
<th>Information</th>
<th>Suggested action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Segment Reference</td>
<td>Indicates that the device has been designated as the segment reference device and is ready for stacking.</td>
<td>No action is required.</td>
</tr>
<tr>
<td>Normal</td>
<td>Indicates that the device is functioning normally.</td>
<td>No action is required.</td>
</tr>
<tr>
<td>Missing peer</td>
<td>Indicates a peer device is not connected to the stacking port.</td>
<td>Validate that the stacking port is connected to a peer device. See Install the stacking components on page 484.</td>
</tr>
</tbody>
</table>
<pre><code>                                                                            | Indicates the peer device that is connected to the stacking port does not have stacking enabled. | Validate that stacking is enabled on the peer device. |
</code></pre>
<table>
<thead>
<tr>
<th>Status</th>
<th>Information</th>
<th>Suggested action</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Peer" /> <strong>Peer</strong> {device-name} is not a stack member</td>
<td>Indicates that a device stacking port references a device that is not actually a part of the stack. This message appears once for each stacking port.</td>
<td>Update the stack configuration to add the device. See Add a device to the stack on page 493.</td>
</tr>
<tr>
<td><img src="image" alt="Not in stack" /></td>
<td>Not in stack</td>
<td>Indicates that the device is not in the stack topology.</td>
</tr>
<tr>
<td><img src="image" alt="No stacking ports" /></td>
<td>No stacking ports</td>
<td>Indicates that the device does not have the required 40 GbE QSFP+ I/O module in slot 4.</td>
</tr>
<tr>
<td><img src="image" alt="Wrong I/O Modules in slot(s)" /></td>
<td>Wrong I/O Modules in slot(s) {slot numbers}</td>
<td>Indicates that there is an I/O module on the device that does not match the I/O module in the segment reference device.</td>
</tr>
<tr>
<td><img src="image" alt="Unknown peer(s) found" /></td>
<td>Unknown peer(s) found</td>
<td>The peer device that is connected to the stacking port is not managed by the SMS.</td>
</tr>
</tbody>
</table>

**Verify stack member state**

The **Summary** tab displays the state of each stack member as reported by the device. If the status of a stack member is not green (normal), identify and resolve any issues.

**To verify stack member state**
1. In the SMS tools, click **Devices**.
2. In the **All Devices** workspace, double-click the stack.
3. In the **Summary** tab, use the **Stack Member State** column to verify the stack member status.

The following information provides stack member status information and suggested actions.

**Table 117. Stack member status**

<table>
<thead>
<tr>
<th>Status</th>
<th>Information</th>
<th>Suggested action</th>
</tr>
</thead>
<tbody>
<tr>
<td>![RTI - Normal]</td>
<td>Indicates that the stack member is working correctly.</td>
<td>No action is required.</td>
</tr>
<tr>
<td>![NRTI - Unknown]</td>
<td>Indicates that the stack member is not inspecting traffic for an unknown reason.</td>
<td>This is a transitory state and no action is required.</td>
</tr>
<tr>
<td>![NRTI - Rebooting]</td>
<td>Indicates that the stack member is not inspecting traffic because it is rebooting.</td>
<td>This is a transitory state and no action is required.</td>
</tr>
<tr>
<td>![NRTI - L2FB]</td>
<td>Indicates that the stack member is not inspecting traffic because it is stuck in Intrinsic HA L2FB.</td>
<td>At a minimum, reboot the device. If the device returns to this state, a hardware-related issue is likely.</td>
</tr>
<tr>
<td>![NRTI - L2FB, Recoverable]</td>
<td>Indicates that the stack member is not inspecting traffic because it is waiting for you to disable Intrinsic HA L2FB.</td>
<td>Disable Intrinsic HA L2FB on the stack. See <em>Intrinsic HA</em> on page 521.</td>
</tr>
<tr>
<td>![RTI - L2FB]</td>
<td>Indicates that the stack member is in Intrinsic HA L2FB but can return to Ready to Inspect - Normal when the stack master determines that the minimum number of devices are ready to inspect.</td>
<td>Depending on whether you configured the stack for resiliency, all but one of the stack members, or all of the stack members must declare they are Ready to Inspect -</td>
</tr>
</tbody>
</table>
Verify device state

The Summary tab displays the state of each device. If the status of a device is not green (normal), identify and resolve any issues.

To verify device state

1. In the SMS tools, click Devices.
2. In the All Devices workspace, double-click the stack.
3. In the Summary tab, use the Device State column to verify the device status.

The following information provides device status information and suggested actions.

Table 118. Device status

<table>
<thead>
<tr>
<th>Status</th>
<th>Information</th>
<th>Suggested action</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Normal]</td>
<td>Indicates that the device is working normally.</td>
<td>No action is required.</td>
</tr>
<tr>
<td>![Updating]</td>
<td>Indicates that the device is updating its status.</td>
<td>This is a transitory state and no action is required.</td>
</tr>
<tr>
<td>![Unmanaged]</td>
<td>Indicates the device is not managed by the SMS.</td>
<td>In the SMS, manage the device:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>a. In SMS tools, click Devices.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>b. Right-click the unmanaged device and click Edit &gt; Manage Device.</td>
</tr>
<tr>
<td>Status</td>
<td>Information</td>
<td>Suggested action</td>
</tr>
<tr>
<td>--------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Not Communicating</td>
<td>Indicates that the device is not communicating across the management network with the SMS.</td>
<td>Verify network connectivity between the SMS and the device. Also, verify the required ports are not blocked.</td>
</tr>
<tr>
<td>Layer 2 Fallback</td>
<td>Indicates that the device is not inspecting traffic because Intrinsic HA L2FB is enabled.</td>
<td>If you enabled Intrinsic HA L2FB on the device, disable Intrinsic HA L2FB. See Intrinsic HA on page 522. If you cannot disable Intrinsic HA L2FB, determine whether stacking has put the device into Intrinsic HA L2FB. See Verify stack member state on page 508.</td>
</tr>
<tr>
<td>Rebooting</td>
<td>Indicates that the device has started a reboot based on a request from the SMS.</td>
<td>This is a transitory state and no action is required.</td>
</tr>
</tbody>
</table>

Verify stack synchronization

The **Sync Health** tab displays stack synchronization status. For example, synchronization status indicates whether the same TippingPoint Operating System (TOS) version is installed on each device. If the status of the synchronization health is not green (normal), identify and resolve any issues.

There are configuration items that should match across each segment of the stack. For example, virtual segments and segment group membership should be the same. Profiles must be the same on corresponding segments. If they do not match, the SMS indicates the mismatch and shows the stack health degraded.

**To verify stack synchronization**

1. In the SMS tools, click **Devices**.
2. In the **All Devices** workspace, double-click the stack.
3. Click the **Sync Health** tab.
4. Use the **Status For** and **Issue** columns to identify synchronization issues.

   The following information provides synchronization status information and suggested actions.
Table 119. Stack synchronization status

<table>
<thead>
<tr>
<th>Stack information</th>
<th>Information</th>
<th>Suggested Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>🚩 TOS</td>
<td>Indicates the TippingPoint Operating System (TOS) version for each of the devices.</td>
<td>Distribute the TOS version to the stack.</td>
</tr>
<tr>
<td></td>
<td>Critical indicator ▢ Mismatch in versions or distribution.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Tip:</strong> To filter synchronization information by this type of issue, use the Type column to filter by TOS Versions.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> For information about where the options are different for managing a stack of devices instead of a single device, see <em>Differences between configuring a stack and a standalone device</em> on page 526.</td>
<td></td>
</tr>
<tr>
<td>🚩 Digital Vaccine</td>
<td>Indicates the Digital Vaccine (DV) version for each of the devices.</td>
<td>Distribute the DV package to the stack.</td>
</tr>
<tr>
<td></td>
<td>Major indicator ▢ Mismatch in versions or distribution.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Tip:</strong> To filter synchronization information by this type of issue, use the Type column to filter by Digital Vaccines.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> For information about where the options are different for managing a stack of devices instead of a single device, see <em>Differences between configuring a stack and a standalone device</em> on page 526.</td>
<td></td>
</tr>
<tr>
<td>🚩 <code>{aux-dv-sub type-name}</code> ThreatDV Versions</td>
<td>Indicates the ThreatDV version of a specific ThreatDV subtype for each of the devices. If a ThreatDV subtype has not been distributed to a device, the cell value is <code>&lt;None&gt;</code>.&lt;br&gt;&lt;br&gt;Major indicator ▢ Mismatch in versions or distribution.&lt;br&gt;&lt;br&gt;If a ThreatDV subtype is not distributed to any devices, it is not displayed.</td>
<td>Distribute the ThreatDV package to the stack.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> For information about where the options are different for managing a stack of devices instead of a single device, see <em>Differences between configuring a stack and a standalone device</em> on page 526.</td>
<td></td>
</tr>
<tr>
<td>Stack information</td>
<td>Information</td>
<td>Suggested Action</td>
</tr>
<tr>
<td>-------------------</td>
<td>-------------</td>
<td>-----------------</td>
</tr>
<tr>
<td><strong>Tip:</strong> To filter synchronization information by this type of issue, use the Type column to filter by ThreatDV Versions.</td>
<td><strong>Tip:</strong> To filter synchronization information by this type of issue, use the Type column to filter by DVToolkit Versions.</td>
<td>Distribute the DVToolkit package to the stack.</td>
</tr>
<tr>
<td>![dvt-name] Indicates the Digital Vaccine Toolkit (DVT) version of a specific DVT for each of the devices. If a DVT has not been distributed to a device, the cell value is &lt;None&gt;. Major indicator: Mismatch in distributions (not versions). If a DVT is not distributed to any devices, it is not displayed. <strong>Tip:</strong> To filter synchronization information by this type of issue, use the Type column to filter by DVToolkit Versions.</td>
<td></td>
<td><strong>Note:</strong> For information about where the options are different for managing a stack of devices instead of a single device, see Differences between configuring a stack and a standalone device on page 526.</td>
</tr>
<tr>
<td>![physical-segment-name-and-direction] Indicates the <code>{profile name}</code> <code>{profile-version}</code> was distributed to a physical segment on each of the devices. Major indicator: Mismatch between profile name, profile version, or distribution. Major indicator: &lt;Unknown&gt; A profile has not been distributed to a segment on one of the devices.</td>
<td></td>
<td><strong>Note:</strong> For information about where the options are different for managing a stack of devices instead of a single device, see Differences between configuring a stack and a standalone device on page 526.</td>
</tr>
<tr>
<td>Stack information</td>
<td>Information</td>
<td>Suggested Action</td>
</tr>
<tr>
<td>-------------------</td>
<td>-------------</td>
<td>------------------</td>
</tr>
<tr>
<td><strong>Tip:</strong> To filter synchronization information by this type of issue, use the Type column to filter by Physical Segment's Profiles.</td>
<td>Indicates the <code>{profile-name}</code> <code>{profile-version}</code> was distributed to a virtual segment on each of the devices.</td>
<td>Distribute the profile to the virtual segment.</td>
</tr>
<tr>
<td>Indicates a virtual segment exists on the SRD but is missing from all the other stack members.</td>
<td><strong>Note:</strong> For information about where the options are different for managing a stack of devices instead of a single device, see Differences between configuring a stack and a standalone device on page 526.</td>
<td><strong>Note:</strong> For information about where the options are different for managing a stack of devices instead of a single device, see Differences between configuring a stack and a standalone device on page 526.</td>
</tr>
<tr>
<td>Critical indicator: There is one missing virtual segment row for each virtual segment on the SRD that is not on any of the other member devices.</td>
<td><strong>Tip:</strong> To filter synchronization information by this type of issue, use the Type column to filter by Virtual Segment's Profiles.</td>
<td><strong>Tip:</strong> To filter synchronization information by this type of issue, use the Type column to filter by Virtual Segment's Profiles.</td>
</tr>
</tbody>
</table>
### Stack information

<table>
<thead>
<tr>
<th>Stack information</th>
<th>Information</th>
<th>Suggested Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Tip:</strong> To filter synchronization information by this type of issue, use the Type column to filter by <strong>Missing Virtual Segment.</strong></td>
<td>Indicates an extra virtual segment exists on one of the stack members but is missing from the SRD. <strong>Critical indicator:</strong> There is one extra virtual segment row for each virtual segment that is not in the segment reference device but is in one of the other devices in the stack. <strong>Tip:</strong> To filter synchronization information by this type of issue, use the Type column to filter by <strong>Extra Virtual Segment.</strong></td>
<td>Delete the extra virtual segment if it is not applicable. Or, edit and save the virtual segment to update the stack. <strong>Note:</strong> For information about where the options are different for managing a stack of devices instead of a single device, see Differences between configuring a stack and a standalone device on page 526.</td>
</tr>
<tr>
<td><strong>Mismatched group for {virtual-segment-name}</strong></td>
<td>Indicates the <strong>Mismatch</strong> to which a virtual segment belongs for each of the devices. <strong>Critical indicator:</strong> Mismatch displayed. There is one row for each virtual segment that has a mismatch in segment groups. <strong>Tip:</strong> To filter synchronization information by this type of issue, use the Type column to filter by <strong>Virtual Segment's Group.</strong></td>
<td>Edit and save the segment group (without making any changes) to update the segment group with all of its segments. <strong>Note:</strong> For information about where the options are different for managing a stack of devices instead of a single device, see Differences between configuring a stack and a standalone device on page 526.</td>
</tr>
<tr>
<td>Stack information</td>
<td>Information</td>
<td>Suggested Action</td>
</tr>
<tr>
<td>-------------------------------------------------------</td>
<td>----------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>⚠️ Mismatched group for <code>{physical-segment-name}</code></td>
<td>Indicates the <code>{segment-group-name}</code> to which a physical segment belongs for each of the devices.</td>
<td>Edit and save the segment group (without making any changes) to update the segment group with all of its segments.</td>
</tr>
<tr>
<td></td>
<td>Critical indicator ⚠️ Mismatch displayed.</td>
<td><strong>Note:</strong> For information about where the options are different for managing a stack of devices instead of a single device, see <em>Differences between configuring a stack and a standalone device</em> on page 526.</td>
</tr>
<tr>
<td></td>
<td>There is one row for each physical segment that has a mismatch in segment groups.</td>
<td></td>
</tr>
<tr>
<td><strong>Tip:</strong> To filter synchronization information by this type of issue, use the Type column to filter by Physical Segment's Group.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Edit and save the segment group (without making any changes) to update the segment group with all of its segments.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> For information about where the options are different for managing a stack of devices instead of a single device, see <em>Differences between configuring a stack and a standalone device</em> on page 526.</td>
<td></td>
</tr>
<tr>
<td>🚭 Extra rule <code>{inspection-bypass-rule-name}</code></td>
<td>Indicates that there is an inspection bypass rule on a stacking device that is not on the SRD.</td>
<td>Edit and save the inspection bypass rule (without making any changes) to update the stack.</td>
</tr>
<tr>
<td></td>
<td>Critical indicator ⚠️ Mismatch displayed.</td>
<td><strong>Note:</strong> For information about where the options are different for managing a stack of devices instead of a single device, see <em>Differences between configuring a stack and a standalone device</em> on page 526.</td>
</tr>
<tr>
<td></td>
<td>There is one row for each inspection bypass rule.</td>
<td></td>
</tr>
<tr>
<td><strong>Tip:</strong> To filter synchronization information by this type of issue, use the Type column to filter by Extra Rule.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Edit and save the inspection bypass rule (without making any changes) to update the stack.</td>
<td></td>
</tr>
<tr>
<td>🚭 Missing <code>{inspection-bypass-rule-name}</code></td>
<td>Indicates that there is an inspection bypass rule on the SRD that is missing from a device in the stack.</td>
<td><strong>Note:</strong> For information about where the options are different for managing a stack of devices instead of a single device, see <em>Differences between configuring a stack and a standalone device</em> on page 526.</td>
</tr>
<tr>
<td></td>
<td>Critical indicator ⚠️ Mismatch displayed.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>There is one row for each inspection bypass rule.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Edit and save the inspection bypass rule (without making any changes) to update the stack.</td>
<td></td>
</tr>
<tr>
<td>Stack information</td>
<td>Information</td>
<td>Suggested Action</td>
</tr>
<tr>
<td>---------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Tip:</strong> To filter synchronization information by this type of issue, use the Type column to filter by <strong>Missing Rule.</strong></td>
<td></td>
<td>single device, see <em>Differences between configuring a stack and a standalone device</em> on page 526.</td>
</tr>
<tr>
<td>Stack Resilience</td>
<td>Indicates that there is at least one device that has a different Stack Resilience option than what is configured for the stack in the SMS.</td>
<td>Edit and save the stack configuration (without making any changes) to update all of the stacking devices.</td>
</tr>
<tr>
<td><strong>{stack-resilience-value}</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Critical indicator <a href="#">Mismatch displayed</a>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Tip:</strong> To filter synchronization information by this type of issue, use the Type column to filter by <strong>Device Resilience Mismatch.</strong></td>
<td></td>
</tr>
<tr>
<td>Extra VLAN</td>
<td>Indicates that there is a VLAN translation rule on a stacking device that is not on the SRD.</td>
<td>Remove the device from the stack, restore the device to its original settings, and then add the device to the stack.</td>
</tr>
<tr>
<td><strong>{translation-description}</strong></td>
<td>There is one row for each VLAN translation rule.</td>
<td>If necessary, edit the VLAN translation mappings for the SRD to include the VLAN translation mapping from the stacking device.</td>
</tr>
<tr>
<td></td>
<td><strong>Tip:</strong> To filter synchronization information by this type of issue, use the Type column to filter by <strong>Extra VLAN.</strong></td>
<td></td>
</tr>
<tr>
<td>Missing VLAN</td>
<td>Indicates that there is a VLAN translation on the SRD that is missing from a device in the stack.</td>
<td>Edit and save the VLAN translation mapping on the SRD (without making any changes) to update all of the stacking devices.</td>
</tr>
<tr>
<td><strong>{translation-description}</strong></td>
<td>There is one row for each VLAN translation rule.</td>
<td></td>
</tr>
</tbody>
</table>
Resolve issues adding a device to the stack

The following information describes how to identify and resolve issues with adding a device to the stack configuration in the SMS.

The following information provides device status and suggested actions for adding a device to the stack.

**Table 120. Device status – adding a device to the stack**

<table>
<thead>
<tr>
<th>Status</th>
<th>Information</th>
<th>Suggested action</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Ready for stacking" /></td>
<td>Indicates that there is no issue with adding the device to the stack.</td>
<td>No action is required.</td>
</tr>
<tr>
<td><img src="image" alt="No QSFP+ module in slot 4" /></td>
<td>Indicates that the device does not have the required I/O module in slot 4.</td>
<td>Verify the 40 GbE QSFP+ I/O module is properly installed in slot 4. If necessary, reboot the device.</td>
</tr>
<tr>
<td><img src="image" alt="This device's model doesn't match the model for the selected devices." /></td>
<td>Indicates that there is a device model mismatch.</td>
<td>Select devices that are either all 7500NX or all 7100NX.</td>
</tr>
<tr>
<td><img src="image" alt="This device's TOS version doesn't match the TOS version for the selected devices." /></td>
<td>Indicates that there is a TOS version mismatch.</td>
<td>The TippingPoint Operating System (TOS) version must be the same on each device in the stack. If necessary, install a matching TOS version on the device and then add it to the stack.</td>
</tr>
<tr>
<td>Status</td>
<td>Information</td>
<td>Suggested action</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
<td>----------------</td>
</tr>
<tr>
<td>This device does not support stack sizes of more than ## devices</td>
<td>Indicates a device is valid for stacking, but that the maximum number of devices in the stack has been reached.</td>
<td>Remove a device from the stack so that you can add the device. See Remove a device from the stack on page 492.</td>
</tr>
<tr>
<td>Device is not communicating</td>
<td>Indicates that the device is not communicating with the SMS.</td>
<td>Verify network connectivity between the SMS and the device. Also, verify the required ports are not being blocked.</td>
</tr>
<tr>
<td>Device is unmanaged</td>
<td>Indicates that the device is no longer managed by the SMS.</td>
<td>In the SMS, manage the device: 1. In SMS tools, click Devices. 2. Right-click the unmanaged device and click Edit &gt; Manage Device.</td>
</tr>
</tbody>
</table>

**View stacking tier statistics**

In the SMS, use the stacking tier statistics to view stacking (Tier S) data for a stacking device in addition to device tiers 1–4. Tier S data includes stacking data from the stacking ports and the 40 GbE QSFP+ I/O module.

The tier statistics area provides information on packets and speed as measured in Mbps by tier.

<table>
<thead>
<tr>
<th>Inspection Tier</th>
<th>Information</th>
</tr>
</thead>
</table>
| Stack : Segment Ports | This inspection tier presents the total I/O module throughput for the network segment device as well as the receive rates from the I/O module to each stack member. When stacking is enabled, the following information is displayed:  
  • Segment Rx Mbps displays the aggregate received traffic from all network segments on this device.  
  • Segment Tx Mbps displays the aggregate traffic transmitted from all network segments on this device. |
### Inspection Tier

<table>
<thead>
<tr>
<th>Information</th>
</tr>
</thead>
</table>
| • **Stack Balance (A/B/C)** displays the load balance percentage, in which 100% equates to perfect balance across the number of devices in the stack. For devices that are in Intrinsic HA L2FB, the Rx rate is zero, and this zero value is included in the load balance calculation. This statistic is similar to the A/B/C Balance percentage in Tier 1.  
  ○ `<host n>` Rx Mbps displays the traffic balanced from this device's network segments to the other devices in the stack. Note that the number of packets going through each host is flow-based, so it is not uncommon to see a slight difference between them.  
  • **Segment ratio to tier 1** displays the percentage of traffic being inspected by this device as a ratio of the segment Rx traffic. |

**Stack : Stack Ports**  
This inspection tier presents stacking port throughput, including through traffic and return traffic rates.  
When stacking is enabled, the following information is displayed:  
• **Stack Rx Mbps** displays the aggregate received traffic from both stacking ports.  
• **Stack Tx Mbps** displays the aggregate traffic that is transmitted from both stacking ports.  
• **Stack Rx > Stack Tx** displays the total amount of transit or through traffic on the stacking ports; for example, traffic received on Stack port 1, which is forwarded by the switch to stack port 2.  
• **Stack Rx > Seg Tx** displays the amount of return traffic coming in on a stacking port that is returning to the outbound network segment.  
• **Stack ratio to tier 1** displays the percentage of traffic being inspected by this device as a ratio of the stack Rx traffic.

---

See *Tier statistics for the vTPS, TPS, and IPS (NX-Platform) devices* on page 409.

### Enable or disable Intrinsic High Availability Layer-2 Fallback

_Intrinsic High Availability (Intrinsic HA)* determines how the device manages traffic on each segment in the event of a system failure. Layer-2 Fallback (L2FB) mode either permits or blocks all traffic on each segment, depending on the Intrinsic HA L2FB action setting for the segment. Any permitted traffic is not inspected.
In the SMS, you can enable Intrinsic HA L2FB on a stack member or the entire stack, for example, to perform scheduled maintenance. When you finish, disable Intrinsic HA L2FB to resume normal operation.

Stacking automatically enables and disables Intrinsic HA L2FB on a stack member or the stack as needed, depending on the inspection state of the stack or the devices.

- **Ready to Inspect (RTI)** indicates that a device or the stack is ready to inspect traffic. If enough devices are RTI, the stack master takes the stack out of Intrinsic HA L2FB. See *Enable or disable stack resiliency* on page 491.

- **Not Ready to Inspect (NRTI)** indicates that a device or the stack is not ready to inspect traffic.

  When a device or stack is NRTI, Intrinsic HA L2FB remains enabled until the NRTI cause is resolved. In some cases, NRTI is a temporary recoverable condition and in other cases, NRTI recovery requires manual intervention. See *Verify stack member state* on page 508.

**Tip:** If a device or the stack is in Intrinsic HA L2FB, disable Intrinsic HA L2FB on the stack to restore the stack to Normal mode. If the stack does not return to Normal mode, verify the stack health to determine why the stack is in Intrinsic HA L2FB and resolve any issues. See *Verify stack health and synchronization* on page 502.

### Enable or disable Intrinsic HA L2FB on the stack

In the SMS, enable Intrinsic HA L2FB mode on the stack to either permit or block all traffic on each segment of the devices in the stack, depending on the Intrinsic HA L2FB action setting for the segment. When you disable Intrinsic HA L2FB on the stack, any devices in Intrinsic HA L2FB are restored to Normal mode.

To resume normal operation, the stack must validate:

- The minimum number of devices are RTI - Normal. See *Verify stack health and synchronization* on page 502.

- The stack members communicate regularly with the stack master.

  If the number of missed heartbeats exceeds a threshold value, or if the device does not send a heartbeat message within 15 minutes of rebooting, the device is NRTI.

- The same TippingPoint Operating System (TOS) version is installed on each device. See *Verify stack synchronization* on page 511.

If you manually enable Intrinsic HA L2FB on the stack, you must also disable it to resume inspection. If necessary, resolve Intrinsic HA L2FB issues on a device to bring the stack out of Intrinsic HA L2FB.

### To enable or disable Intrinsic HA L2FB on the stack

1. In the SMS tools, click **Devices**.

2. In the **All Devices** workspace, right-click the stack and click **Edit > Intrinsic HA**, then choose an option:
- **Fallback** puts the stack in Intrinsic HA L2FB.
- **Normal** takes the stack out of Intrinsic HA L2FB.

Enable or disable Intrinsic HA L2FB on a stacking device

In the SMS, enable Intrinsic HA L2FB mode on a stacking device to either permit or block all traffic on each segment, depending on the Intrinsic HA L2FB action setting for the segment. When you disable Intrinsic HA L2FB on the device, Intrinsic HA L2FB is restored to Normal mode.

Before you enable Intrinsic HA L2FB on a stacking device, verify whether the loss of the device would place the entire stack into Intrinsic HA L2FB. See Enable or disable stack resiliency on page 491.

**To enable or disable Intrinsic HA L2FB on the stacking device**

1. In the SMS tools, click **Devices**.
2. In the **All Devices** workspace, double-click the stack.
3. In the left navigation pane, expand the stack.

   If a stacking device is in Intrinsic HA L2FB, the name of the device is appended by (fallback). In the following example, **MyStack** and its stack members are in Intrinsic HA L2FB.

**Figure 23. Stack in Intrinsic HA L2FB**

1. Click the device that is in Intrinsic HA L2FB.
The stacking device shelf-level graphic is displayed.

5. In the **Device** workspace, right-click the shelf-level graphic and click **Edit > Intrinsic HA**, then choose an option:

   - **Fallback** puts the device in Intrinsic HA L2FB.
   - **Normal** takes the device out of Intrinsic HA L2FB.

**CLI commands for stacking**

On the IPS, use the Command Line Interface (CLI) to display stacking status information from the device. For more information about stacking-related commands, see the *IPS Command Line Interface Reference*.

**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) v3.9.0 (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. Unlike the SMS, the device does not validate the presence of the 40 GbE QSFP+ NX module in slot 4.

```
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
```
Number of devices configured in stack: 3
Number of devices required in stack: 2
Stack state: Stack Ready to Inspect - Normal

<table>
<thead>
<tr>
<th>Device Hostname</th>
<th>Advertised State</th>
</tr>
</thead>
<tbody>
<tr>
<td>device01 (local host)</td>
<td>Device Ready to Inspect - Normal</td>
</tr>
<tr>
<td>device02 (master)</td>
<td>Device Ready to Inspect - Normal</td>
</tr>
<tr>
<td>device03</td>
<td>Device Ready to Inspect - Normal</td>
</tr>
</tbody>
</table>

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 IPS 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>

Limitations

When you consider stacking, keep these points in mind:

- The following options, which require state information to be shared across multiple devices, are not supported in a stacking configuration:
- Transparent HA
- IPS Quarantine. As a workaround, use SMS Responder to propagate IPS Quarantine to stack members.

**Note:** For information about the differences between configuring a stack of devices compared with configuring a standalone device, see *Differences between configuring a stack and a standalone device* on page 526.

- Scan/sweep filters
- Policy-based rate limits

- The SMS is required to manage the stack and any stack members. You cannot manage the stack from the Local Security Manager (LSM) or CLI on the device.
- When stacking is enabled, do not make the following configuration changes to the slot 4 I/O module segments:
  - Enable link-down synchronization
  - Configure VLAN translation rules
  - Configure inspection bypass rules
  - Enable and disable ports
- All stack members must use consistent sets of inspection profiles to ensure inspection policies are applied consistently, regardless of which device inspects the traffic.

### Repurpose a device

If you have existing TippingPoint 7100NX or 7500NX devices that are not currently deployed in your network, you can repurpose the devices for use in a stack. Also, if you remove a device from a stack, you can repurpose it for use in another stack or as a standalone device.

For information about adding a device to the stack, see *Add a device to the stack* on page 493.

#### To repurpose a device

- Use the `debug factory-reset` command to restore the device to its original settings.

Keep the following items in mind when you repurpose a device for use in a stack:

- The same TippingPoint Operating System (TOS) version, v3.9.0 or later, must be installed on each NX Series device in the stack.
- A 40 GbE QSFP+ I/O module must be installed in slot 4. If another type of I/O module is installed in slot 4, replace the module. The process is:
  a. Replace the existing I/O module with the 40 GbE QSFP+ I/O module.
b. Use the `reboot -full` command to reboot the device. See the *IPS Command Line Interface Reference* for more information.

**Differences between configuring a stack and a standalone device**

The following information highlights options that are exclusive for configuring security policy on a stack:

- *Security policy configuration* on page 526
- *Events and reports* on page 529
- *System updates and snapshots* on page 530
- *SMS database restore to a different SMS* on page 531

**Security policy configuration**

Configure the security policy on the stack using the same steps you would follow for configuring the security policy for a standalone TippingPoint IPS or TPS security device.

Use the following table as a guideline when configuring the security policy for your stack:

**Table 121. Security policy on the stack**

<table>
<thead>
<tr>
<th>TippingPoint Operating System (TOS) distribution</th>
<th>TippingPoint Operating System (TOS) distribution to the stack places all of the stacking devices into Intrinsic HA L2FB while the TOS update is installed. (Best Practice) Perform a planned TOS update by enabling Intrinsic HA L2FB on the stack and then distributing the TOS update to the stack. Stacking requires the same TOS version on each of the stacking devices. See <em>Distribute the TOS</em> on page 340.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Digital Vaccine Labs package distribution</td>
<td>When you distribute a DV to the stack, the SMS distributes Digital Vaccine, AUX DV, and DV Toolkit packages to each member of the stack. All devices in a stack must have the same DV packages. <strong>Note:</strong> Each time you add or delete a member in a stack, you must update the DV distribution schedule. This is because DVs are always distributed according to which members were in the stack at the time the distribution was first scheduled. For example, if you schedule a distribution and then remove a device from the stack, the SMS still distributes the package to all the devices that were members of stack when the distribution was first scheduled, including the device you removed.</td>
</tr>
</tbody>
</table>
See *Distributing DV packages overview* on page 196.

| Inspection profile distribution | Distribute your inspection profiles so that they are sent to selected segments on the stack. To do this, specify the virtual segments or segment groups on the segment reference device (SRD) when you distribute the profile. After you do this, the inspection profile goes to the corresponding segments or segment groups on each member of the stack.  
(Best Practice) Distribute an inspection profile to all segments of the stack, including any disabled ports. If a network segment does not have a profile, a Major indicator is displayed in the Sync Health tab. On the IPS only, slot 4 is reserved for the stacking bus. See *Verify stack synchronization* on page 511. See *Distribute profiles* on page 142. |

| Scheduled profile distribution | When working with scheduled profile distributions on the stack, keep the following points in mind:  
  - **Scheduled profile distributions – Stack:** A scheduled profile distribution to the stack runs on the stack members that were in the stack when you created the scheduled profile distribution. If you reconfigure the stack, update the list of target devices in the scheduled profile distribution to include the current stack membership. For example, update the list of target devices when you:  
    - Add a device to the stack  
    - Remove a device from the stack  
    - Delete the stack  
    **Note:** After you delete the stack, the scheduled profile distribution continues to run on the SRD. On the IPS only, subsequent profile distributions are not distributed to slot 4 of the SRD.  
  - **Scheduled profile distributions – Segment Group:** A scheduled profile distribution to a segment group on the stack runs on the stack members that were in the stack when you created the scheduled profile distribution. If you reconfigure the stack, update the list of target devices in the scheduled profile distribution to include the current stack membership. For example, update the list of target devices when you:  
    - Add a device to the stack  
    - Remove a device from the stack  
    - Delete the stack |
After you delete the stack, any scheduled profile distributions continue to run on all physical network segments that were in the stack. Scheduled profile distributions no longer run on a network segment without a physical network I/O module.

See *Scheduled distributions* on page 196.

<table>
<thead>
<tr>
<th>Device configuration</th>
<th>Device configuration on the stack updates all of the stacking devices. You can configure all of the stacking devices as you would a standalone device.</th>
</tr>
</thead>
</table>
| **To edit the device configuration for the stack:** | 1. Click **Devices** on the SMS toolbar.  
2. In the All Devices workspace, right-click the stack and select **Edit Stack Member Configuration**.  
3. In Device Configuration options, configure the stacking devices. See *Device Configuration wizard* on page 324. |

| Segment groups | When creating a segment group for the stack, choose from the physical segments on the SRD. See *Create a segment group* on page 343. |

| Virtual segment details - physical segments | When you create a virtual segment on the stack, the available physical segments consist of network segments. On the IPS only, slot 4 is reserved for the stacking bus. See *Create a virtual segment* on page 340. |

| Active Responder policy - quarantine actions | When you want a stack to quarantine network traffic, use an Active Responder policy in the SMS to propagate the IPS Quarantine action set to the stack. Responder applies the policy thresholds to the stack so that a filter hit on any stack member is applied to the policy threshold, and any stack member that inspects the traffic can also quarantine the traffic when the stack-level policy is triggered. See *Responder* on page 251. |

| Inspection bypass rules | When working with inspection bypass rules, keep the following points in mind:  
• Create inspection bypass rules on the SRD. See *Device details* on page 498.  
• Network I/O slots are available for inspection bypass rules. On the IPS only, slot 4 is reserved for the stacking bus. |
• Inspection Bypass mismatches are displayed in the Sync Health tab. See verify stack health and synchronization on page 502.

To resolve any issues, update the inspection bypass rules on the SRD. The Sync Health tab automatically updates the synchronization status.

• The SMS synchronizes inspection bypass rules across the stack when you finish updating inspection bypass rules on the SRD.

Note: Before you configure an inspection bypass rule, the segment must have a profile distributed to it.

See Create or edit an inspection bypass rule on page 349.

VLAN translation

When working with VLAN translation, keep the following points in mind:

• Network I/O slots are available for VLAN translation. On the IPS only, slot 4 is reserved for the stacking bus.

• Create VLAN translations on the physical segments that connect to the network. If the same network is on more than one segment, create the same VLAN translations on the segments. VLAN translation occurs after inspection but before the traffic exits the stack, so it is important to only configure VLAN translation on the segments that connect to the network.

See Create/edit VLAN translation on page 292.

Events and reports

View events and reports for a stack using the same steps you would follow for a standalone TippingPoint IPS or TPS security device.

The following table provides stacking-related information for events and reports.

Table 122. Events and reports with stacking

| Events | When you create an inspection query with filter criteria for the stack, keep the following points in mind:
|        | • Query the segments from the segment reference device (SRD) to include events from all corresponding segments across the stack. |
• You can filter inspection events by stack. In the **Device/Segment/Rule** section of the criteria, there is a box for selection of Device/Group/Stack. Events are reported on the stack member that inspected the flow.

• A saved event query on the SRD includes events from any devices that are currently members of the stack. If the SRD is replaced, the query includes events for that device only.

See **Inspection events** on page 59.

<table>
<thead>
<tr>
<th>Reports</th>
<th>When you report on the stack, keep the following points in mind:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Query a segment from the SRD to include data from all corresponding segments across the stack.</td>
</tr>
<tr>
<td></td>
<td>• Stack member-level reporting shows the traffic statistics for the specified segment.</td>
</tr>
<tr>
<td></td>
<td>• Saved report queries on the SRD include data from any devices that are currently a member of the stack. If the SRD is replaced, the query includes data for that device only.</td>
</tr>
<tr>
<td></td>
<td>• The Device Traffic report can be run on the stack or a particular segment on the SRD to report on statistical changes in network traffic patterns across the stack. Network I/O slots are available for stack traffic reporting. On the IPS only, slot 4 is reserved for the stacking bus.</td>
</tr>
</tbody>
</table>

See **Reports** on page 96.

**System updates and snapshots**

Do not rollback to an unsupported version of the TippingPoint Operating System (TOS) or to a snapshot that was taken of the device before it was added to the stack.

If you rollback to a snapshot that has a different stack resiliency setting, the **Sync Health** tab in the SMS displays the misconfiguration. To resolve this issue, edit and save the stack configuration with the stack resiliency setting you want. See **Enable or disable stack resiliency** on page 491.

Never rollback to an unsupported version. For example, if you rollback the TippingPoint Operating System on a stacking device from v3.9.0 to v3.8.x, then the unsupported TOS version prevents the device from participating in the stack. This problem can also occur if you restore a snapshot on a stack member, but the snapshot was taken before the device was added to the stack.
See Rollback to a previous version on page 334.

**Note:** If you restore a stacked device snapshot to a standalone device, the device state will be invalid. As a workaround, use the `reboot -full` command to put the device back into a valid state.

### SMS database restore to a different SMS

When you restore the SMS backup to a different SMS that manages a stack with virtual segments, you must manually repair the stack configuration to update its virtual segments.

**To repair the stack configuration:**

1. Click **Devices** on the SMS toolbar.
2. In the All Devices workspace, add each of the devices in the stack.
3. In the left navigation pane, click **Virtual Segments**.
4. In the Virtual Segments list, edit and save each virtual segment (without making any changes) with physical segments from any of the devices in the stack (including any hidden segments). A *hidden segment* is a segment on a stacking device that does not have a network I/O module.

   **Note:** Use the Segments Assigned column to identify the virtual segments with physical segments and hidden segments. For example, a virtual segment with a Segments Assigned value of 8 (16 hidden) indicates there are eight physical segments and 16 hidden segments.

5. Delete any virtual segments that have no physical or hidden segments. For example, delete a virtual segment where the Segments Assigned value is 0 (0 hidden).

See Restore the SMS database on page 590.
Administration

The SMS client provides administration options to enable you to manage user access, system and audit logs, and system settings. Options are also available to back up the SMS database, configure the SMS server, and upgrade SMS software and licenses.

The Admin workspace enables you to manage user access, system and audit logs, and system settings. Options available through the Admin workspace are limited to users with the appropriate role and access level.

To open the Admin workspace, click Admin on the SMS toolbar.

General administration

General administration of the SMS server includes tasks, such as upgrading or patching the SMS software, administering licenses, reviewing system health, and other maintenance tasks.

Working with the Admin (General) screen

The General screen in the Admin workspace displays information about your SMS including system time and server uptime, current software version and installed patches, software and patches available for download, license information, security certificates, and the certificate key.

SMS server

The SMS Server panel displays the system date and time according to the time zone and network time options configured on the SMS. Buttons in this panel allow you to Refresh the connection with the SMS, or Reboot or Shutdown the SMS server.

⚠️ Caution: Before rebooting or shutting down an SMS Server consult your company’s policies for handling service interruptions of key servers. At a minimum, you might need to communicate that all connections to the SMS server will be disrupted.

⚠️ Important: When you shut down or reboot an HA-configured cluster, both nodes of the cluster are shut down or rebooted.

SMS software

The SMS Software panel displays the current SMS software version installed on the server, any SMS software that is available for you to download, and SMS software that has been downloaded and is ready to be installed. From this panel, you can download, import, and install SMS software.

When it is connected to the TMC, the server monitors for newer versions of the SMS software. When a version newer than the current version is detected, the Available for Download field displays the software version number, and the Download button on the SMS Software panel becomes available.
Before you download and install a new version of the SMS software, read the SMS Release Notes thoroughly and take note of the following caveats:

- The SMS server can obtain the software automatically from the TMC or can import a patch file from storage media such as a CD-ROM or hard drive.
- You cannot roll back an upgrade.
- An SMS software upgrade can take up to thirty minutes. Connect to the SMS server by display console to monitor the process.
- Installing a new version of SMS causes the SMS server to reboot and close all client connections. If you perform an upgrade from an SMS client, the client eventually loses connection because the SMS server to which it is connected must reboot.
- When the SMS server is unavailable during the reboot process, the availability and operations of TippingPoint devices managed by the SMS are not affected. IPS and other devices continue to operate as usual and without interruption.
- The version of SMS client software should match the version of the SMS server. When you upgrade the SMS server, you might be unable to connect to the server through an SMS client until you have upgraded the SMS client software. You can still connect to the SMS server through the command-line interface and through a Web browser.
- If your SMS server is configured for High Availability (HA), you must disable HA prior to performing an upgrade of the SMS servers. To upgrade a HA cluster, break down the cluster, upgrade each SMS individually, and then re-establish the cluster.

Download and install SMS software

1. Click **Download** (when the button is available) to download the software update.
   
   When the download is complete, the value in the Available for Download field matches the value in the Available for Install field.
2. Click **Install** to install the downloaded package.
3. Click **Yes** to confirm the installation.
4. Update each SMS client that connects to the SMS server.
   
   You can also obtain SMS software through media such as a CD, or you can download the software to a system through a direct login to the TMC. In this case, you must first import the software package, and then install it.

   **Note:** Do not modify the name of the file prior to importing it.

Import and install SMS software from a CD or the TMC

1. Click **Import**.
2. Select the SMS software package, and click **Open**.
3. Click **Install** to install the imported package.
4. Click **Yes** to confirm the installation.
5. Update each SMS client that connects to the SMS server.

**SMS patches**

The SMS Patches panel displays information about software patches that are currently installed and software patches that are available for download from the TMC. The SMS Patch Notifications field indicates whether SMS patch notifications are enabled or disabled.

SMS patches provide updates to the SMS server, the SMS client, or both. Patches are cumulative; the latest patch includes all previously released patches for a particular version of the product. For more details, refer to the Release Notes available during the patch upgrade process or on the Software Details page for the patch on the TMC.

The SMS server, when connected to the TMC, monitors the TMC for SMS software patches. In the SMS client, you can enable or disable SMS patch notifications that indicate when a more recent patch is available. If patch notifications are enabled, a green check and the value “Enabled” are displayed in the SMS Patch Notifications field. If patch notifications are disabled, the value “Disabled” is displayed. Click the button to the right of the field to enable or disable patch notifications.

Before you download and install an SMS patch, read the SMS Release Notes thoroughly and take note of the following caveats:

- The SMS server can obtain the software automatically from the TMC or can import a patch file from storage media such as a CD-ROM or hard drive.

- You can typically roll back a patch; refer to the patch Release Notes for rollback information. If you choose to roll back a patch, it rolls back the cumulative patch, effectively removing all patches from the SMS server. A patch rollback typically requires a restart of the SMS server application.

- Installing an SMS patch typically causes the SMS server application to restart, and in some cases requires the SMS server to reboot. All client connections to the SMS are stopped during the patch process.

- When the SMS server is unavailable during the reboot process, the availability and operations of TippingPoint devices managed by the SMS are not affected. IPS and other devices continue to operate as usual and without interruption.

- The version of SMS client software should match the version of the SMS server. Some patches require an update to the SMS client as well as the SMS server. In this case, all clients are prompted to upgrade to the newer version when they try to connect to the patched SMS server.

- If your SMS server is configured for High Availability (HA), see *How do I apply SMS software updates to a cluster?* on page 638.
Install an SMS patch

1. Click **Update** to open the SMS Patch wizard.
2. Do one of the following:
   - Import an SMS patch file from storage media or your local drive:
     a. Select **Import from File**, and then click **Next**.
     b. Choose the SMS patch file to import.
     c. Click **Import**.
     d. Click **Finish**.
   
   **Note:** Do not modify the name of the file prior to importing it.

   Download an SMS patch file from the TMC website:
     a. Select **Download from TMC**, and then click **Next**.
     b. If there are any available SMS patches, select the appropriate patch from the list. The Release Notes section displays information about the selected patch.
     c. Click **Download** to download the selected patch.
3. Click **Install** to install the downloaded package.
4. Click **Finish**.

   If necessary, update each SMS client that connects to the SMS server.

Roll back an SMS patch

1. On the SMS Patches panel, click **Rollback**.
2. Click **Rollback** again on the Confirm Rollback screen to confirm the operation.
3. Click **Finish**.

   The SMS server rolls back the patch, which requires a restart of the SMS server software. When the rollback process is complete, the SMS server is running the base SMS software (without any patches).

**SMS web security SSL certificate**

The SMS uses a web security SSL certificate to establish secure communication between a web browser and the SMS server. When the SMS is configured for high availability (HA), the certificate is synchronized across nodes in the SMS HA cluster.
You can import a certificate now, or if you have already imported a certificate into the SMS certificate repository, simply choose the one you want. For more information about certificate management, see Viewing certificates on page 568.

**Note:** The web security SSL certificate is included in an SMS backup. The certificate is reset during a factory reset operation.

The SMS web security SSL certificate panel displays the following information for the current certificate:

- **Current Certificate** – The SMS name of the certificate.
- **Pending Certificate** – If you edit the name of the certificate, the SMS will display the new name until you reboot the SMS. After you reboot the SMS, the certificate name will appear as the current certificate.

The SMS provides a <Default Certificate>. If you experience problems with the certificate, you can reset the certificate to the default.

**Reset the SMS web security SSL certificate**

1. On the SMS Web Security SSL Certificate panel, click **Reset**.
2. In the Conform Reset dialog, click **Yes**.
3. Restart the SMS server for the new certificate to take effect.

**Note:** Resetting the certificate generates and installs a default SMS Web Security SSL Certificate, which replaces the current certificate.

In some cases, you might want to replace the default certificate with a root Certificate Authority (CA) signed certificate to establish a trusted relationship between Web clients and the SMS Web server. The SMS client enables you to import an X.509 certificate and corresponding PKCS#8 DER-encoded private key for use as a Web server certificate.

**Import a custom Web security SSL certificate**

You can specify a custom Web security SSL certificate.

1. On the SMS Web Security SSL Certificate panel, click **Import**.
2. In the dialog, provide the locations of the X.509 and the corresponding PKCS#8 private key.

**Important:** The PKCS#8 file must not be password protected.

3. Click **Import**.
4. Restart the SMS server for the new certificate to take effect.

**Note:** When import a custom Web security SSL certificate, and then run the SMS in FIPS mode, when you attempt to log on to the SMS client, a dialog box will appear prompting you to trust the new certificate.
SMS certificate key

The SMS Certificate Key panel displays information about the currently installed certificate key including the certificate number, key size, and description. The SMS certificate key is an RSA certificate that contains the serial number used to identify this SMS. It is also used as the SSL certificate for communication between the SMS client and the SMS server.

By default, the SMS comes from manufacturing with a 1K key (1024 bits). We recommend that you upgrade this certificate with the 2K (2048 bits) version, which also uses stronger hashing functions. The upgraded 2K key certificate will have the same serial number as the one it replaces. If SMS is currently running a 1K key, it will display a message about upgrading to a 2K key.

Note: Only users with SuperUser capabilities are able to upgrade the SMS certificate key.

Before you upgrade the SMS certificate key, note the following caveats:

• The SMS can obtain the certificate key package automatically from the TMC, or you can import the key from a file.

• Some devices (NGFW appliances running TOS v1.2.3, TPS devices running TOS v4.0, and CoreController) are incompatible with the larger certificate key size. Before you upgrade to the 2K, review the list of unsupported devices available on the TMC. After you upgrade the SMS certificate key, you will not be able to manage any of the unsupported device types.

• Installing the 2K key requires a restart of the SMS. The 2K key will not be in use until you restart the SMS. When you install the 2K key without restarting the SMS, a message will display on the SMS Certificate Key panel.

• After you install the 2K key, you will lose device management functionality on the SMS, if you roll back to the following versions:
  ◦ TPS devices running TOS v4.0
  ◦ NGFW appliances running TOS v1.2.1 or earlier

For more information, see Rollback to a previous version on page 334.

FIPS mode and certificate key size

If the SMS is currently running a 1K key, it will display a message about upgrading to a 2K key to be fully FIPS compliant. You can still enable FIPS mode on the SMS without installing the 2K key, but when the SMS is in FIPS mode, you cannot install the 2K key. For more information, see FIPS mode on page 591.

High Availability (HA)

When the SMS is configured for HA, keep in mind:

• You cannot install the 2K key in either SMS while the SMS is running in HA. You must first disable the HA cluster, install the 2K key on each SMS, and then reconfigure the SMS HA cluster.
Both SMS systems in the HA cluster must be running the same key size. For example, the primary SMS cannot be running a 1K key and the secondary SMS be running a 2K key.

For more information, see "High Availability" on page 635.

**Update the SMS certificate key**

By default, the SMS will be running with the 1K key installed. Follow these steps to upgrade to the 2K key.

1. Click **Upgrade** to open the SMS Certificate Key Upgrade wizard, review the list of incompatible devices, and then click **Next**.

2. Do one of the following:
   - Download the SMS certificate key from the TMC:
     a. Select **Download from TMC**, and then click **Next**. The SMS displays the status of the certificate key package download. The SMS displays an error message if a connection cannot be made to the TMC, the file is not found, or the file is invalid.
     b. Click **Download** to download the selected patch.
   - Import the SMS certificate key file from storage media or your local drive:
     a. Select **Import from File**, and then click **Next**.
     b. Click **Browse**, and then select the SMS certificate key package.
     c. Click **Import**.

3. (Optional) Select the **Restart the SMS when finished** check box to immediately restart the SMS.

   The 2K key will not be in use until you restart the SMS. If you install the 2K key without restarting the SMS, a message will display on the SMS Certificate Key panel.

4. Click **Finish**.

**Viewing system health**

The System Health screen in the Admin workspace enables you to monitor and review the health of the SMS server, including hardware and software. To open the screen, expand the General node in the navigation pane and select **System Health**.

The System Health screen displays a summary of the current state of the monitored statistics in a table, and shows longer-term historical statistics in a series of graphs. When the SMS is configured in a HA cluster, the System Health screen displays information for both the active and the passive server using a separate tabbed view for each server.
The SMS monitors memory usage, CPU utilization, swap usage, and various file system categories (archive, database, package, system, report, and operating system). The top portion of the screen displays current health statistics in a table view. The Refresh button directly below the table refreshes the current statistics.

**Note:** The System Health screen displays temperature for a physical SMS appliance, but not for a virtual deployment (vSMS).

You can adjust is to customize how the SMS client presents this information. See *SMS features* on page 27.

The bottom portion of the screen displays Memory, CPU, and File System graphs that represent historical statistics over time. To view realtime data from any of the historical graphs, click the **Realtime** icon. See *SMS features* on page 27.

**Viewing port health**

The Port Health screen in the Admin workspace enables you to view statistics related to the SMS server ethernet ports. To open the screen, expand the General node in the navigation pane and select **Port Health**.

The Port Health screen displays a summary of port usage statistics in a table, and shows longer-term historical statistics in a series of graphs. When the SMS is configured in a HA cluster, the Port Health screen displays information for both the active and the passive server using a separate tabbed view for each server.

The top portion of the Port Statistics screen displays current port statistics in a table view. For each interface, the table displays the number of bytes incoming and outgoing, the number of packets discarded, and the number of errors, as described in the following table.

<table>
<thead>
<tr>
<th>Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Network interface, typically shown as primary port or secondary port.</td>
</tr>
<tr>
<td>Total In: Bytes</td>
<td>Total number of bytes that have passed into the port.</td>
</tr>
<tr>
<td>Total Out: Bytes</td>
<td>Total number of bytes that have passed out of the port.</td>
</tr>
<tr>
<td>Total In: Discards</td>
<td>Number of inbound packets discarded, although no errors were detected.</td>
</tr>
<tr>
<td>Total Out: Discards</td>
<td>Number of outbound packets discarded, although no errors were detected.</td>
</tr>
<tr>
<td>Total In: Errors</td>
<td>Sum of all errors that prevented the final transmission of inbound packets.</td>
</tr>
<tr>
<td><strong>Information</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>----------------</td>
<td>----------------</td>
</tr>
<tr>
<td>Total Out: Errors</td>
<td>Sum of all errors that prevented the final transmission of outbound packets.</td>
</tr>
</tbody>
</table>

The Refresh button directly below the table refreshes the current statistics.

You can adjust table properties to customize how the SMS client presents this information. See *SMS features* on page 27.

The bottom portion of the screen displays a graph for each ethernet port. Data in the graph shows historical statistics over time. To view realtime data from any of the historical graphs, click the **Realtime** icon. See *SMS features* on page 27.

**Viewing the SMS system log**

The SMS System Log contains information about software processes that control TippingPoint devices, including startup and maintenance routines. By default the log contains information about events that have occurred during the current day. To open the screen, expand the General node in the navigation pane and select **SMS System Log**.

For each event, the system log displays the date and time it took place, the severity level of the event (Info, Warn, or Error), and a message-level description of the event.

Viewing logged events can help you troubleshoot SMS and device issues. You can export one, or all, of the events and send them to a customer support organization for a detailed analysis of the information.

**Note:** The system log is accessible only to users with superuser privileges. See *Syslog format options* on page 600.

You can adjust table properties to customize how the SMS client displays system log information. See *SMS features* on page 27.

**View the SMS system log**

1. In the navigation pane for the Admin workspace, expand **General**, and then select **SMS System Log**.
2. On the Date Range panel, do one of the following:
   a. Click the first option, and select a duration from the drop-down menu.
   b. Click the second option, and specify Start Time and End Time.
3. Click **Refresh**.

**Export SMS system log entries**

1. Select the appropriate options on the Date Range Panel to view the SMS system log.
2. Click **Refresh**.
3. Do one of the following:
   a. To export the full set of results, click **Export All**.
   b. To export specific events, select the events in the list, and then click **Export Selected**.
4. In the dialog, specify a name and location for the file and click **Save**.
   
   To change the file format, select another option in the file type drop-down menu before you click Save.
   
   Note that you can use the **Find** utility to locate a specific event. Also, you can select **Details** from the right-click menu to view System Log Record Details for an event.

**Viewing the SMS audit log**

The SMS Audit Log contains detailed information about user activity. By default the log contains information about events that have occurred during the current day. To open the screen, expand the General node in the navigation pane and select **SMS Audit Log**.

The following table describes the information shown on the SMS Audit Log screen.

<table>
<thead>
<tr>
<th>Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number</td>
<td>System-assigned identification number for reference purposes.</td>
</tr>
<tr>
<td>Time</td>
<td>Date and time the operation occurred.</td>
</tr>
<tr>
<td>User</td>
<td>User name for the account that performed the action. The field might include a user entry for SMS, LSM, and CLI. These entries are entered by those applications into the audit log as a Super User level of access.</td>
</tr>
<tr>
<td>Host</td>
<td>Name of the host from which the user operation occurred.</td>
</tr>
<tr>
<td>Session ID</td>
<td>Identification number assigned by the server for the login session. You might also see the following session ID numbers:</td>
</tr>
<tr>
<td></td>
<td>-1 indicates the user is not yet authenticated.</td>
</tr>
<tr>
<td></td>
<td>0 or -2 might indicate system actions instead of user actions.</td>
</tr>
<tr>
<td>Operation</td>
<td>Description of the action performed by the user.</td>
</tr>
<tr>
<td>Status</td>
<td>Result of the operation; valid status is either success or failure.</td>
</tr>
</tbody>
</table>
Audit log events can help you investigate user-initiated activities. You can export one, or all, of the events and send them to a customer support organization for a detailed analysis of the information.

**Note:** The system log is accessible only to users with superuser privileges. See *Syslog format options* on page 600.

You can adjust table properties to customize how the SMS client displays system log information. See *SMS features* on page 27.

The view and export options for the SMS Audit Log are identical to the options for the SMS System Log. See *View the SMS system log* on page 540 and *Export SMS system log entries* on page 540.

## Authentication and authorization

Authentication and Authorization includes tasks such as configuring authentication, managing user roles, configuring user groups, and setting up user accounts.

**Note:** Users must meet authorization requirements to perform tasks described in this section. The user account must be a member of a group with SuperUser role capabilities or the SMS Authentication and Authorization Admin capabilities.

## Managing active sessions

The Admin (Authentication and Authorization) screen displays information about active sessions on the SMS. This screen allows you to view and manage client sessions active on the SMS. In addition to viewing information about active client sessions, you have the ability to terminate user sessions if necessary.

The following table describes the fields in the Active Sessions table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session ID</td>
<td>System-assigned identification number for the login session.</td>
</tr>
<tr>
<td>User Name</td>
<td>User name of the account with which the session connection is established.</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP address of the system that initiated the session and with which the SMS has an active connection.</td>
</tr>
<tr>
<td>Groups</td>
<td>Groups to which the user account is a member. Also specifies the New Resource Group (target creation group for the account).</td>
</tr>
</tbody>
</table>
### Field | Description
---|---
Login Time | Date and time, based on the time zone of the SMS Server, that the session initiated its connection with the SMS Server.

A New Resource Group is the target group into which objects created by a user are contained and verified for authorized access. When a remote user logs on to the SMS, the user may be prompted to set a New Resource Group if one is not already assigned in SMS or mapped to an Active Directory group.

If the New Resource Group is not set through automatic mapping to an Active Directory group, then you can set or change the New Resource Group for a user logged on to the SMS.

### Set or change a new resource group for a user account
1. In the navigation pane for the Admin workspace, click **Authentication and Authorization**.
2. Select the session row in the Active Sessions table, and then click **Set New Resource Group**.
3. In the dialog, select a New Resource Group from the list, and then click **OK**.

*Note:* When you are using Active Directory for authentication and authorization — If you want to use telephone notes to determine new resource group mapping and the SMS is set to reject login on group mapping failure, you must be a member of any groups listed in your telephone notes. If you include a group in your telephone notes that you are not a member of in AD, then you will not be allowed to login to the SMS. See **Edit Active Directory global group mapping** on page 549.

### Terminate an active session
1. On the Admin (Authentication and Authorization) screen, select the session in the Active Sessions table.
2. Click **Terminate**.

   When a session is terminated, the SMS Server does not request confirmation, nor does it send notification to the SMS client when the connection is ended. From the perspective of the end user, the SMS client closes without warning.

*Note:* To terminate an active session, your account must have SuperUser privileges or user management capabilities. In addition, you cannot terminate your own active session.

### Configuring authentication

The Authentication screen enables you to configure the mechanism with which the SMS server authenticates user login requests.

The SMS supports five types of user authentication: local, RADIUS, Active Directory, TACACS+, and CAC. You must choose one authentication method per SMS server:

- **Local** – Authentication is performed locally on the SMS.
• **RADIUS** – Authentication is performed on the RADIUS server; user role and access rights are maintained on the SMS server. If the RADIUS server is unavailable, the SMS can authenticate local users. You cannot manage the SMS user account on the RADIUS server, and you can modify the user password only from the RADIUS server.

• **Active Directory** – Authentication is performed on the Active Directory (AD) server; for SMS accounts, user role and access rights are maintained on the SMS server. If the AD server is unavailable, the SMS can authenticate local users if the Authentication Mode for the active group mapping is set to “Allow only users defined in the SMS to login.” If another mode has been configured, only users whose access privileges are maintained locally on the SMS are able to login. You cannot manage the SMS user account on the AD server; you can modify the user password only from the AD server.

• **TACACS+** – Authentication is performed on the TACACS+ server; user role and access rights are maintained on the SMS server. If the TACACS+ server is unavailable, the SMS can authenticate local users. You cannot manage the SMS user account on the TACACS+ server, and you can modify the user password only from the TACACS+ server.

• **CAC** – Authentication is performed on the SMS server using Certificate Authority (CA) certificates and an ActivClient smartcard reader. User role and access rights are maintained on the SMS server. If the SMS is in CAC Authentication mode, all SMS users must log in using CAC and a PIN number.

Only one authentication method per SMS server is permitted at any one time, but the SMS does allow an administrator to designate user accounts that must always be authenticated locally regardless of the designated authentication source. In this way, you can configure the SMS to use either RADIUS, Active Directory, TACACS+, or CAC as an authentication source, but to specify user accounts that must be authenticated on the SMS.

**Tip:** We recommend that you have at least one SuperUser account that authenticates locally to ensure access for system troubleshooting.

### Authentication source

The Authentication Source panel displays the authentication method that is currently enabled. By default, the authentication method is set to Local Authentication.

Before you can change the authentication source to use remote authentication, you must configure those options. See *Authentication and authorization* on page 542.

When you enable an authentication source, you can specify users that must always be authenticated locally regardless of the designated authentication source. The SMS does not support the use of RADIUS, Active Directory, TACACS+, and CAC authentication on the same SMS server.

**Edit the SMS server authentication source**

1. In the Admin workspace, expand Authentication and Authorization and select **Authentication**.
2. Click **Edit** on the Authentication Source panel.
3. In the dialog, select an option as the group mapping method:
• Use Local Authentication
• Use RADIUS Authentication
• Use Active Directory Authentication
• Use TACACS+ Authentication
• Use CAC Authentication

**Note:** You cannot select Active Directory, RADIUS, or TACACS+ authentication options until these options are configured. See *Configuring authentication* on page 543. For more information on configuring CAC Authentication, see *Configure CAC authentication* on page 552.

4. In the lower portion of the dialog, select user accounts that are only authenticated locally, even if a remote authentication server is selected as authentication source.

5. Click **OK**.

**Authentication configuration**

The Authentication Configuration panel contains separate tabs for RADIUS, Active Directory (AD), TACACS+, and CAC configuration. Select the appropriate tab to configure one of these authentication options.

To secure information passed during authentication, you can enable SSL-based encrypted communication between the SMS and an AD authentication server, and you can import an x509 certificate from a RADIUS server to the SMS. The SMS server accepts DER (binary) or PEM (Base64) encoded x509 certificates. TACACS+ servers do not use SSL-based encryption or certificate-based authentication.

To edit authentication configuration, your user account must be a member of a group with superuser role capabilities or the **SMS Authentication and Authorization Admin** capabilities.

**Configure RADIUS authentication**

Remote Authentication Dial In User Service (RADIUS) is an industry-standard method used to authenticate user login requests.

Although user authentication is performed on the RADIUS server, user authorizations and access rights are maintained on the SMS server. If the RADIUS server is unavailable, the SMS can authenticate local users. The SMS does not permit you to manage SMS user accounts on the RADIUS server; the account password for a RADIUS authenticated user must be changed on the RADIUS server.

**Note:** When the SMS is configured to operate in HA mode and the authentication source is RADIUS, the SMS HA cluster must use the shared virtual management IP address. In addition, the shared virtual management IP address must be designated as a RADIUS client in the RADIUS configuration file.

**Edit the RADIUS server configuration**

1. On the Authentication screen, select the RADIUS tab on the Authentication Configuration panel.
2. Click **Edit** to the right of the Primary RADIUS Server panel.

3. In the dialog, configure the RADIUS server options described in the following table.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>IP address of the RADIUS server.</td>
</tr>
<tr>
<td>Port</td>
<td>Port on the RADIUS server that listens for authentication requests; the default value is 1812.</td>
</tr>
<tr>
<td>Authentication Protocol</td>
<td>Authentication method used on the RADIUS server:</td>
</tr>
<tr>
<td></td>
<td>• PAP</td>
</tr>
<tr>
<td></td>
<td>• MD5</td>
</tr>
<tr>
<td></td>
<td>• PEAP/EAP-MSCHAPv2</td>
</tr>
<tr>
<td></td>
<td>To use the PEAP/EAP-MSCHAPv2 protocol, you must first import an X509 certificate for the RADIUS server. You can click <strong>Import</strong> to import a certificate or choose a previously imported one from the SMS certificate repository. For more information about certificate management, see <strong>Viewing certificates</strong> on page 568.</td>
</tr>
<tr>
<td>Important:</td>
<td>A certificate import or reset is a separate operation from configuring the authentication source and takes effect immediately. The SMS administration should carefully coordinate certificate and the RADIUS configuration changes.</td>
</tr>
<tr>
<td>Secret/Confirm Secret</td>
<td>String used to encrypt and sign packets between RADIUS clients and the RADIUS server, set in the RADIUS client configuration file.</td>
</tr>
<tr>
<td>Timeout</td>
<td>Timeout, in seconds, for communication with the RADIUS server; the default value is 3 seconds.</td>
</tr>
</tbody>
</table>

4. Test the RADIUS configuration by entering a valid User Name and Password for the server (and confirming), and then clicking **Test**.

5. Click **OK** to save the server configuration.

An X509 certificate is required for validating PEAP/EAP-MSCHAPv2 authentication responses. The certificate is generated on the RADIUS server, and must be imported to the SMS. The SMS server accepts DER (binary) or PEM (Base64) encoded X509 certificates.
You can also change the configuration of RADIUS servers by selecting **Devices > device-name > Authentication > RADIUS Groups > Edit > RADIUS Servers > Edit.**

**Configure Active Directory authentication**

Active Directory is a Microsoft-produced, Windows-centric method used to authenticate user login requests. Although user authentication is performed on the Active Directory server, user authorizations and access rights are maintained on the SMS server. If the Active Directory (AD) server is unavailable, SMS can authenticate the user locally. The account password for an AD-authenticated user must be changed on the SMS. The SMS does not permit you to manage user accounts on the Active Directory server. User credentials for remote AD accounts must be managed on the Active Directory server. The SMS is not permitted to change passwords for user accounts on the Active Directory server.

The SMS server supports using Active Directory to authenticate logon requests as well as mapping users to AD groups for authorization requests. You specify Active Directory Global Group Mapping when you configure the Active Directory server for authentication on the SMS.

Before you configure an Active Directory server for user authentication, the SMS must be able to resolve the IP address of the server. The Domain Name System (DNS) must be configured and enabled on the Active Directory server, and all domain clients must use the AD server as their primary DNS server.

**Note:** When using an Active Directory server for user authentication on the SMS, the **User ID** is case-sensitive. You must type the **User ID** on Active Directory exactly as it was entered on the SMS.

**Note:** If you experience a problem with the DNS configuration on Active Directory, contact customer support (TAC) for assistance.

**Note:** When the SMS is configured to operate in HA mode and the authentication source is Active Directory, the SMS HA cluster must use the shared virtual management IP address. In addition, the shared virtual management IP address must be configured on the Active Directory server as a location from which to accept authentication requests.

**Allowing remote users with Active Directory authentication**

When the SMS is configured to allow Active Directory (AD) users to log in without an SMS account and the Mapping Failure Action is set to Reject Authentication, users must be mapped to a local SMS resource group through an AD group membership or the AD account Telephone Notes field. If there is not a member of an AD group that is mapped to a local SMS Resource group, the user will receive an error when they attempt to log in.

When using this authentication model, users are not added directly to an SMS resource group. Membership for the local resource group is controlled by the mapped AD group. Another option is to include the mapped AD group name in the Telephone Notes section of a user’s AD account. Choose which method to use when you configure your AD authentication.

**Note:** If you want to use telephone notes to determine new resource group mapping and the SMS is set to reject login on group mapping failure, you must be a member of any groups listed in your telephone
notes. If you include a group in your telephone notes that you are not a member of in AD, then you will not be allowed to login to the SMS.

**Edit the Active Directory server configuration**

1. On the Authentication screen, select the Active Directory tab on the Authentication Configuration panel.
2. Click **Edit** to the right of the Active Directory Server Configuration panel.
3. In the dialog, configure the Active Directory server options described in the following table.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Address</td>
<td>IP address or host name of the Active Directory server.</td>
</tr>
<tr>
<td>Enable SSL</td>
<td>Select <strong>Using LDAPS</strong> to enable Lightweight Directory Access Protocol (LDAP) over SSL. If enabled, you must also import an Active Directory SSL certificate. See <em>Configure Active Directory authentication</em> on page 547.</td>
</tr>
<tr>
<td>Port</td>
<td>The port on the Active Directory server that listens for authentication requests. The default non-SSL port is 389; if SSL is enabled, the default port is 636.</td>
</tr>
<tr>
<td>Timeout</td>
<td>Timeout, in seconds, for communication with the Active Directory server; the default value is 30 seconds.</td>
</tr>
<tr>
<td>Search Base</td>
<td>Top-level distinguished name in the Active Directory hierarchical structure where the authentication request begins.</td>
</tr>
<tr>
<td></td>
<td>Example: <em>DC=adomain, DC=example, DC=com</em></td>
</tr>
<tr>
<td>Admin Name/DN</td>
<td>Identifies the account on the Active Directory server that is permitted to search the LDAP directory within the defined search base. This is the bind user on the Active Directory server that enables the SMS to query the LDAP directory and authenticate users.</td>
</tr>
<tr>
<td></td>
<td>Example: <em>Administrator@DOMAINNAME</em></td>
</tr>
<tr>
<td>Admin Password</td>
<td>Active Directory server administrative password.</td>
</tr>
</tbody>
</table>

4. Test the Active Directory configuration, enter the Admin Password for the server, and then click **Test**.
5. Click **OK** to save the server configuration.
All SMS users must be identified with a New Resource Group. See Managing active sessions on page 542. An AD-authenticated user that does not belong to an SMS group must be mapped to an Active Directory group or specify a New Resource Group at first logon. You can manage the SMS-assigned New Resource Group for AD users from the Active Sessions screen.

**Edit Active Directory global group mapping**

1. On the Authentication screen, select the Active Directory tab on the Authentication Configuration panel.
2. Click **Edit** to the right of the Active Directory Global Group Mapping panel.
3. In the dialog, select a group mapping method and options for the SMS to use.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication Mode</td>
<td>Select one: <strong>Allow only users defined in the SMS to log in</strong> or <strong>Allow AD users to log in with or without an SMS account</strong>. If you choose to allow access for non-local users, you must also specify how the New Resource Group will be determined for those users. By default, users are allowed to choose a New Resource Group.</td>
</tr>
<tr>
<td>Authorization Mode</td>
<td>If you configured Authentication Mode to allow only users defined in the SMS to log in, then you can select either of two options: <strong>Use SMS local group mappings</strong> or <strong>Use active directory group mappings</strong>. Otherwise, Authorization Mode uses active directory group mappings.</td>
</tr>
</tbody>
</table>
| New resource group mapping mechanism   | Specify how the New Resource Group is set for Active Directory (AD) authenticated users:  
  • Allow user to choose – users specify an SMS group as their New Resource Group  
  • Use Active Directory Primary Group – automatically sets the AD primary group as the New Resource Group; users are unable to set the group manually. Typically, the default primary AD group is Domain Users.  
  • Use Active Directory ... attribute – specify an AD attribute for the SMS to use in mapping a New Resource Group for all AD-authenticated SMS users. |
| Mapping Failure Action                 | Select an action to take when an Active Directory group cannot be mapped:  
  •  
  •  
  •  

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Reject Authentication</td>
<td></td>
</tr>
<tr>
<td>• Accept Authentication with local sms group mappings – available only if Authentication Mode is configured to allow only users defined in the SMS to log in.</td>
<td></td>
</tr>
<tr>
<td>• Accept Authentication – Select an SMS user group to which the user is assigned for authorized access.</td>
<td></td>
</tr>
</tbody>
</table>

4. Click **OK**.

An X509 certificate is required for validating authentication responses over an SSL connection. The certificate is generated on the Active Directory server, and must be imported to the SMS. The SMS server accepts DER (binary) or PEM (Base64) encoded X509 certificates.

**Import an Active Directory SSL certificate**

1. On the Active Directory tab, click **Import** to the right of the Active Directory SSL Certificate panel.
2. Select the X509 certificate file from your local drive or storage media, and click **Import**.

   **Important:** A certificate import is a separate operation from configuring the authentication source and takes effect immediately. The SMS administration should carefully coordinate certificate and the Active Directory configuration changes.

3. (Optional) If you have already imported a certificate into the SMS certificate repository, simply choose the one you want. For more information about certificate management, see *Viewing Certificate Authority (CA) certificates* on page 573.

**Configure TACACS+ authentication**

Terminal Access Controller Access-Control System Plus (TACACS+) is another industry-standard method used to authenticate user login requests.

TACACS+ authenticates over TCP. Because TCP is a connection-oriented protocol, TACACS+ does not require transmission control the way RADIUS does. While RADIUS encrypts only passwords, TACACS+ uses MD5 encryption on all communication and is consequently less vulnerable to attacks.

Unlike RADIUS authorization, the role (privilege level) of a TACACS+ user is determined by the TACACS default-user group configuration on the TPS device. For example, if the TACACS+ default-user group is set to *operator*, TACACS users are assigned the *operator* role. This might not provide sufficient control for the user's environment. To assign a TACACS+ user a higher role from the default-user group role:

1. On the TPS device, create a local user that uses the same name as the TACACS user.
2. Assign that local TPS user to a user group. The TPS device references that user group to determine the authorization level of the TACACS user.
Note: Because authentication is through the TACACS+ server, do not create a password for the local TPS user.

This differs from RADIUS authorization; for that, TPS devices can use the filter ID returned from the RADIUS server during user authentication to determine a RADIUS user role. If the RADIUS server does not return the filter ID, the TPS device uses the RADIUS default-user group configuration to determine the user role.

Although user authentication is performed on the TACACS+ server, user authorizations and access rights are maintained on the SMS server. If the TACACS+ server is unavailable, the SMS can authenticate local users. The SMS does not permit you to manage SMS user accounts on the TACACS+ server; the account password for a TACACS+ authenticated user must be changed on the TACACS+ server.

Edit the TACACS+ server configuration

1. On the Authentication screen, select the TACACS+ tab on the Authentication Configuration panel.
2. Click Edit to the right of the Primary TACACS+ Server panel.
3. In the dialog, configure the TACACS+ server options described in the following table.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address / Hostname</td>
<td>IP address or hostname of the TACACS+ server. The IP Address field can contain an IPv4, IPv6, or named IP address. The Hostname field can contain an unqualified hostname or a fully qualified hostname (hostname+domain name).</td>
</tr>
<tr>
<td>Port</td>
<td>Port on the TACACS+ server that listens for authentication requests; the default is port 49.</td>
</tr>
<tr>
<td>Authentication Protocol</td>
<td>Authentication method used on the TACACS+ server:</td>
</tr>
<tr>
<td></td>
<td>• ASCII</td>
</tr>
<tr>
<td></td>
<td>• PAP (default)</td>
</tr>
<tr>
<td></td>
<td>• CHAP</td>
</tr>
<tr>
<td></td>
<td>• MSCHAP (supported with IPS devices only)</td>
</tr>
<tr>
<td>Secret/Confirm Secret</td>
<td>Case-sensitive string used to encrypt and sign packets between TACACS+ clients and the TACACS+ server, set in the TACACS+ client configuration file. Maximum is 63 characters.</td>
</tr>
<tr>
<td>Setting</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Timeout</td>
<td>Timeout, in seconds, for communication with the TACACS+ server. Default is 15.</td>
</tr>
<tr>
<td>Attempts</td>
<td>Number of times, between 1 and 10, communication with the TACACS+ server is attempted. Default is 3 attempts.</td>
</tr>
</tbody>
</table>

4. Test the TACACS+ configuration by entering a valid User Name and Password for the server, and then clicking **Test**.

5. Click **OK** to save the server configuration.

6. If a TACACS+ server is already configured, click **Reset** to the right of the TACACS+ Server panel to delete that configuration.

   If the configuration you reset is the last configured TACACS+ server, and if TACACS+ is the current authentication choice, then the SMS changes the current authentication source to Local.

You can also change the configuration of TACACS+ servers by selecting **Devices > device-name > Authentication > TACACS+ Groups > Edit > TACACS+ Servers > Edit**.

**Configure CAC authentication**

Common Access Card (CAC) authentication enables you to secure SMS client access by using two-factor authentication, which is more secure than the standard username and password authentication.

CAC Authentication on the SMS offers:

- Interoperability with ActivClient software and Windows compatible smart card readers.
- Support for Common Access Cards (CAC).
- Compatibility with major certificate authorities using Public Key Infrastructure (PKI).

<table>
<thead>
<tr>
<th>CAC authentication on the SMS</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ActivClient software</td>
<td>ActivClient extracts certificate information from the CAC that the SMS uses to authenticate users. ActivClient interacts with identification tokens, certificate authorities, and smart card readers.</td>
</tr>
<tr>
<td>Certificate management</td>
<td>PKI certificates come from an approved Certificate Authority (CA) and are used to verify and authenticate the card holder.</td>
</tr>
<tr>
<td>CAC authentication on the SMS</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Go to Admin &gt; Certificate Management &gt; CA Certificates to import, replace, and view certificate details.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Personal identifier</th>
<th>The Personal identifier is a 10-digit number used to uniquely identify the card holder.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Go to Admin &gt; Authentication and Authorization &gt; Authentication to import, edit, or delete personal identifiers.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CAC authentication</th>
<th>When CAC authentication is enabled on the SMS:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• All users must use their CAC and PIN to log in to the SMS client.</td>
<td></td>
</tr>
<tr>
<td>• Users will not be able to access the SMS Web client.</td>
<td></td>
</tr>
<tr>
<td>• The SMS will not allow an administrator to designate user accounts to be authenticated locally (local authentication).</td>
<td></td>
</tr>
<tr>
<td>Go to Admin &gt; Authentication and Authorization &gt; Authentication to select the authentication source that the SMS will use to authenticate users.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Managing user roles and user accounts</th>
<th>The SMS uses capabilities and roles to give users permissions to perform specific actions.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Go to Admin &gt; Authentication and Authorization &gt; Roles to set the capabilities for each role.</td>
<td></td>
</tr>
<tr>
<td>Users with enabled access to the SMS CLI capability can log in from the SMS CLI to disable CAC authentication, which sets the SMS back to the default authentication method (local authentication).</td>
<td></td>
</tr>
<tr>
<td>Go to Edit/Create Role &gt; Capabilities &gt; Admin &gt; SMS Management &gt; Access Management &gt; Access SMS CLI to expand or limit this capability.</td>
<td></td>
</tr>
<tr>
<td>When CAC authentication is enabled on the SMS, the Personal Identifier will be required when you create a new user account.</td>
<td></td>
</tr>
</tbody>
</table>
CAC authentication overview

The following diagram illustrates the prerequisites required before you can configure the SMS to use CAC authentication. It also shows the high-level steps needed to enable CAC authentication on the SMS. Once CAC authentication is enabled, it shows how SMS users can log on to the SMS.
Prerequisites:

Install the ActivClient software.

Install the SMS Client & verify the cac.properties reference the ActivClient DLL.

How to enable CAC Authentication on the SMS:

1. Import CA Certificates.
2. Add/Import Personal Identifier.
3. Configure CAC as authentication source.
4. Attach USB card reader to the SMS client workstation.
5. To enable CAC Authentication, log out of the SMS client.

How to log in to the SMS when CAC Authentication is enabled:

1. Insert CAC into the card reader.
2. Enter PIN.
3. Select the correct certificate.
Prerequisites

All SMS client workstations that are enabled with CAC authentication source require ActivClient software, a Windows compatible smart card reader, and the common access card (CAC).

ActivClient software requirements

ActivClient must already be installed and configured before you can configure CAC authentication in the SMS. ActivClient is supported on the following Windows operating systems.

<table>
<thead>
<tr>
<th>Windows operating system</th>
<th>ActivClient version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 7 (32- and 64-bit)</td>
<td>ActivClient 6.2 or ActivClient 7.0.2</td>
</tr>
<tr>
<td>Windows 8 (32- and 64-bit)</td>
<td>ActivClient 6.2 or ActivClient 7.0.2</td>
</tr>
</tbody>
</table>

Perform the following tasks before you configure CAC authentication on the SMS:

1. Install the ActivClient software. For additional details, refer to the ActivClient documentation.
2. Disable all other smart card readers. To do this, go to Control Panel > Hardware and Sound > Device Manager > Smart card readers, right-click on any other enabled driver, and then click Disable.
3. Install the SMS client. See Install the SMS client on page 7.
4. Verify the SMS client references the ActivClient DLL.
   To do this, go to the location where you installed the SMS client, expand the config folder, and then open the cac.properties file.
   The file contains name, library, and description details, and the path is similar in format to the following:
   
   library="C:/Program Files/ActivIdentity/ActivClient/acpkcs211.dll"
   
   Note: If the cac.properties file is not available under the SMS client program files, make sure you have installed ActivClient and either install the software again or refer to the ActivClient documentation.

Import CA Certificates

Certificates come from an approved Certificate Authority (CA) and are used to validate the CAC certificate when the card holder attempts to log in to the SMS.

1. Go to Admin > Certificate Management > CA Certificates.
2. Click Import and then do the following:
   a. Enter a name for the certificate in the Certificate Name field.
b. Click **Browse** and then browse to and select the certificate.

c. Select the certificate format according to the certificate file.

d. Click **OK**.

3. Repeat Steps 1-3 for all Root and Intermediate certificates that are used in the chain of validation.

---

**Add, edit, import, or delete personal identifiers**

When managing the personal identifiers for SMS users, keep in mind:

- You can configure personal identifiers for user accounts without having to enable CAC authentication.
- The current user must have a personal identifier to enable CAC authentication.
- When CAC authentication is enabled on the SMS, the current user’s personal identifier cannot be deleted.
- Each personal identifier must be a unique number. If you enter or import a personal identifier that is already associated to an existing SMS user account, the SMS will display an error message.
- When CAC authentication is enabled on the SMS, the personal identifier will be required when you create a new user account.

1. Go to **Admin > Authentication and Authorization > Authentication**.
2. Click the **CAC** tab.
3. Do one of the following:

   - Select an SMS user name, and then click **Edit Personal Identifier** to enter or modify the 10-digit number used to uniquely identify the user.

   - Click **Import Personal Identifier(s)**, and then browse to and select the CSV file that contains a record of SMS user names and 10-digit numbers. (The user names and personal identifiers must be enclosed in quotation marks).

     The Personal Identifier Import Results lists the total number of imported records, the number of changed and unchanged personal identifiers, and any errors. The SMS will display an error if the file contains unknown SMS user names or duplicate or invalid personal identifiers. From here you can compare the personal identifiers and user names. Click **Save Personal Identifier(s)** to commit the changes.

   - Select one or more SMS user names, and then click **Delete Personal Identifier(s)** to remove the 10-digit number from the selected user.

4. Click **OK**.

---

**Enable CAC authentication**

After you import the CA Certificates and add the personal identifiers for SMS user accounts, you can configure the SMS to authenticate user login requests using CAC authentication.
When CAC authentication is enabled on the SMS, keep in mind:

- All users must use their CAC and PIN to log in to the SMS client.
- Users will not be able to access the SMS Web client. If a user backs up the SMS database, the backup will not be available on the Web client, but it will be available on the SMS at Admin > Database > Backup.

2. Under Authentication Source, click Edit.
3. Select Use CAC Authentication.

   **Note:** The SMS will not allow an administrator to designate user accounts to be authenticated locally (Local Authentication). However, users (with SMS CLI role capabilities) can log in to the SMS command line interface (CLI) to disable CAC authentication. Disabling CAC authentication sets the SMS back to the default authentication method (Local Authentication). For more information, see Managing user roles on page 558.

4. Click OK.
5. To enforce CAC authentication, do the following:
   a. Attach the USB card reader to the SMS client workstation.
   b. Log out of the SMS client.

*Log in to the SMS using CAC authentication*

When CAC authentication is enabled on the SMS, all users must log in using a CAC and a PIN.

1. Insert your Common Access Card (CAC) into the card reader.
2. Type the IP address in the SMS Server field.
3. Enter your PIN, and then click OK.
4. Select the appropriate certificate from Certificates drop-down list.
5. Click Login.

*Managing user roles*

The SMS uses capabilities and roles to give users permissions to perform specific actions within the system. A capability is an ability to affect an object in the system; for example, the ability to add a device. A role is a collection of capabilities.

The SMS uses three predefined, basic roles: superuser, admin, and operator. You cannot modify the predefined system roles, but you can use them as starting points to initialize new roles. When you create a role, you can select a base system role from which to initialize the new role. The new role is given the same capabilities as the system role it is initialized from, until you customize the capabilities.
You can create new roles to expand or limit the capabilities of existing roles or to target a specific set of capabilities for a group of SMS users. You can further control the access rights and capabilities of users through Groups. See Managing user groups on page 560.

The User Roles screen displays a list of user roles. This screen enables you to create new user roles as well as edit, delete, and save copies of existing roles.

In the Admin workspace, expand Authentication and Authorization in the navigation pane and select Roles to display the User Roles screen.

Create a user role

1. On the User Roles screen, click New.

2. In the Create Role wizard, provide the following information:
   
   • Role Name – Name for the role you are defining. For example, you might assign the name DeviceAdmin to a role that includes the full set of capabilities for managing devices in the SMS.
   
   • Role Description – Provide more detail to describe the role you are defining.
   
   • Initialize from System Role – Select the system role (SuperUser, Admin, or Operator) you want to use to initialize the new role, or select None.

3. Click Next.

4. On the Capabilities screen, select the capabilities you want to assign to the role.

   If you initialized this role from a system role, capabilities for that system role are preselected. (If you initialized the new role with no system role, then no capabilities are preselected.) You can clear these selections and select new capabilities as needed.

   The Capabilities screen displays a green checkmark to indicate whether an Admin or Operator role includes that specific capability. The SuperUser role includes all capabilities.

   Click an icon in the Capabilities screen toolbar to view the capabilities for that functional area, and then select the capabilities you want to assign to the role, using the following options:

   • All capabilities for a functional area: Select the top-level list item, so that a checkmark appears to the left of every capability in the list.
   
   • All capabilities in a group: Select a parent list item, so that a checkmark appears to the left of every capability under that parent.
   
   • Named capabilities: Select one or more named capabilities from the list. If you select single capabilities, consider that one capability may depend on others for full access rights to complete a task. For example, the Distribute profile capability also requires the Snapshot management capability to successfully distribute profiles.

   Note: Capabilities are listed hierarchically in groups; child capabilities are required for that particular group function.
5. Click **Finish** to complete the role definition.

If a user role was initialized from a system role, the specified system role determines how the user role is affected during an SMS upgrade. Capabilities that were added for a new SMS release are added to this role based on the system role specified.

When you edit a user role, you can change the base system role that the SMS uses to determine what to do during an SMS upgrade. For example, if you created a user role based on the Admin system role, but you do not want this role automatically updated with new Admin role capabilities during an upgrade, you can change the value for the **Upgrade As** field to “None.”

You cannot edit the predefined system roles, but you can initialize new user roles based on a system role (as described above), or you can copy the system role by selecting it in the User Roles list and clicking **Save As**.

To delete an unused or unwanted user role, select the role from the User Roles list, and click **Delete**. In the Confirmation dialog, click **OK** to confirm that you want to permanently delete the role.

**Note:** You cannot delete a role when it is in use by a Resource Group.

**Edit a user role**

1. On the User Roles screen, select the user role you want to edit and click **Edit**.
2. In the Edit Role wizard, make the necessary changes on the Name & Description screen and the Capabilities screen.
3. Click **OK** to save your changes to the user role.

**Managing user groups**

SMS user groups provide a way to align user capabilities with functional areas on the SMS. An user group pairs a role with resources that group members can access.

The SMS has one predefined group called **superuser**. The system superuser group includes the superuser role and provides access to all SMS features and functionality. Give careful scrutiny before you assign users to the superuser group.

In a typical new installation, you must create new user groups to specify access rights for users who do not have superuser privileges. The new groups assign role capabilities (such as admin and operator capabilities) to resources. The role assigned to a group specifies the rights to execute the capabilities to manage the group resources, such as devices and profiles. If Active Directory authentication is configured for the SMS, users may be authorized through a mapped AD group.

Any user account that logs on to the SMS must be assigned to at least one user group, because a user account must have a New Resource Group. See **Managing active sessions** on page 542. You can use user groups to delineate the functional capabilities of users by authorizing, at a granular level, which security tasks can be implemented from the SMS on TippingPoint devices. The User Groups screen displays a list of groups, the role associated with the group, and a description provided for the defined group. This screen
enables you to create, edit, and delete user groups. In the Admin workspace, expand Authentication and Authorization in the navigation pane and select Groups to display the User Groups screen.

**Create a user group**

1. On the User Groups screen, click **New**.

2. In the Create Group wizard, provide the following information:
   - **Group Name** – Provide a name for the user group. This should be a name that is meaningful in describing the purpose of the group. For example, if the group is to limit management activities to test devices only, consider naming the group TestDeviceManagers.
   - **Role** – Select a role to be assigned to the user group. You can select an existing role, create a new role, or select a role and edit the role capabilities. See [Create a user role](#) on page 559 and [Edit a user role](#) on page 560.
   - **Group Description** – Provide a detailed description of the user group. (Optional).

   **Note:** When you assign a role, keep in mind that you cannot modify predefined system roles. If you edit role capabilities for a user role, changes are saved to the role, not just to the group.

3. Click **Next** to display the next screen in the wizard, or select a category in the navigation pane, and then specify the following options:

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Devices</td>
<td>Select devices (if any) that group members have access permissions to manage.</td>
</tr>
<tr>
<td>Segment Groups</td>
<td>Select segment groups (if any) that group members have access permissions to manage.</td>
</tr>
<tr>
<td>Profiles</td>
<td>Select profiles (if any) that group members have access permissions to manage.</td>
</tr>
<tr>
<td>DV Toolkit Packages</td>
<td>Select DV Toolkit packages that group members have access permissions to manage.</td>
</tr>
<tr>
<td>Action Sets</td>
<td>Select action sets that group members have access permissions to manage.</td>
</tr>
<tr>
<td>Reports</td>
<td>Select reports that group members have access permissions to manage.</td>
</tr>
</tbody>
</table>

4. Click **Next**, or select **Active Directory Global Group Mapping** in the navigation pane, and then do one of the following to map the SMS group name to an Active Directory group name:
• Select **Map this group to the same named group in active directory** if you have named this group the same as a group in the Active Directory to which you will map.

• Select **Map this group to a specific active directory group** to map this user group to a named group in Active Directory that is different than the name of this group. If you select this option, then specify the group name in the text box. Enter the user group without entering the fully qualified distinguished name; for example, Domain Users.

If you provided an Active Directory Global Group Mapping, click **Test** to test the mapping.

5. Click **Finish** to close the Create Group wizard.

**Edit a user group**

1. On the User Groups screen, click **Edit**.

2. In the Edit Group wizard, make changes as necessary. See *Create a user group* on page 561.

3. Click **OK** to close the Edit Group wizard.

**Delete a user group**

1. On the User Groups screen, click **Delete**.

2. In the Delete User Groups dialog, click **OK** to confirm.

**Note:** To delete a group, you must have appropriate permissions, such as superuser authorization or **SMS Auth Management** and **SMS Group Management** capabilities. You cannot delete a group that is in use by any users.

**Managing user accounts**

The User Accounts screen displays a list of SMS user accounts as well as basic information, as described in the following table. This screen enables you to create, edit, and delete user accounts.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>Indicates whether the user ID is enabled (green checkmark) or disabled (blank).</td>
</tr>
<tr>
<td>User Id</td>
<td>Displays the user identifier, which is commonly referred to as <strong>username</strong>. This is the identifier a user provides to log in to the SMS client.</td>
</tr>
<tr>
<td>Groups</td>
<td>Displays the SMS user groups in which the user account is a member. Groups specify functional areas and tasks the user account can access. The group may be a predefined group (superuser, admin, or operator) or a custom group.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Password Exp</td>
<td>Displays the settings for password expiration. The system-wide security level affects password requirements.</td>
</tr>
<tr>
<td>Name</td>
<td>Displays the name of the contact for the user account, specified in Contact Details.</td>
</tr>
<tr>
<td>Email</td>
<td>Displays the email address for the user account, specified in Contact Details.</td>
</tr>
<tr>
<td>Local</td>
<td>Indicates whether authentication of the user occurs locally on the SMS Server or on a remote authentication server such as RADIUS, Active Directory, or TACACS+.</td>
</tr>
</tbody>
</table>

Administration of SMS user accounts involves functionality located on this screen as well as other parts of the Authentication and authorization on page 542 area. To manage user sessions, see Managing active sessions on page 542.

In the Admin workspace, expand Authentication and Authorization in the navigation pane and select Users to display the User Accounts screen.

**User accounts**

The SMS server is a critical component of the TippingPoint network security solution. Security of the SMS Server is itself critical, given that tasks performed on the SMS server can affect the availability, performance, and configuration of network security devices.

User administration should take into consideration user roles and correlating group assignments, password requirements, and user ID requirements. The tasks users are required to perform in the SMS must have access privileges and permissions defined in the group or groups to which the user account is assigned.

General guidelines for creating a new user account include the following:

- Specify a user name that meets the requirements of the selected security level.
- Specify a password that adheres to the guidelines set by the security level.
- Assign the user to a group.

**Specify a user name**

Specify a user name that meets the requirements of the security level selected during SMS server configuration. Use the following table as a guide.
<table>
<thead>
<tr>
<th>Security level</th>
<th>Username requirements</th>
</tr>
</thead>
</table>
| Level 0        | • User names cannot contain spaces.  
|                | • Must be unique in the first 32 characters.  
|                | • Contain a maximum of 150 characters.  |
| Levels 1, 2, and 3 | A valid user name must meet Level 0 requirements and the following:  
|                | • Must contain at least 6 characters.  |

**Note:** Security level is system-wide. To view or modify the system-wide settings, select **Edit > Preferences**. See *Security* on page 38.

### Specify a password

Specify a password that adheres to the guidelines set by the security level. The SMS enforces secure access through security policies that are specified by the security level set in the system preferences. See *Security* on page 38.

We recommend that you use Level 3 security, which enforces the highest level of security for access to the SMS server.

### Assign the user to a group

Assign the user to a group. If you assign a user to multiple groups, set a default group that will contain any new resources created by the user with access rights. This group is referred to as the New Resource Group. See *Managing active sessions* on page 542.

The user inherits the access permissions and user role capabilities defined for an assigned group. See *Managing user groups* on page 560.

### Create a user account

1. On the User Accounts screen, click **New**.
2. In the Create User wizard, provide the following information on the Authentication screen:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>Select <strong>Enabled</strong> to enable this user account when it is created, or clear the check box to create a disabled account.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>User Id</td>
<td>Enter a unique user name. Be sure you know which security level is set, and then adhere to the requirements for that level. See Table on page 563.</td>
</tr>
<tr>
<td>Password/ Confirm Password</td>
<td>Enter a password for the account that meets security level requirements. See Table on page 564. Re-enter the password in the Confirm Password field.</td>
</tr>
<tr>
<td>Password Expiration</td>
<td>Select <strong>Enabled</strong> and specify a number of days (1–365) to enable password expiration for the account.</td>
</tr>
<tr>
<td>Change password on next login</td>
<td>Select <strong>Change password on next login</strong> to require the user to change the account password on next login.</td>
</tr>
<tr>
<td>Authentication</td>
<td>Select <strong>Local Authentication Only</strong> if this SMS user must authenticate using SMS local credentials. See Authentication source on page 544.</td>
</tr>
</tbody>
</table>

3. Click **Next**, or select **Group Membership** in the navigation pane, and assign a group to the account.

   Click **Add** and select the group or groups to assign to the account then click **OK**.

   **Note:** By default, the first group assigned to the user account becomes its New Resource Group. If you assign multiple groups to a user, then you can designate any one of them as New Resource Group. Select the group and click **Set Resource Group**.

4. Click **Next** and provide the information requested in the **Contact Details** area, including contact name, email address, phone number, and cell phone number.

5. Click **Finish** to complete the user account setup.

   The User Account screen enables you to edit user accounts, including scenarios in which you need to change the password for a user account or you need to add or change the group assignments for a user account.

   **Note:** You cannot change Active Directory user account passwords in the SMS. For an AD account used to log on to the SMS, you must change the password on the Active Directory server.

**Edit a user account**

1. On the User Accounts screen, select a user account and click **Edit**.

2. In the Edit User wizard, go to the appropriate screen (Authentication, Group Membership, or Contact Details), and make changes as necessary.

   See **Create a user account** on page 564.
3. Click **OK** to close the Edit User wizard.

   **Note:** To change a user password, you must either be logged in as the user whose password you want to change or be logged in with SuperUser capabilities.

Delete a user account

1. On the User Accounts screen, select a user account and click **Delete**.
2. In the Delete User(s) dialog, click **Yes** to confirm.

   **Note:** You can delete users whose accounts are enabled or disabled. If you delete a user that has an active session, the user will be deleted but the active session will remain until the user logs off or the session is ended.

## Certificate Management

Certificate management enables the SMS to maintain a central repository from which certificates and private keys are automatically distributed to the appropriate TippingPoint devices. Unlike previous releases, you no longer need to load the certificates and private keys onto each device. Instead, import your certificates and private keys into the SMS, and update the device configuration to assign the appropriate certificates.

Certificate Management provides general X.509 certificates management on the SMS and its managed devices using the following:

- *The SMS certificate password* on page 566
- *Certificates* on page 568
- *Certificate Authority (CA) certificates* on page 573
- *Revocation* on page 575
- *Certificate Signing Requests (CSRs)* on page 577

### Managing the SMS certificate password

The SMS certificate password protects the private keys in the SMS certificate repository with encryption. The SMS encrypts the private keys using a randomly generated 2048-bit RSA key pair. The private key of this key pair is encrypted using a 256-bit AES cipher based on your SMS certificate password.

Setting up the SMS certificate password is required when you import private keys into the SMS certificate repository.

**Note:** Managing the SMS certificate password requires the *Admin Certificate Management* capability in your user role.
Private key encryption status

<table>
<thead>
<tr>
<th>Status</th>
<th>What it means</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unused</td>
<td>There are no private keys in the SMS certificate repository. You can set up the SMS certificate password without importing private keys.</td>
</tr>
<tr>
<td>Setup Required</td>
<td>There are private keys pending to be in the SMS certificate repository. Click <strong>Setup Encryption</strong> to set up the SMS certificate password to import private keys.</td>
</tr>
<tr>
<td>Password Required</td>
<td>Enter the SMS certificate password to manage certificates with private keys and export them to devices. Go to <strong>Admin &gt; Certificate Management &gt; Enter Password.</strong></td>
</tr>
</tbody>
</table>

Set up encryption

Once you set up the SMS certificate password, keep in mind:

- The SMS does not store the SMS certificate password. You must enter this password every time the SMS server restarts.
- There is no way to recover a lost password. If you lose your password, you must reset your password. Resetting the SMS certificate password deletes all of the private keys in the SMS certificate repository, which breaks the corresponding certificates. To repair the broken certificates, re-import your private keys.

1. Go to **Admin > Certificate Management.**
2. Click **Setup Encryption.**
3. Provide a password in the password and the confirm fields.
4. Click **OK.**

A new RSA key pair is generated after password validation. The new password encrypts the private key of this key pair which encrypts your private keys in your SMS certificate repository.

Change the certificate password

Change the SMS certificate password to update the password that secures the SMS certificate repository.
Changing the certificate password requires the current SMS certificate password.

**Note:** Changing the certificate password requires the *Admin Certificate Management* capability in your user role.

1. Go to **Admin > Certificate Management**.
2. Click **Change Password**.
   
   Provide the current password and a new password in the Change SMS Certificate Password dialog.
3. Click **OK**.

### Reset the certificate password

Reset the SMS certificate password to delete the private keys in the SMS certificate repository and create a new SMS certificate password. Resetting the SMS certificate password is only necessary when you have lost the SMS certificate password.

If you want to change the SMS certificate password, we recommend that you do not reset the certificate password. Resetting the SMS certificate password breaks the corresponding server certificates for:

- SSL inspection
- SMS web server

A broken certificate cannot be used until it is repaired. For information about repairing a broken certificate, see *Repair a certificate* on page 572.

To avoid losing any pending CSRs created by the SMS, we recommend resetting the SMS certificate password after you import the corresponding CA certificate and public key. After the SMS certificate password is reset, the SMS cannot associate the CSR private key in the certificate repository with the new CA certificate and public key.

**Note:** Resetting the certificate password requires the *Admin Certificate Management* capability in your user role.

1. Go to **Admin > Certificate Management**.
2. Click **Reset**.
   
3. Click **OK**.

### Viewing certificates

The Certificates table lists the server certificates in the SMS certificate repository. Right-click the certificate and select **Show Usage** to view certificate usage.

The following table describes the fields in the Certificates table.
**Important:** The SMS does not notify you when a certificate is about to expire. Use the Certificates table to verify that the certificates are up-to-date and avoid expired certificate errors.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>An icon with the private key status and a unique identifier for the certificate. Hover over this column to view data from the certificate.</td>
</tr>
<tr>
<td>Issued To</td>
<td>The Subject Common Name (CN).</td>
</tr>
<tr>
<td>Issued By</td>
<td>The Issuer Common Name (CN).</td>
</tr>
<tr>
<td>Status</td>
<td>An icon with verification status and the state of the certificate.</td>
</tr>
<tr>
<td>Expires On</td>
<td>The date and time of the expiration of the certificate.</td>
</tr>
</tbody>
</table>
| Private Key| One of the following:  
  • Checkmark – The certificate has a private key.  
  • Empty circle – The certificate does not have a private key.  
  • Broken – The certificate is missing its private key after an SMS certificate password reset. Repair the certificate by reimporting the private key. |
| Exportable| One of the following:  
  • Checkmark – The certificate and the private key can be exported.  
  • Empty circle – The private key cannot be exported. |
Import a certificate

Importing a certificate to the SMS certificate repository makes that certificate available to the SMS and all managed devices for:

- SSL inspection. For more information, see *Manage SSL inspection from the SMS* on page 661.
- SMS web server. For more information, see *SMS web security SSL certificate* on page 535.
- Captive portals. For more information, see *Captive portal rules* on page 245.

**Note:** Importing certificates requires the *Admin X509 Certificate Management* capability in your user role.

1. Go to **Admin > Certificate Management > Certificates**.
2. Click **Import**.
3. Provide a unique certificate name to reference a PEM/DER certificate or a unique base name for PKCS12 certificates in the Certificate Name field.
4. Browse to and open a certificate in the Certificate File field.
5. Select the file format of the certificate.
   - PEM/DER format allows optional private key file import. Browse to and open the associated private key. If the private key is encrypted, enter the appropriate password in the Password field.
   - PKCS12 format imports multiple certificates with or without private keys. If the private keys are encrypted, enter the appropriate password in the Password field.
6. Check Private Key Export to enable private key export from the SMS, and include private keys in the SMS backup.

   Disabling private key export cannot be undone. If necessary, you can disable private key export later by right-clicking the certificate in the Certificates table and selecting **Make Non-Exportable**.
7. Click **OK**.

Export a certificate

Exportable certificates and their associated private keys can be written to a file for external use.

**Note:** Exporting a certificate and a key to a file requires the *Admin X509 Certificate Private Key Management* capability in your user role and the SMS certificate password.

1. Go to **Admin > Certificate Management > Certificates**.
2. Click **Export**.
3. Select a file format for your certificate, private key, or both.
   You can enter an optional password to encrypt `.p12` or `.key` files.
4. Specify the file name and location under Export To File.
5. Click **OK**.

### Replace a certificate

Replace a certificate with a new one, for example, when you have certificates which have expired or will expire soon. When you replace a certificate, the SMS certificate repository automatically updates managed devices with the new certificate.

Simply adding the new certificate and deleting the old one would require you to also update any configuration settings to use the new certificate. Replacing the certificate changes the certificate while preserving any existing references in these configuration settings.

When replacing a certificate, consider the following:

- A certificate with a private key must be replaced by another certificate with a private key.
- A certificate without a private key must be replaced by another certificate without a private key.
- The replacement certificate is not already in the SMS certificate repository.
- You must have the *Device X509 Certification Configuration* capability in your user role for all of the devices where the certificate is replaced.
- All devices with the certificate must be managed by the SMS at the time of replacement. If the SMS cannot communicate with all of the devices with the certificate, the SMS displays an error message.

**Note:** Replacing certificates requires the *Admin X509 Certificate Management* capability in your user role.

1. To replace certificates, go to **Admin > Certificate Management > Certificates**. To replace CA certificates, go to **Admin > Certificate Management > CA Certificates**.
2. Click **Replace**.
   - For certificates with a private key, browse to and open a certificate. For PEM/DER certificates, browse to and open the associated private key. (Optional) Provide a password to encrypt the private key.
   - For certificates without a private key or CA certificates, browse to and open a certificate. Private keys in PKCS12 files are ignored. Select the file format of the certificate.
3. Click **OK**.

The replaced certificate is saved under the original name with `_REPLACED` appended. The new certificate replaces the old certificate on the corresponding devices and the SMS.
Repair a certificate

Repair a broken server certificate to re-import its private key into the SMS certificate repository. Repairing a certificate is necessary, for example, when you reset the SMS certificate password, or when you restore a backup which does not include private keys.

1. Go to Admin > Certificate Management > Certificates.
2. Right-click the broken certificate and select Repair.
3. Browse to and open the corresponding private key file.
4. Select the file format of the private key.
5. (Optional) Provide a password to encrypt the private key.
6. Click OK.

The new private key is copied to the private key file of the broken certificate.

Make a private key non-exportable

Make a private non-exportable to disable private key export from the SMS, and if the SMS backup is configured to include private keys, exclude the private key from the SMS backup. This command is useful for securing a private key that was imported into the SMS without disabling private key export.

To make a private key exportable after you make it non-exportable, you must delete the corresponding certificate and private key and then re-import the certificate and private key.

Note: Making a private key non-exportable requires the Admin X509 Certificate Private Key Management capability in your user role.

1. Go to Admin > Certificate Management > Certificates.
2. In the Certificates table, right-click a certificate with an Exportable private key and click Make Non-Exportable.

Delete a certificate

Delete a certificate to remove it from the SMS certificate repository and any managed devices. If the certificate is in use by the SMS or a managed device, you cannot delete it.

Note that to make a private key exportable after you make it non-exportable, you must delete the corresponding certificate and private key, and then reimport the certificate and private key.

Note: Deleting a private key requires the Admin X509 Certificate Private Key Management capability in your user role.

1. Go to Admin > Certificate Management > Certificates.
2. In the Certificates table, right-click a certificate and click Delete.
Viewing Certificate Authority (CA) certificates

The CA Certificates table lists the CA certificates in the SMS certificate repository. CA certificates are issued by a CA and do not have private keys. Right-click the CA certificate and select **Show Usage** to view CA certificate usage.

The following table describes the fields in the CA Certificates table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>An icon with the type of the CA certificate and a unique identifier for the CA certificate. Hover over this column to view data from the CA certificate.</td>
</tr>
<tr>
<td>Issued To</td>
<td>The Subject Common Name (CN).</td>
</tr>
<tr>
<td>Issued By</td>
<td>The Issuer Common Name (CN).</td>
</tr>
<tr>
<td>Status</td>
<td>An icon with verification status and the state of the CA certificate.</td>
</tr>
<tr>
<td>Expires on</td>
<td>The date and time of the expiration of the CA certificate.</td>
</tr>
</tbody>
</table>

**Import a CA certificate**

Importing a CA certificate to the SMS certificate repository makes that CA certificate available to the SMS and all managed devices for:

- Radius authentication (SMS and device)
- LDAP authentication (SMS)
- VPN configuration
- Remote syslog

**Note:** Importing CA certificates requires the **Admin X509 Certificate Management** capability in your user role.

1. Go to **Admin > Certificate Management > CA Certificates.**
2. Click **Import.**
3. Provide a unique certificate name to reference a PEM/DER certificate or a unique base name for PKCS12 certificates in the Certificate Name field.

4. Browse to and open a CA certificate in the Certificate File field.

5. Select the file format of the CA certificate.

6. Click **OK**.

**Export a CA certificate**

CA certificates can be written to a file for external use.

**Note:** Exporting a CA certificate requires the *Admin X509 Certificate Private Key Management* capability in your user role and the SMS certificate password.

1. Go to **Admin > Certificate Management > CA Certificates**.

2. Click **Export**.

3. Select a file format for your CA certificate.
   
   You can enter an optional password to encrypt `.p12` files.

4. Specify the file name and location under Export To File.

5. Click **OK**.

**Replace a CA certificate**

Replace a certificate with a new one, for example, when you have certificates which have expired or will expire soon. When you replace a certificate, the SMS certificate repository automatically updates managed devices with the new certificate.

Simply adding the new certificate and deleting the old one would require you to also update any configuration settings to use the new certificate. Replacing the certificate changes the certificate while preserving any existing references in these configuration settings.

When replacing a certificate, consider the following:

- The replacement certificate is not already in the SMS certificate repository.
- You must have the *Device X509 Certification Configuration* capability in your user role for all of the devices where the certificate is replaced.
- All devices with the certificate must be managed by the SMS at the time of replacement. If the SMS cannot communicate with all of the devices with the certificate, the SMS displays an error message.

**Note:** Replacing certificates requires the *Admin X509 Certificate Management* capability in your user role.

1. To replace certificates, go to **Admin > Certificate Management > Certificates**. To replace CA certificates, go to **Admin > Certificate Management > CA Certificates**.

2. Click **Replace**.
• For certificates with a private key, browse to and open a certificate. For PEM/DER certificates, browse to and open the associated private key. (Optional) Provide a password to encrypt the private key.
• For certificates without a private key or CA certificates, browse to and open a certificate. Private keys in PKCS12 files are ignored. Select the file format of the certificate.

3. Click **OK**.

   The replaced certificate is saved under the original name with `_REPLACED` appended. The new certificate replaces the old certificate on the corresponding devices and the SMS.

### Managing Revocation

Revocation in Certificate Management verifies the certificates issued by the CA certificates in the SMS certificate repository. You can specify Online Certificate Status Protocol (OCSP) settings and Certificate Revocation List (CRL) locations for each CA certificate.

#### Viewing Online Certificate Status Protocol (OCSP) settings

The OCSP Settings table lists the OCSP settings in the SMS. OCSP gets the revocation status of a certificate. You can specify one OCSP setting per CA certificate.

The following table describes the fields in the OCSP Settings table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate Authority</td>
<td>The name of the CA certificate using the specified OCSP setting.</td>
</tr>
<tr>
<td>OCSP URI</td>
<td>The URI to the OCSP with revocation information.</td>
</tr>
</tbody>
</table>

Specify an OCSP setting

You can specify an OCSP URI that overrides the OCSP URI defined in the CA certificate.

**Note:** Specifying, editing, and deleting an OCSP setting require the **Admin X509 Certificate Management** capability in your user role.

1. Go to **Admin > Certificate Management > Revocation**.
2. Click **New** under OCSP Settings.
3. Choose a Certificate Authority.
4. Specify an OCSP URI for the chosen CA certificate.
Viewing Certificate Revocation Lists (CRLs)

The Certificate Revocation Lists table lists the configured CRLs in the SMS. A CRL contains a list of revoked certificates. You can configure one CRL location per CA certificate.

The following table describes the fields in the Certificate Revocation Lists table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate Authority</td>
<td>The name of the CA certificate with the configured CRL.</td>
</tr>
<tr>
<td>Source</td>
<td>The file location or the URL of the CRL.</td>
</tr>
<tr>
<td>Entries</td>
<td>The number of the certificates revoked by the CRL.</td>
</tr>
<tr>
<td>Status</td>
<td>The state of the CRL.</td>
</tr>
<tr>
<td>Published</td>
<td>The date and time of the publication of the CRL.</td>
</tr>
<tr>
<td>Next Publish</td>
<td>The date and time of when the CRL will publish next.</td>
</tr>
<tr>
<td>Last Update</td>
<td>The date and time of when the CRL updated on the SMS.</td>
</tr>
</tbody>
</table>

Configure a CRL location

You can specify a CRL location that overrides the CRL location defined in the CA certificate.

**Note:** Configuring, editing, and deleting a CRL requires the *Admin X509 Certificate Management* capability in your user role.

1. Go to **Admin > Certificate Management > Revocation**.
2. Click **New** under Certificate Revocation Lists.
3. Choose a Certificate Authority.
4. Specify a Distribution Point URL or browse to and open a Local CRL File.
5. Click **OK**.
Viewing signing requests

The Signing Requests table lists the Certificate Signing Requests (CSRs) in the SMS. A CSR contains information that identifies the requestor.

To request a signed certificate with a CSR and use it in the SMS,

1. *Create a CSR* on page 578.
2. *Export a CSR* on page 579
3. Send the exported CSR to a CA. The CA signs the CSR and sends back a certificate.
4. *Import the certificate* on page 579.

The following table describes the fields in the Signing Requests table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the certificate request.</td>
</tr>
<tr>
<td>Common Name (CN)</td>
<td>The CN stored in the CSR.</td>
</tr>
<tr>
<td>Requestor</td>
<td>The RFC822 name stored in the CSR.</td>
</tr>
<tr>
<td>Signing Certificate</td>
<td>One of the following:</td>
</tr>
<tr>
<td></td>
<td>• Check mark – The CSR has the key certificate sign bit set in the key usage extension. The &quot;Make it a signing certificate&quot; box is checked in the request.</td>
</tr>
<tr>
<td></td>
<td>• Empty circle – The CSR does not have the key certificate sign bit set in the key usage extension. The &quot;Make it a signing certificate&quot; box is unchecked in the request.</td>
</tr>
<tr>
<td>Key Size (bits)</td>
<td>The number of bits used to create the private key.</td>
</tr>
</tbody>
</table>
Create a new signing request

You can create a new CSR, public key, and private key in the New Signing Request dialogue.

**Note:** Creating and deleting a signing request require the *Admin X509 Certificate Management* capability in your user role and the SMS certificate password.

1. Go to **Admin > Certificate Management > Signing Requests**.
2. Click **New**.
3. Fill out the General section to specify CSR information used in the SMS and to create the private key.
   a. Provide a unique request name for the CSR to be stored in the SMS.  
      **The request name is not stored in the generated CSR.**
   b. Select a key size.
      **We recommend 2048 bits or greater.**
   c. Check or uncheck "Make it a Signing Certificate".
      **A signing certificate sets the key certificate sign bit in the key usage extension and sets the basic constraints extension to true.**
4. Fill out the Subject Distinguished Name section to define the subject of the certificate to be generated for the CSR.
   a. (Optional) Provide a valid email address for the subject.
   b. Provide a fully qualified domain name or the IP address of the owner for the certificate as the CN.
   c. (Optional) Provide the organization unit or the department name of the certificate's subject DN.
   d. (Optional) Provide the organization name of the certificate's subject DN.
   e. (Optional) Provide the locality or the city of the certificate's subject DN.
   f. (Optional) Provide the state of the certificate's subject DN.
   g. (Optional) Provide the two-letter ISO code for the country of the certificate's subject DN.
5. Fill out the Subject Alternative Name section to add a DNS and RFC822 name to the subject alternative name extension in the CSR.
   a. (Optional) Provide a domain name for the subject alternative name.
   b. (Optional) Provide a user name of the owner as an email address.
6. Click **OK**.

The CSR fields are saved to the SMS database. A public and private key pair is generated. A certificate is generated from the data and is used to create the actual CSR to be saved in the SMS database.
Export a signing request

CSRs can be written to a .pem file to be sent to a CA to generate a certificate.

**Note:** Exporting a signing request require the *Admin X509 Certificate Management* capability in your user role and the SMS certificate password.

1. Go to **Admin > Certificate Management > Signing Requests**.
2. Select a signing request and click **Export**.
3. Specify the file location and provide a unique name.
4. Click **OK**.

Import the certificate

You can import the CA-signed certificate that is generated from a CSR into the SMS. For more information, see *Import a certificate* on page 570.

When you import the certificate, the SMS retrieves the private key associated with that CSR and places it in the imported certificate. You may delete the corresponding CSR after the import.

Database

Administration of the SMS database includes viewing database statistics and managing data retention policies, configuring external access and replication of the database, and backing up and restoring the database.

In the Admin workspace, select Database in the navigation pane to display database-related information and to perform tasks on the database.

Working with the Admin (Database) screen

The Database screen in the Admin workspace displays database statistics and enables you to manage data retention policies, perform cleanup of selected database entries, and configure external database settings.

Database maintenance

The SMS database cleanup processes leverage the retention policies. The database needs to be managed to ensure its size does not exceed a desired maximum. By removing old data and limiting the amount of data stored for a particular data type, the database size can be constrained.

The SMS performs automatic cleanup procedures based on the values specified in the maintenance settings of the retention policies, that is, the age of the data and maximum rows allowed. The cleanup process removes rows that are older than the Age setting and also decreases the number of stored rows so as not to exceed MaxRows. This cleanup process is automatically performed at least one time within a 24-hour period. You have the ability to initiate an immediate clean up and to edit the retention values.
The Database Maintenance area displays the following information.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data</td>
<td>Name of the database data.</td>
</tr>
<tr>
<td>Rows</td>
<td>Current number of rows of data in the database.</td>
</tr>
<tr>
<td>Max Rows</td>
<td>Maximum number of rows for the data in the database. The system clears records at the end of the list to make room for the newest entries, always keeping the number of total records equal to or less than this value. You can edit this value.</td>
</tr>
<tr>
<td>Age</td>
<td>Number of days to keep data before clearing it. The system clears data older than this setting. You can edit this setting.</td>
</tr>
<tr>
<td>Status</td>
<td>Cleanup status.</td>
</tr>
<tr>
<td>Last Cleanup</td>
<td>Last time the entries were cleaned. Cleanup occurs daily. You can also initiate an immediate cleanup by clicking <strong>Cleanup Now</strong>.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Events</td>
<td>Filter hits retrieved from managed devices.</td>
</tr>
<tr>
<td>Audit Log</td>
<td>Audit log records for the SMS.</td>
</tr>
<tr>
<td>Malware DV</td>
<td>Auxiliary DV (Threat DV) filter package for the SMS.</td>
</tr>
<tr>
<td>Device Audit Log</td>
<td>Audit log records for managed devices.</td>
</tr>
<tr>
<td>Device Monitoring Data</td>
<td>Monitoring statistics for managed devices.</td>
</tr>
<tr>
<td>Column</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>---------------------------------------------------------------</td>
</tr>
<tr>
<td>Device System Log</td>
<td>System log records for managed devices.</td>
</tr>
<tr>
<td>Device Traffic Data</td>
<td>Traffic statistics for managed devices.</td>
</tr>
<tr>
<td>DV</td>
<td>Digital Vaccine for the SMS.</td>
</tr>
<tr>
<td>Firewall Block</td>
<td>X-series firewall block logs.</td>
</tr>
<tr>
<td>Firewall Traffic</td>
<td>X-series firewall traffic statistics.</td>
</tr>
<tr>
<td>Historical Events</td>
<td>Filter hit-based data for SMS reporting.</td>
</tr>
<tr>
<td>Historical DDOS Stats</td>
<td>Device DDOS statistics for SMS reporting.</td>
</tr>
<tr>
<td>Historical IP User Mapping</td>
<td>IP user mapping data for SMS reporting.</td>
</tr>
<tr>
<td>Historical Port Traffic Stats</td>
<td>Device port traffic statistics for SMS reporting.</td>
</tr>
<tr>
<td>Historical Rate Limit Stats</td>
<td>Device rate limit statistics for SMS reporting.</td>
</tr>
<tr>
<td>Network Mapping</td>
<td>Network mapping and IP correlation data for Responder.</td>
</tr>
<tr>
<td>IP Address Lookup Results</td>
<td>IP addresses and IP address groups for event IP address lookup.</td>
</tr>
<tr>
<td>IP User Mapping</td>
<td>IP user and group mapping.</td>
</tr>
<tr>
<td>Next Generation Firewall</td>
<td>Profile information for managed NGFW appliances.</td>
</tr>
<tr>
<td>Profile Snapshots</td>
<td></td>
</tr>
<tr>
<td>Next Generation Firewall Events</td>
<td>Firewall event data from managed NGFW appliances.</td>
</tr>
<tr>
<td>Column</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>Device SSL Log</td>
<td>SSL inspection log for managed devices.</td>
</tr>
<tr>
<td>Next Generation VPN Log</td>
<td>VPN logs from managed NGFW appliances.</td>
</tr>
<tr>
<td>Notifications</td>
<td>Latest SMS and managed device log notifications.</td>
</tr>
<tr>
<td>Profile Change History</td>
<td>Inspection profile version history.</td>
</tr>
<tr>
<td>Response History</td>
<td>Response History events for Responder.</td>
</tr>
<tr>
<td>sFlow®</td>
<td>sFlow® statistics from managed devices.</td>
</tr>
<tr>
<td>SMS Monitoring Data</td>
<td>SMS-specific monitoring data.</td>
</tr>
<tr>
<td>Events HTTP Context</td>
<td>URI metadata (i.e., hostname, URI, and Method) from managed devices.</td>
</tr>
<tr>
<td>User ID IP Correlation</td>
<td>User log in and group information from the Identity Agent.</td>
</tr>
<tr>
<td>VPN</td>
<td>X-series VPN logs.</td>
</tr>
<tr>
<td>Segment Traffic Stats</td>
<td>Segment traffic statistics from managed devices.</td>
</tr>
</tbody>
</table>

**Edit data retention settings**

1. On the Admin (Database) screen, select the data row for the retention settings you want to edit, and then click **Edit**.

2. Enter a value for the maximum permitted age of data in the **Clear data older than** field.
   
   Data older than the entered value is removed from the database during the cleanup process.

3. Enter a value for the maximum number of permitted rows in the **Clear records exceeding the newest** field.
   
   The database cleanup process removes records at the end of the list to make room for the newest entries, always keeping the number of total records equal to or less than this value.

4. Click **OK**.
Reset data statistics

1. On the Admin (Database) screen, select the data row for the retention settings you want to reset, and then click **Reset**.
2. Click **Yes** to confirm that you want to delete all data from the selected database table.

Initiate an immediate cleanup of data statistics

1. On the Admin (Database) screen, select the data row for the retention settings you want to reset, and then click **Cleanup Now**.
2. Click **Yes** to confirm you want to continue.

Depending on settings, the system removes or archives all entries older than the **Age** setting and more than the set **Max Rows**.

External database settings

The External Database Settings panel at the bottom of the screen enables you to configure settings for external access to the SMS database and for database replication. If you enable external database access, an external system can perform a number of read-only tasks such as reading the SMS database, generating additional custom reports, and replicating the database.

The SMS does not allow modifications to the database through external connections. External systems are restricted to read-only access to the SMS database. You can secure external access by granting access to a specific list of IP addresses.

**Note:** Enabling external access and enabling database replication to an external system both require a reboot of the SMS Server. Follow your company’s server downtime policies, including notification to SMS clients of the pending reboot.

The External Database Settings panel indicates whether the following services are enabled or disabled:

- **External Database Access** – Allows read-only access to the SMS database. A typical use of this service is to allow an external reporting tool to generate custom reports. You must reboot the SMS to enable or disable this service. When enabled, the database name to connect to is **ExternalAccess**.

- **External Database Replication** – Allows an external database server to replicate reporting data from the SMS. You must reboot the SMS to enable or disable this service.

- **Access Restrictions** – Restricts external access to a specified list of IP addresses. You select these addresses from a list of user-defined Named Resources.

In addition, the External Database Settings panel displays a link to the Exports and Archives page in the Admin workspace. This is the target location for SMS-created files, including snapshots and SMS exports and archives.

For more information on the external database, see the **SMS External Interfaces Guide**.
Configure the SMS for external access

This service opens a MariaDB read-only database for any third-party access or reporting tool. The read-only database name is **ExternalAccess**.

**Note:** Running complex report against SMS server may slow down the SMS response time significantly.

1. In the SMS, go to **Admin > Database**.
2. On the External Database Settings panel, click **Edit**.
3. In the Edit External Database Settings wizard, select **External Access Settings**.
4. Select **Enable external database access** to enable the service. (To disable the service, clear the check box.)
5. Provide the following:
   - **Username** – Provide the user name for an account with sufficient rights to read all the desired data from the SMS database.
   - **Password** – Provide the password for the user account. Retype the password in the Confirm Password field.
6. If you changed the external access settings, click **Reboot** to restart the SMS server and initialize the service.
   **Note:** Follow your company’s server downtime policies, including notification to SMS clients of a pending reboot. Before you reboot the SMS, gracefully stop other client connections to the server.
7. Click **OK**.

   If you verification fails or you encounter issues, check the following items:
   - Make sure that the username and password on the database are the same as the ones you set up on the SMS client.
   - Make sure to reboot the SMS before you try to access the database.

Configure the SMS for replication

This service allows an external database server to replicate data from the SMS. Using an external database for data replication allows you to offload report processing to an external server which can provide performance gains to your existing system. Reboot the SMS to completely enable or disable this service.

Before you begin, make sure that your replication system has sufficient disk space to accommodate the database and any increase in size due to additional data or reporting.

1. In the SMS, go to **Admin > Database**.
2. On the External Database Settings panel, click **Edit**.
3. In the Edit External Database Settings wizard, select **External Replication Settings**.
Note: To configure external database replication, you must create an SMS database snapshot, and then copy the snapshot to the target replication system and import it into a MariaDB database before the SMS server can replicate its data to the target system.

4. Select **Enable external database replication** to enable the service. (To disable the service, clear the check box.)

5. Provide the following:
   - **Username** – Provide the user name for an account with sufficient rights to read all the desired data from the SMS database.
   - **Password** – Provide the password for the user account. Retype the password in the Confirm Password field.

6. If you changed the replication settings, click **Reboot** to restart the SMS server and initialize the service.

   **Note:** Follow your company’s server downtime policies, including notification to SMS clients of a pending reboot. Before you reboot the SMS, gracefully stop other client connections to the server.

7. Click **Create Snapshot**, and select **Include Events in Snapshot** if you want the snapshot to include event data.

   **Note:** The snapshot is saved locally on the SMS server. You must copy the snapshot to the target replication system and import it into a new or existing MariaDB database before the SMS server can replicate its data to the target system.

8. Click **OK**.

   **Note:** External database replication and the SMS High Availability (HA) features both leverage the same functionality in the underlying MariaDB database. The SMS database does not support replication to multiple destinations; therefore, we do not recommend using SMS HA and external database replication at the same time.

Configure the SMS to enable restricted access

This service allows access to the external database to be restricted to a set of IP addresses.

1. In the SMS, go to **Admin > Database**.
2. On the External Database Settings panel, click **Edit**.
3. In the Edit External Database Settings wizard, select **Access Restrictions**.
4. Select **Enable restricted access** to enable the service. (To disable the service, clear the check box.)
5. Provide the following:
   - **Named IP Address Group** – To restrict a set of IP addresses, click the arrow, and either select a Named IP Address Group or create a new one.
6. Click **OK**.
Backup and restore

The SMS server maintains important data in both its database and its configuration files. The database contains data from current and historical events and operations as well as devices the SMS manages. Configuration files contain such data as SMTP server, NAT configuration, and user data. This data is critical to the operation of the SMS Server; you should back up the data periodically to assist in recovery from any unexpected failures.

Backup

The backup process backs up both the database and the configuration files. By default, event-related and statistics-related database tables are not backed up due to their size, but you can choose to include these tables as well as other, optional configuration files.

**Note:** You should include event data when you backup your SMS prior to migrating to a new version.

Backing up the SMS database is a resource-intensive process, particularly if the server is under heavy load conditions and the database is large. Take this into consideration when scheduling a regular backup or initiating an immediate backup.

**Backup the SMS database**

1. In the Admin navigation pane, expand **Database** and select **Backup**.
2. Do one of the following:
   - Click **New** on the Scheduled Backups panel to schedule a one-time or recurring backup.
   - Click **Backup Now** on the Backup and Restore panel to initiate an immediate backup.
3. For an immediate backup, skip to the next step. For a one-time or recurring backup, provide a **Schedule Name** and select the recurrence options for your scheduled backup, and then click **Next**.
4. Configure your backup from the available options.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Include... most recent Digital Vaccine(s)</td>
<td>Select the number (1–6) of Digital Vaccines to include in the backup. The most recent Digital Vaccine is always included in a backup.</td>
</tr>
<tr>
<td>Include... most recent Device TOS packages</td>
<td>Select up to the six most recent Device TOS packages to include in the backup.</td>
</tr>
<tr>
<td>Setting</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Include... most recent Custom packages</td>
<td>Select up to the six most recent custom packages to include in the backup. The active DV Toolkit (if you have one) is always included in a backup.</td>
</tr>
<tr>
<td>Include contents of events table</td>
<td>Select this option to include data from the Events table in the backup.</td>
</tr>
<tr>
<td>Email the backup results</td>
<td>Select this option to send a copy of the backup results to members of the SMS notification list. The System Notification List is defined in the Server Properties. See <em>Server properties</em> on page 590.</td>
</tr>
<tr>
<td>Use timestamp as suffix of the backup file name</td>
<td>Select this option to append the current timestamp to the end of the backup filename.</td>
</tr>
<tr>
<td>Encrypt backup</td>
<td>Select this option to encrypt the backup file. If you select this option, you must provide an encryption password. Note that this password is not recoverable. You cannot restore the contents of an encrypted backup without this password.</td>
</tr>
</tbody>
</table>

5. Click **Next**.

6. Select the protocol the backup process is to use, and then click **Next**.

   **Note:** If you choose **HTTP(S)**, the backup file is placed on the SMS server. Best practices imply that you move the file to other storage media. To do this, use a Web browser to connect to the SMS server and copy the file. (The backup location is provided in the backup configuration summary.)

   If you choose **NFS**, ensure the NFS share grants the SMS Server write permissions for the anonymous user.

7. If prompted, provide the appropriate access information, and click **Next**.

   Depending on the protocol you select, access information might include one or more of the following:

   - **Location** path, including hostname, directory structure, and backup file name.
   - **Username** and **Password** for account with sufficient access to write to the identified storage location.
   - **Domain** in which the storage location resides.
   - **Username** and **Password** for account with sufficient access to write to the identified storage location.
8. On the Summary screen, verify your backup configuration and then click Finish.

The backup procedure validates access to the storage location and then proceeds to back up the data. Backup time varies according to amount of data, server performance, and the performance of the storage location/device.

**Note:** An SMS backup includes the web certificate (and its private key in encrypted form) configured for the system. If the SMS is configured to use a custom web certificate, and a backup (that was created before the custom web certificate was imported) is restored, the custom web certificate will be overwritten with the original web certificate (and its private key) from the backup. If this happens, you will need to re-import the custom web certificate. To secure the private key, you can encrypt the backup.

**Note:** If the backup version does not match the current SMS version, the vulnerability scan (eVR) converters are not restored. The vulnerability scan (eVR) converters are only restored during a backup if the backup version and the current version of the SMS are the same.

**Edit a scheduled backup**

1. On the Backup and Restore screen, select a scheduled backup in the list, and click Edit.
2. In the SMS Backup wizard, edit the backup options as needed.
3. Click Finish to save your changes.

**Delete a scheduled backup**

1. On the Backup and Restore screen, select a scheduled backup in the list, and click Delete.
2. In the Delete Confirmation dialog, click Yes.

**Restore**

The restore process restores the SMS database and configuration files from a backup file. Before restoring the database, the SMS validates the integrity of the backup file. If the file is invalid, the SMS console displays an error message. To ensure database integrity, the system automatically reboots after the restore operation.

The SMS supports restoring a backup taken from a previous version of SMS. For example, you can restore a backup taken with SMS 3.5 and restore it to an SMS 3.6 server. When you restore a backup file from a previous version, the database is not only restored, but the data is migrated and data structures conform to the version of SMS running on your SMS server.

**Note:** If you restore a backup to an SMS server on which SMS patches are installed, you might need to rollback and reapply an SMS patch. In this case, the restoration process displays a dialog that indicates if you need to perform this task.

Backup and restore processes require access to storage, either to back up data to storage or restore data from storage. The SMS backup and restore processes can perform their tasks using any of the following storage access protocols:

- Network File System (NFS) Protocol — Does not require local storage on the SMS.
• Server Message Block (SMB) Protocol — Microsoft-based shared-access file system. Does not require local storage on the SMS.

• Secure File Transfer Protocol (sFTP) — Does not require local storage on the SMS.

• Secure Copy Protocol (SCP) — Requires temporary local storage on the SMS.

• Hypertext Transfer Protocol (HTTP) and Secure Hypertext Transfer Protocol (HTTPS) — Data is stored locally on the SMS.

**Note:** The use of HTTP or HTTPS requires that the service be enabled on the SMS server. See *Services* on page 593.

During backup and restore processes, the SMS server performs the following tasks:

• Mount the storage destination, referred to in the SMS product as the location.

• Stop the SMS server database and SMS server application.

• Back up or restore the database files to/from the specified storage location.

• Unmount the storage destination.

• Restart the SMS server database and SMS Server application. If it is a restore operation the SMS server is restarted and rebooted, which stops client connections to the SMS server.

Some of the supported storage access protocols allow IPv6 addressing. When you specify a backup location in the SMS backup wizard with an IPv6 address, be sure to follow the following syntax requirements:

• **NFS** — Does NOT support IPv6

• **SMB** — IPv6 address MUST be surrounded by brackets

• **SCP** — IPv6 address with or without brackets

• **sFTP** — IPv6 address with or without brackets

If the restored SMS is a different platform or version than the SMS from which you backed up then the following configurations will not be restored and will remain unchanged:

• **Admin Server Properties** (Admin > Server Properties)
  - Management: System Information and Services
  - Network: Network Interface, Date/Time, and DNS

• **Auto DV Activation** (Profiles > Digital Vaccines > DV Inventory > Auto DV Activation)
  - Automatic Download
  - Automatic Activation
  - Automatic Distribution
**Restore the SMS database**

Before you initiate the restore process, ensure there are no active client connections to the SMS server through the SMS client, command line interface, or Web browser.

For information about how you can restore the SMS database with a stack of devices, see *SMS database restore to a different SMS* on page 531.

1. On the Backup and Restore screen, click **Restore**.
2. In the SMS Restore wizard, select the backup file you want to restore, and click **OK**.
3. Click **Import**.

   The **SMS Restore** wizard verifies the integrity of the chosen file and proceeds if the file is valid. If the file is invalid, the SMS displays an error message.

4. A summary page appears. If the information is correct, click **Finish**.

   Database restoration begins, with the restored data overwriting the existing data. When complete, the SMS Server reboots to finalize the restore process and ensure data integrity of the restored database.

**Server properties**

During installation and initial setup, basic settings for the SMS server are configured. The SMS Server Properties enables you to edit these settings and to configure additional options and services.

Use the Server Properties screen to change system and network information, enable services, configure syslog, and enable NAT, SNMP, and TLS protocols.

In the Admin workspace, select **Server Properties** in the navigation pane to display the Admin (Server Properties) screen.

**Note:** You can also use the SMS Command Line Interface (CLI) to configure many of the server properties discussed in this topic.

**Configuring management properties**

The Management Properties tab enables you to view and update system information, enable or disable FIPS mode, and select which services to enable.

**Note:** Only users with SuperUser privileges can modify SMS server properties.

**System information**

The System Information panel displays the following SMS system information. In the table below, an asterisk (*) indicates a read-only field.
<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Hostname of the SMS. The name should easily and uniquely identify each SMS system.</td>
</tr>
<tr>
<td>Contact</td>
<td>Name or email address of the system administrator responsible for the server.</td>
</tr>
<tr>
<td>Location</td>
<td>Location of the server or the administrator.</td>
</tr>
<tr>
<td>Serial Number*</td>
<td>Serial number of the server.</td>
</tr>
<tr>
<td>Management Port Speed*</td>
<td>Port speed.</td>
</tr>
<tr>
<td>Management Port Duplex*</td>
<td>Port duplex setting (full or half).</td>
</tr>
<tr>
<td>Management Port Negotiation</td>
<td>Option to enable auto negotiation for the management port.</td>
</tr>
</tbody>
</table>

* On the System Information panel, you can update the Name, Contact, and Location fields, and you can enable or disable Management Port Negotiation.

Update system information

1. On the Admin (Server Properties) screen, select the Management tab.
2. Enter new values directly into the text boxes for any of the three editable fields (Name, Contact, and Location).
3. Select or clear Management Port Negotiation to enable or disable automatic negotiation on the management port.
4. Click Apply to save your changes.

FIPS mode

The Federal Information Processing Standard (FIPS) Publication 140-2 is a U.S. government computer security standard used to accredit cryptographic modules. The FIPS 140-2 publication coordinates requirements and standards for cryptography modules that include both hardware and software...
components. Some United States federal agencies and departments require software, including the SMS, to comply with the 140-2 standards.

The SMS supports two levels of FIPS operation:

- **Disabled** — No FIPS compliance actions or restrictions are activated on the SMS server.

- **FIPS Crypto Core** — In this mode the SMS uses cryptographic libraries certified by the National Institute of Standards and Technology to be compliant with FIPS 140-2 publication. The SMS automatically reboots when placed into FIPS Crypto Core mode or when FIPS Crypto Core mode is disabled.

The FIPS Mode panel allows you to enable FIPS mode and request a particular state or level of operation.

**Note:** If the SMS is currently running a 1K key, it will display a message about upgrading to a 2K key to be fully FIPS compliant. You can still enable FIPS mode on the SMS without installing the 2K key, but when the SMS is in FIPS mode, you cannot install the 2K key.

**Enable or disable FIPS Crypto Core mode**

Only the cryptographic libraries used by SMS version 4.2.1 and later are FIPS 140-2 certified. Because of this, FIPS mode in SMS version 4.2.1 and later is called **FIPS Crypto Core**.

1. On the Admin (Server Properties) screen, select the **Management** tab.
2. On the FIPS Mode panel, click **Edit**.
3. Review the current state. The current state radio button indicates if the SMS is in FIPS Crypto Core mode. If it is not, the radio button is unselected and the current state displays as Disabled.
   a. If the current state is Disabled, select the **FIPS Crypto Core** radio button to enter FIPS Crypto Core mode.
   b. If the current state is FIPS Crypto Core, select the **Disabled** radio button to turn that mode off.
4. Click **OK**.

When you submit the request to enter FIPS Crypto Core mode, the SMS server reboots and begins a process that deactivates Telnet and HTTP services, if they are active.

**Note:** This process, along with the reboot, also occurs when transitioning out of FIPS Crypto Core mode.

When this process is complete, the SMS operates in FIPS Crypto Core mode. The following restrictions apply in this mode:

- Upgrading the SMS certificate key will not be allowed. For more information, see *SMS certificate key* on page 537.

- SMS will not be able to communicate with the Identity Agent. For more information, see *User ID IP Correlation* on page 648.

- SMS High Availability (HA) will not be available.
○ The SSH terminal will negotiate connections using only FIPS 140-2 approved algorithms.
○ Custom Responder Actions cannot be imported or executed.
○ To get logs from a managed SSL device, you must first set up SMS as the syslog destination in the SSL web client.
○ Telnet and HTTP services will not be available.

**Services**

The Services panel allows you to enable and disable services that are running on the SMS server. Services listed on the panel are used to communicate with the SMS server. Not all services are secure; be sure to carefully consider which services you enable. HTTP and Telnet are not secure services.

The services, along with a brief description of each, are shown in the following table.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSH</td>
<td>Secure communication connection used for CLI. Requires Super User access. SSH is enabled by default. When enabled, you can set the login grace time. The grace time is the amount of time a user has to enter a password and establish a connection. The SMS disconnects after this time if the user has not successfully logged in. The default is 60 seconds, but you can set the time from 30 to 600 seconds. A limit of three invalid SSH connection attempts can now be configured. When set at 3, the SSH disconnects after three unsuccessful attempts.</td>
</tr>
<tr>
<td>HTTPS</td>
<td>Secure network communication for Web pages. Enabling HTTPS enables Web services for the SMS. HTTPS is enabled by default. See <em>TippingPoint SMS Web Services API</em>.</td>
</tr>
<tr>
<td>HTTP</td>
<td>Unsecure network communication connection for Web pages. Enabling HTTP enables Web services for the SMS. See <em>TippingPoint SMS Web Services API</em>.</td>
</tr>
<tr>
<td>Telnet</td>
<td>Unsecure network communication connection used for CLI. Requires Super User access.</td>
</tr>
<tr>
<td>Ping</td>
<td>Allows the SMS to respond to an ICMP request. Ping is enabled by default.</td>
</tr>
</tbody>
</table>

**Enable or disable the SMS services**

1. On the Admin (Server Properties) screen, select the **Management** tab.
2. On the Services panel, do one of the following:
• Select Enable next to a service to enable it.
• Clear the check box next to a service to disable it.

3. Click Apply.

Note: By default, HTTP and telnet are not enabled. Enabling these services opens unsecure network communications on the SMS server.

Configuring network properties

The Network Properties tab enables you to view and update network interface details, SMS date and time, SMTP server settings, TMC proxy connections and DNS server addresses.

Note: When you make changes to properties shown in the Network screen, for example enabling NTP or identifying a DNS server, you must click Apply in the lower right of the display to save the changes.

Network interface

The Network Interface panel displays the following network information. In the table below, an asterisk (*) indicates a read-only field.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet MAC ID*</td>
<td>Unique identifier assigned by the manufacturer to network interface cards (NICs) capable of supporting the IPv4 standard.</td>
</tr>
<tr>
<td>Scope Link Address*</td>
<td>Unique identifier assigned by the manufacturer to network interface cards (NICs) capable of supporting the IPv6 standard.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Internet protocol (IP) address of the SMS server used for management communication.</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>Subnet mask of the IP address.</td>
</tr>
<tr>
<td>Gateway</td>
<td>Network gateway through which SMS Server traffic flows.</td>
</tr>
<tr>
<td>IPv6 Address</td>
<td>IP version 6 address of the SMS Server.</td>
</tr>
<tr>
<td>Default Router</td>
<td>IP address of the default router through which SMS Server traffic is routed to/from the network.</td>
</tr>
</tbody>
</table>
Update network interface information

1. On the Admin (Server Properties) screen, select the **Network** tab.
2. On the Network Interface panel, update the following information as needed:
   - IP address
   - IPv6 address
   - Subnet mask
   - Default router
   - Gateway
3. Click **Apply**.

   **Note:** If you change the management IP address, you must reboot the SMS server. Go to (Admin > General > SMS Server), and then click **Reboot**.

**Date/Time**

The Date/Time panel allows you to configure how the SMS Server obtains its date and time. You can configure the SMS Server to obtain its date and time from a network-based network time protocol (NTP) server or you can set the date and time manually.

To keep date and time consistent between the SMS Server and the devices it manages, consider configuring your SMS Server as an NTP Server, and configure the managed devices to obtain their date and time from the SMS Server. You can then configure the SMS Server to obtain its time from another NTP Server.

**Caution:** Do not set the time backwards on the SMS server as it might cause inconsistencies in system services that depend tightly on time.

**Note:** The SMS will restart if the time zone is changed, or if the time change is greater than 1 minute.

Enable Network Time Protocol

1. On the Date/Time panel, select **Enable Time Protocol (NTP)**.
2. Provide the IP address or hostname of one or more NTP servers in the appropriate fields.
   
   **Note:** If Enable Time Protocol (NTP) is selected, you must identify at least one NTP Server.
3. Click the **Time Zone** drop-down list, and select the correct time zone in which the SMS server operates.
4. Click **Apply**.

Enable SMS Network Time Protocol authentication settings

You can only enable Network Time Protocol (NTP) authentication settings for the SMS from the SMS CLI. For details, see "ntp-auth" in the **CLI Reference**.
Manually set the time and date

1. On the Date/Time panel, clear the **Enable Time Protocol (NTP)** check box.
2. Click the calendar icon next to the Date/Time field.
3. Use the controls in the pop-up window to select the month, year, day, and time, and then click **OK**.
4. Click the **Time Zone** drop-down list, and select the correct time zone in which the SMS server operates.
5. Click **Apply**.

**SMTP server**

The SMTP Server panel enables you to identify a Simple Mail Transfer Protocol (SMTP) server through which the SMS can send email messages, typically generated when critical operational states trigger email communications with system and network administrators.

The SMS sends email messages for specific events, including the following:

- SMS HA fail-over and activation
- SMS start and stop
- Critical device failures (device can no longer communicate)
- Critical or Error entries in the device syslog
- Database backup
- SMS migrate
- Auto DV down load and activation
- Auto DV distribution including both success and failures
- Reports can be configured for scheduled runs where an email is sent

**Edit SMTP server settings**

1. Click **Edit** on the SMTP Server panel.
2. In the Edit SMTP Server Settings dialog, provide the following information:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Address</td>
<td>IP address or hostname of the SMTP mail server through which the SMS can send email messages.</td>
</tr>
<tr>
<td>SMTP Port</td>
<td>Port on the mail server that listens for SMTP requests; this is typically port 25.</td>
</tr>
</tbody>
</table>
### Setting | Description
--- | ---
Aggregation Period | Amount of time (in seconds) that the SMS aggregates the device email notifications before it sends the notifications in a single email.
If you set the aggregation to zero (default), the SMS will immediately disable the email aggregation.
The maximum number of emails the SMS can collect for a single aggregation period is 10,000. When the SMS reaches this limit, it will discard new device email notifications received.
This setting only applies to device notifications. All other SMS emails are sent immediately.
System Notification List | List of email addresses or email address groups to which the SMS sends email notifications.
From | Email address or address group to appear as the sender for email notifications sent by the SMS.
Reply To | Email address or address group to receive replies to email notifications originally sent by the SMS.

3. If the mail server requires authentication, select **Authentication** and provide the required user name and password.
4. Click **Test**.

   The SMS transmits a test email to the SMTP Server, which should then send the email to the designated recipients. The test verifies whether the SMS can connect to the mail server using the SMTP server settings; it does not verify that the designated recipients receive the email, which is the responsibility of the SMTP server.
5. Click **OK** to save your changes and return to the Network tab.

#### TMC proxy
The TMC Proxy panel allows you to identify a proxy server for communication between the SMS and the TMC website.

Configure a proxy TMC connection
1. On the TMC Proxy panel, select **Proxy TMC Connections**.
2. Provide the IP address or hostname and the port number for the proxy server.
3. If the proxy server requires authentication, select Use Proxy Authentication and provide the user name and password in the appropriate fields.

4. Click Apply.

**Domain Name Service (DNS)**

The Domain Name Service panel allows you to identify DNS servers the SMS can use to locate other servers and to register its own identity. You are not required to identify a DNS server.

**Configure DNS**

1. On the Domain Name Service (DNS) panel, provide the IP address or hostname of up to three DNS servers.
2. Click Apply.

**Configuring NAT properties**

An SMS NAT address enables you to manage a device when the IP address for the SMS network interface is not available to the device because the SMS is behind a network address translation (NAT) boundary or a network address translation protocol translation (NAT-PT) boundary.

Typically, when the SMS discovers a TippingPoint device, the SMS communicates with the device via the IP address of the SMS. When the SMS is behind a NAT boundary, it can provide devices with an alternate IP address that the device can reach. An alternate IP address can be defined as part of a global NAT, per network NAT, or both.

The NAT tab enables you to configure alternate IP addresses that devices can use to communicate with the SMS Server.

**Tip:** For basic NAT configuration, you can choose to use only the global NAT option. When you use the per network NAT option, you may want to configure a global NAT address that can be used if the system is unable to match a device network.

**SMS NAT**

Global NAT is an alternate IP address that is made available across multiple networks that managed devices can use to connect with the SMS. Use the SMS NAT panel to configure a global NAT address.

**Enable SMS global NAT**

1. Click Edit on the SMS NAT panel.
2. In the SMS Global NAT Settings dialog, select Enable Global NAT.
3. In the text field, provide an alternate IP address that devices should use to communicate with the SMS.
4. Click OK.
Disable SMS global NAT

1. Click **Edit** on the SMS NAT panel.
2. In the SMS Global NAT Settings dialog, clear the **Enable Global NAT** check box.
3. Click **OK**.

SMS per network NAT

Per network NAT enables you to specify a list of alternate IP addresses so that managed devices separated from the SMS Server by a NAT layer can connect to the SMS through an address that resides on the same network as each device.

Enable SMS per network NAT

1. Click **Enable** on the SMS Per Network NAT panel.
2. Click **Add**.
3. In the SMS NAT Address dialog, provide an IP address for the device network, along with its prefix length in bits.

   **Note:** The Prefix Length is the number of bits that make up the network portion of the address. The maximum is 32 bits for an IPv4 address and 128 for an IPv6 address.

4. Provide an SMS NAT Address that the device can use to connect to the SMS.
5. Click **OK**.
6. Continue to add NAT addresses for each device network as needed.

Add or edit an SMS per network NAT address

1. On the SMS Per Network NAT panel, do one of the following:
   - Click **Add**.
   - Select an address in the list, and then click **Edit**.
2. Add or edit the information as needed. See **Enable SMS per network NAT** on page 599.
3. Click **OK**.

Delete SMS per network NAT addresses

1. On the SMS Per Network NAT panel, select one or more addresses in the list.
2. Click **Delete**.

   **Note:** There is no confirmation dialog box; be sure you really want to delete the NAT information before you click **Delete**.
Address determination

If Per Network NAT is enabled, the system consults the list of SMS NAT Addresses and chooses the entry whose network matches that of the specified device address. In case of multiple matches, the system chooses the most specific match. If no network address matches, the system consults the Global SMS NAT settings.

If Global SMS NAT is enabled, the system uses the specified Global NAT Address as the SMS IP address.

If the system cannot locate an SMS NAT address or a Global NAT address, it uses the configured IP address of the SMS network interface.

Configuring integration properties

The Integration tab allows you to enable and configure the IDResolver tool, which is a third-party tool that you can use to provide extended protection for your network.

The SMS provides built-in User ID IP correlation through the User Resolver feature.

The SMS also supports the option of using A10 Networks ID management appliances to resolve user IDs.

IDResolver

IDResolver uses an Internet Protocol to Identity service to retrieve user information from an A10 Networks appliance. This service provides information about a user based on a host association entry on the A10 appliance.

Configuring syslog properties

The SMS Server generates and gathers syslog events, which log information about a variety of conditions and operational state changes from monitored devices.

Through the SMS client, you can define a custom message format that is sent to syslog servers, and you can configure the SMS to send a copy of events to a remote syslog server.

In the Admin workspace, click Server Properties in the navigation pane, and select the Syslog tab to display the Admin (Server Properties) screen.

Syslog format options

This section provides information about the default syslog formats that you can use to for SMS message logging. For a description of the syslog format and example output logs, refer to the following topics:

- SMS system syslog on page 601
- SMS audit syslog on page 601
- Device system syslog on page 602
- Device audit syslog on page 603
The SMS supports Device audit syslog on page 603 and Device system syslog on page 602 for logging data from managed devices, and supports Snort syslog for MARS [Deprecated] on page 603 and Snort syslog for V2 [Deprecated] on page 604 for sending Snort syslog events.

SMS system syslog

<table>
<thead>
<tr>
<th>Column</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Severity — 2 is Info, 3 is Warning, 4 is Error, 5 is Critical</td>
</tr>
<tr>
<td>1</td>
<td>Message</td>
</tr>
<tr>
<td>2</td>
<td>Event timestamp in milliseconds</td>
</tr>
</tbody>
</table>

Event sample data

The following is a log message for one event, as it would appear on the syslog:

2<tab>Auto refresh of TMC package versions at 30-minute interval.<tab>1169158607773

The default settings are TAB for delimiter and Security/Authorization for facility.

SMS audit syslog

<table>
<thead>
<tr>
<th>Column</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>User</td>
</tr>
<tr>
<td>Column</td>
<td>Definition</td>
</tr>
<tr>
<td>--------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td>1</td>
<td>Client address</td>
</tr>
<tr>
<td>2</td>
<td>Client port</td>
</tr>
<tr>
<td>3</td>
<td>Session ID</td>
</tr>
<tr>
<td>4</td>
<td>Status</td>
</tr>
<tr>
<td>5</td>
<td>Description</td>
</tr>
<tr>
<td>6</td>
<td>Event timestamp in milliseconds</td>
</tr>
</tbody>
</table>

**Event sample data**

The following is a log message for one event, as it would appear on the syslog:

```
labuser	152.67.137.78	-1	2	success	View SMS System Log	1169157145027
```

The default settings are TAB for delimiter and Security/Authorization for facility.

**Device system syslog**

<table>
<thead>
<tr>
<th>Column</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Device name</td>
</tr>
<tr>
<td>1</td>
<td>Severity</td>
</tr>
<tr>
<td>2</td>
<td>Component</td>
</tr>
<tr>
<td>3</td>
<td>Message</td>
</tr>
<tr>
<td>4</td>
<td>Time</td>
</tr>
</tbody>
</table>
**Event sample data**

The following is a log message for one event, as it would appear on the syslog:

```
110-400 INFO UDM Completed UDM Load request (force = 0) 1318265740029
```

**Device audit syslog**

<table>
<thead>
<tr>
<th>Column</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Device name</td>
</tr>
<tr>
<td>1</td>
<td>Access level</td>
</tr>
<tr>
<td>2</td>
<td>Interface</td>
</tr>
<tr>
<td>3</td>
<td>Source IP address</td>
</tr>
<tr>
<td>4</td>
<td>Category</td>
</tr>
<tr>
<td>5</td>
<td>Result</td>
</tr>
<tr>
<td>6</td>
<td>Device user</td>
</tr>
</tbody>
</table>

**Event sample data**

The following is a log message for one event, as it would appear on the syslog:

```
110-400 Super User WEB 239.142.226.15 SMS PASS root00
```

**Snort syslog for MARS [Deprecated]**

<table>
<thead>
<tr>
<th>Column</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Date (timestamp)</td>
</tr>
</tbody>
</table>
### Column | Definition
--- | ---
1 | Device identifier
2 | SID
3 | Filter name
4 | Classification
5 | Priority
6 | Protocol (TCP, UDP, ICMP, and IP)
7 | Source address
8 | → (indicates direction of traffic flow: source → destination)
9 | Destination address

**Event sample data**

The following is a log message for one event, as it would appear on the syslog:


Snort syslog for V2 [Deprecated]

### Column | Definition
--- | ---
0 | Device identifier
1 | SID
### Event sample data

The following is a log message for one event, as it would appear on the syslog:

```
```

### SMS 2.0/2.1 syslog

<table>
<thead>
<tr>
<th>Column</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Syslog category — “&lt;32&gt;” — defined facility and severity</td>
</tr>
<tr>
<td>1</td>
<td>Action type — 7 is Permit, 8 is Block, 9 is P2P</td>
</tr>
<tr>
<td>2</td>
<td>Severity — 0 is Normal, 1 is Low, 2 is Minor, 4 is Critical</td>
</tr>
<tr>
<td>3</td>
<td>Policy UUID — TippingPoint UUID for policy</td>
</tr>
<tr>
<td>Column</td>
<td>Definition</td>
</tr>
<tr>
<td>--------</td>
<td>------------</td>
</tr>
<tr>
<td>4</td>
<td>Signature UUID — TippingPoint UUID for signature</td>
</tr>
<tr>
<td>5</td>
<td>Signature name — user-friendly name for signature and policy</td>
</tr>
<tr>
<td>6</td>
<td>Signature number</td>
</tr>
<tr>
<td>7</td>
<td>Signature protocol — protocol of signature (IP, UDP, TCP, HTTP, etc.)</td>
</tr>
<tr>
<td>8</td>
<td>Source address</td>
</tr>
<tr>
<td>9</td>
<td>Source port</td>
</tr>
<tr>
<td>10</td>
<td>Destination address</td>
</tr>
<tr>
<td>11</td>
<td>Destination port</td>
</tr>
<tr>
<td>12</td>
<td>Hit count — number of attacks during aggregation period</td>
</tr>
<tr>
<td>13</td>
<td>Device slot — this slot can be 3, 5, 7, 8</td>
</tr>
<tr>
<td>14</td>
<td>Device segment — device segment of above slot that got event</td>
</tr>
<tr>
<td>15</td>
<td>Device name — user-friendly name of the device event was received</td>
</tr>
<tr>
<td>16</td>
<td>TippingPoint Taxonomy ID — category ID assigned to the signature</td>
</tr>
<tr>
<td>17</td>
<td>Event timestamp in milliseconds</td>
</tr>
<tr>
<td>18</td>
<td>Additional comments about the event</td>
</tr>
<tr>
<td>19</td>
<td>Sequence number of the event in the SMS</td>
</tr>
</tbody>
</table>
Event sample data

The following is a log message for one event, as it would appear on the syslog:

```
<34><tab>7<tab>4<tab>00000002-0002-0002-0002-000000002557
<tab>00000001-0001-0001-000 1-000000002557<tab>2557:
HTTP: HTTP CONNECT TCP Tunnel to Interactive
ports<tab>2557<tab>http<tab>216.136.56.96
<tab>33584<tab>216.136.56.184<tab>80<tab>2<tab>207-2400-Jack<tab>
100862973<tab>1109870461622<tab>additionalcomment<tab>1
```

The default settings are TAB for delimiter and Security/Authorization for facility.

SMS 2.5 syslog

The SMS supports the following syslog format for logging system events for SMS 2.5 and above.

<table>
<thead>
<tr>
<th>Column</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Syslog category — “&lt;32&gt;” — defined facility, and the severity</td>
</tr>
<tr>
<td>1</td>
<td>Action type — 7 is Permit, 8 is Block, 9 is P2P</td>
</tr>
<tr>
<td>2</td>
<td>Severity — 0 is Normal, 1 is Low, 2 is Minor, 3 is Major, 4 is Critical</td>
</tr>
<tr>
<td>3</td>
<td>Policy UUID — TippingPoint UUID for policy</td>
</tr>
<tr>
<td>4</td>
<td>Signature UUID — TippingPoint UUID for signature</td>
</tr>
<tr>
<td>5</td>
<td>Signature name — user-friendly name for signature and policy</td>
</tr>
<tr>
<td>6</td>
<td>Signature number</td>
</tr>
<tr>
<td>7</td>
<td>Signature protocol — protocol of signature (IP, UDP, TCP, HTTP, etc.)</td>
</tr>
<tr>
<td>8</td>
<td>Source address</td>
</tr>
<tr>
<td>9</td>
<td>Source port</td>
</tr>
<tr>
<td>Column</td>
<td>Definition</td>
</tr>
<tr>
<td>--------</td>
<td>------------</td>
</tr>
<tr>
<td>10</td>
<td>Destination address</td>
</tr>
<tr>
<td>11</td>
<td>Destination port</td>
</tr>
<tr>
<td>12</td>
<td>Hit count</td>
</tr>
<tr>
<td>13</td>
<td>Source zone name</td>
</tr>
<tr>
<td>14</td>
<td>Destination zone name</td>
</tr>
<tr>
<td>15</td>
<td>Incoming physical port</td>
</tr>
<tr>
<td>16</td>
<td>VLAN ID</td>
</tr>
<tr>
<td>17</td>
<td>Device name — user-friendly name of the device event was received</td>
</tr>
<tr>
<td>18</td>
<td>TippingPoint taxonomy ID — category ID assigned to signature</td>
</tr>
<tr>
<td>19</td>
<td>Event timestamp in milliseconds</td>
</tr>
<tr>
<td>20</td>
<td>Additional comments about the event</td>
</tr>
<tr>
<td>21</td>
<td>Sequence number of the event in the SMS</td>
</tr>
</tbody>
</table>

**Event sample data**

The following is a log message for one event, as it would appear on the syslog:

7<tab>2<tab>00000002-0002-0002-0002-00000000005
3<tab>00000001-0001-0001-0001-000000000053<tab>0053:
   IP: Source IP Address Spoofed (IANA Reserved)
   <tab>53<tab>ip<tab>120.254.109.188<tab>80<tab>120.156.183.239<tab>1531<tab>1<tab>1A<tab>1B<tab>1<tab>0<tab>sct231-22<tab>100807421
   <tab>1168641645097<tab>additional comment<tab>1

The default settings are TAB for delimiter and Security/Authorization for facility.
<table>
<thead>
<tr>
<th>Column</th>
<th>CEF key name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>CEF</td>
<td>CEF header (Version</td>
</tr>
<tr>
<td>1</td>
<td>app</td>
<td>Application protocol</td>
</tr>
<tr>
<td>2</td>
<td>cnt</td>
<td>Base event count</td>
</tr>
<tr>
<td>3</td>
<td>dst</td>
<td>Destination address</td>
</tr>
<tr>
<td>4</td>
<td>dpt</td>
<td>Destination port</td>
</tr>
<tr>
<td>5</td>
<td>act</td>
<td>Device action</td>
</tr>
<tr>
<td>6</td>
<td>cn1</td>
<td>Device custom number 1: VLAN tag</td>
</tr>
<tr>
<td>7</td>
<td>cn1Label</td>
<td>Device custom number 1 label</td>
</tr>
<tr>
<td>8</td>
<td>cn2</td>
<td>Device custom Number 2: taxonomy ID</td>
</tr>
<tr>
<td>9</td>
<td>cn2Label</td>
<td>Device custom number 2 label</td>
</tr>
<tr>
<td>10</td>
<td>cn3</td>
<td>Device custom number 3: packet trace</td>
</tr>
<tr>
<td>11</td>
<td>cn3Label</td>
<td>Device custom number 3 label</td>
</tr>
<tr>
<td>12</td>
<td>cs1</td>
<td>Device custom string 1: profile name</td>
</tr>
<tr>
<td>13</td>
<td>cs1Label</td>
<td>Device custom string 1 label</td>
</tr>
<tr>
<td>Column</td>
<td>CEF key name</td>
<td>Definition</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
<td>----------------------------------------------</td>
</tr>
<tr>
<td>14</td>
<td>cs2</td>
<td>Device custom string 2; policy UUID</td>
</tr>
<tr>
<td>15</td>
<td>cs2Label</td>
<td>Device custom string 2 label</td>
</tr>
<tr>
<td>16</td>
<td>cs3</td>
<td>Device custom string 3; signature UUID</td>
</tr>
<tr>
<td>17</td>
<td>cs3Label</td>
<td>Device custom string 3 label</td>
</tr>
<tr>
<td>18</td>
<td>cs4</td>
<td>Device custom string 4; zone names</td>
</tr>
<tr>
<td>19</td>
<td>cs4Label</td>
<td>Device custom string 4 label</td>
</tr>
<tr>
<td>20</td>
<td>cs5</td>
<td>Device custom string 5; device name</td>
</tr>
<tr>
<td>21</td>
<td>cs5Label</td>
<td>Device custom string 5 label</td>
</tr>
<tr>
<td>22</td>
<td>cs6</td>
<td>Device custom String 6; message parameters</td>
</tr>
<tr>
<td>23</td>
<td>cs6Label</td>
<td>Device custom string 6 label</td>
</tr>
<tr>
<td>24</td>
<td>src</td>
<td>Source address</td>
</tr>
<tr>
<td>25</td>
<td>spt</td>
<td>Source port</td>
</tr>
<tr>
<td>26</td>
<td>externalID</td>
<td>External ID (event ID)</td>
</tr>
<tr>
<td>27</td>
<td>rt</td>
<td>Event time</td>
</tr>
<tr>
<td>28</td>
<td>cat</td>
<td>Device event category</td>
</tr>
<tr>
<td>29</td>
<td>proto</td>
<td>Transport protocol</td>
</tr>
<tr>
<td>Column</td>
<td>CEF key name</td>
<td>Definition</td>
</tr>
<tr>
<td>--------</td>
<td>-------------------------</td>
<td>-----------------------------------------------------</td>
</tr>
<tr>
<td>30</td>
<td>deviceInboundInterface</td>
<td>Device inbound interface (physical port in)</td>
</tr>
</tbody>
</table>

**Event sample data**

The following is a log message for one event, as it would appear on the syslog:

```
CEF:0|TippingPoint|UnityOne|1.0.0.17|3702|3702:
HARBOR: Remote Command Execution|VeryHigh|app=TCP cnt=1 dst=74.156.184.90
dpt=4123
act=Block
cn1=0 cn1Label=VLAN ID
cn2=17170251 cn2Label=Taxonomy
cn3=0 cn3Label=Packet Trace
cs1=Default cs1Label=Profile Name
cs2=00000002-0002-0002-0002-000000003702 cs2Label=Policy UUID
cs3=00000001-0001-0001-0001-000000003702 cs3Label=Signature UUID
cs4=1B 1A cs4Label=ZoneNames
cs5=110-400 cs5Label=Device Name
cs6= cs6Label=Filter Message
Parms src=222.188.115.183
spt=48345
externalId=60907
rt=131826810021
cat=Exploits
transportProtocol=TCP
deviceInboundInterface=2
```

**ArcSight CEF Format v4.1 [Deprecated]**

<table>
<thead>
<tr>
<th>Column</th>
<th>CEF key name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>CEF</td>
<td>CEF header (Version</td>
</tr>
<tr>
<td>1</td>
<td>app</td>
<td>Application protocol</td>
</tr>
<tr>
<td>2</td>
<td>cnt</td>
<td>Base event count</td>
</tr>
<tr>
<td>3</td>
<td>dst</td>
<td>Destination IPv4 address</td>
</tr>
<tr>
<td>Column</td>
<td>CEF key name</td>
<td>Definition</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
<td>-------------------------------------</td>
</tr>
<tr>
<td>4</td>
<td>dpt</td>
<td>Destination port</td>
</tr>
<tr>
<td>5</td>
<td>act</td>
<td>Device action</td>
</tr>
<tr>
<td>6</td>
<td>cn1</td>
<td>Device custom number 1: VLAN tag</td>
</tr>
<tr>
<td>7</td>
<td>cn1Label</td>
<td>Device custom number 1 label</td>
</tr>
<tr>
<td>8</td>
<td>cn2</td>
<td>Device custom number 2: taxonomy ID</td>
</tr>
<tr>
<td>9</td>
<td>cn2Label</td>
<td>Device custom number 2 label</td>
</tr>
<tr>
<td>10</td>
<td>cn3</td>
<td>Device custom number 3: packet trace</td>
</tr>
<tr>
<td>11</td>
<td>cn3Label</td>
<td>Device custom number 3 label</td>
</tr>
<tr>
<td>12</td>
<td>cs1</td>
<td>Device custom string 1: profile name</td>
</tr>
<tr>
<td>13</td>
<td>cs1Label</td>
<td>Device custom string 1 label</td>
</tr>
<tr>
<td>14</td>
<td>cs2</td>
<td>Device custom string 2: policy UUID</td>
</tr>
<tr>
<td>15</td>
<td>cs2Label</td>
<td>Device custom string 2 label</td>
</tr>
<tr>
<td>16</td>
<td>cs3</td>
<td>Device custom string 3: signature UUID</td>
</tr>
<tr>
<td>17</td>
<td>cs3Label</td>
<td>Device custom string 3 label</td>
</tr>
<tr>
<td>18</td>
<td>cs4</td>
<td>Device custom string 4: zone names</td>
</tr>
<tr>
<td>19</td>
<td>cs4Label</td>
<td>Device custom string 4 label</td>
</tr>
<tr>
<td>Column</td>
<td>CEF key name</td>
<td>Definition</td>
</tr>
<tr>
<td>--------</td>
<td>----------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>20</td>
<td>cs5</td>
<td>Device custom string 5: device name</td>
</tr>
<tr>
<td>21</td>
<td>cs5Label</td>
<td>Device custom string 5 label</td>
</tr>
<tr>
<td>22</td>
<td>cs6</td>
<td>Device custom string 6: message parameters</td>
</tr>
<tr>
<td>23</td>
<td>cs6Label</td>
<td>Device custom string 6 label</td>
</tr>
<tr>
<td>24</td>
<td>src</td>
<td>Source IPv4 address</td>
</tr>
<tr>
<td>25</td>
<td>spt</td>
<td>Source port</td>
</tr>
<tr>
<td>26</td>
<td>externalID</td>
<td>External ID (event ID)</td>
</tr>
<tr>
<td>27</td>
<td>rt</td>
<td>Event time</td>
</tr>
<tr>
<td>28</td>
<td>cat</td>
<td>Device event category</td>
</tr>
<tr>
<td>29</td>
<td>proto</td>
<td>Transport protocol</td>
</tr>
<tr>
<td>30</td>
<td>deviceInboundInterface</td>
<td>Device inbound interface (physical port in)</td>
</tr>
<tr>
<td>31</td>
<td>c6a2</td>
<td>Source IPv6 address</td>
</tr>
<tr>
<td>32</td>
<td>c6a3</td>
<td>Destination IPv6 address</td>
</tr>
<tr>
<td>33</td>
<td>request</td>
<td>URI string</td>
</tr>
<tr>
<td>34</td>
<td>requestMethod</td>
<td>URI method</td>
</tr>
<tr>
<td>35</td>
<td>dhost</td>
<td>URI host</td>
</tr>
</tbody>
</table>
Event sample data

The following is a log message for one event, as it would appear on the syslog:

```
CEF:0|TippingPoint|UnityOne|1.0.0.17|3701|3701:
HTTP: PayPal Login Phish Site|4|app=TCP cnt=1
dst=168.187.175.20
dpt=1185
act=Block
cn1=0 cn1Label=VLAN ID
cn2=33885180 cn2Label=Taxonomy
cn3=0 cn3Label=Packet Trace
cs1=URI Profile cs1Label=Profile Name
cs2=00000002-0002-0002-0002-000000003701
cs2Label=Policy UUID
cs3=00000001-0001-0001-0001-000000003701
cs3Label=Signature UUID
cs4=6A 6B
cs4Label=ZoneNames
cs5=smszorro02
cs5Label=Device Name
cs6= cs6Label=Filter MessageParms
src=189.206.92.117 spt=80
externalId=16118775 rt=1396449083073 cat=Identity Theft proto=TCP
deviceInboundInterface=11
c6a2= c6a2Label=Source IPv6
c6a3= c6a3Label=Destination
IPv6 request=/modules/FCKeditor/upload/Media/index.html?login_cmd=
3Dlogin_access=3D1109785584
requestMethod=GET dhost=www.reptilien-freunde.net
```

ArcSight CEF Format v4.2

<table>
<thead>
<tr>
<th>Column</th>
<th>CEF key name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>CEF</td>
<td>CEF header (Version</td>
</tr>
<tr>
<td>1</td>
<td>app</td>
<td>Application protocol</td>
</tr>
<tr>
<td>2</td>
<td>act</td>
<td>Flow control of the filter</td>
</tr>
<tr>
<td>3</td>
<td>c6a1</td>
<td>Client IPv6 address</td>
</tr>
<tr>
<td>Column</td>
<td>CEF key name</td>
<td>Definition</td>
</tr>
<tr>
<td>--------</td>
<td>-----------------</td>
<td>-------------------------------------------------</td>
</tr>
<tr>
<td>4</td>
<td>c6a1Label</td>
<td>Client IPv6 address field label</td>
</tr>
<tr>
<td>5</td>
<td>c6a2</td>
<td>Source IPv6 address</td>
</tr>
<tr>
<td>6</td>
<td>c6a2Label</td>
<td>Source IPv6 address field label</td>
</tr>
<tr>
<td>7</td>
<td>c6a3</td>
<td>Destination IPv6 address</td>
</tr>
<tr>
<td>8</td>
<td>c6a3Label</td>
<td>Destination IPv6 address field label</td>
</tr>
<tr>
<td>9</td>
<td>cat</td>
<td>Filter name category</td>
</tr>
<tr>
<td>10</td>
<td>cn1</td>
<td>Device custom number 1: VLAN ID</td>
</tr>
<tr>
<td>11</td>
<td>cn1Label</td>
<td>Device custom number 1 label</td>
</tr>
<tr>
<td>12</td>
<td>cn2</td>
<td>Device custom number 2: taxonomy ID</td>
</tr>
<tr>
<td>13</td>
<td>cn2Label</td>
<td>Device custom number 2 label</td>
</tr>
<tr>
<td>14</td>
<td>cn3</td>
<td>Device custom number 3: packet trace</td>
</tr>
<tr>
<td>15</td>
<td>cn3Label</td>
<td>Device custom number 3 label</td>
</tr>
<tr>
<td>16</td>
<td>cs1</td>
<td>Device custom string 1: profile name</td>
</tr>
<tr>
<td>17</td>
<td>cs1Label</td>
<td>Device custom string 1 label</td>
</tr>
<tr>
<td>18</td>
<td>cs2</td>
<td>Device custom string 2: profile UUID</td>
</tr>
<tr>
<td>19</td>
<td>cs2Label</td>
<td>Device custom string 2 label</td>
</tr>
<tr>
<td>Column</td>
<td>CEF key name</td>
<td>Definition</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
<td>------------</td>
</tr>
<tr>
<td>20</td>
<td>cs3</td>
<td>Device custom string 3: filter signature UUID</td>
</tr>
<tr>
<td>21</td>
<td>cs3Label</td>
<td>Device custom string 3 label</td>
</tr>
<tr>
<td>22</td>
<td>cs4</td>
<td>Device custom string 4: zone names (source and destination)</td>
</tr>
<tr>
<td>23</td>
<td>cs4Label</td>
<td>Device custom string 4 label</td>
</tr>
<tr>
<td>24</td>
<td>cs5</td>
<td>Device custom string 5: device name</td>
</tr>
<tr>
<td>25</td>
<td>cs5Label</td>
<td>Device custom string 5 label</td>
</tr>
<tr>
<td>26</td>
<td>cs6</td>
<td>Device custom string 6: filter message parameters</td>
</tr>
<tr>
<td>27</td>
<td>cs6Label</td>
<td>Device custom string 6 label</td>
</tr>
<tr>
<td>28</td>
<td>cnt</td>
<td>Event hit count</td>
</tr>
<tr>
<td>29</td>
<td>deviceInboundInterface</td>
<td>Physical port in</td>
</tr>
<tr>
<td>30</td>
<td>dhost</td>
<td>Host name of the URI</td>
</tr>
<tr>
<td>31</td>
<td>dntdom</td>
<td>Destination domain name</td>
</tr>
<tr>
<td>32</td>
<td>dpt</td>
<td>Destination port</td>
</tr>
<tr>
<td>33</td>
<td>dst</td>
<td>Destination IPv4 address</td>
</tr>
<tr>
<td>34</td>
<td>duser</td>
<td>Destination username</td>
</tr>
<tr>
<td>35</td>
<td>dvchost</td>
<td>Device name</td>
</tr>
<tr>
<td>Column</td>
<td>CEF key name</td>
<td>Definition</td>
</tr>
<tr>
<td>--------</td>
<td>--------------------------------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>36</td>
<td>externalId</td>
<td>Event ID</td>
</tr>
<tr>
<td>37</td>
<td>proto</td>
<td>Network protocol</td>
</tr>
<tr>
<td>38</td>
<td>request</td>
<td>URI string</td>
</tr>
<tr>
<td>39</td>
<td>requestMethod</td>
<td>URI method</td>
</tr>
<tr>
<td>40</td>
<td>rt</td>
<td>Event time stamp</td>
</tr>
<tr>
<td>41</td>
<td>sntdom</td>
<td>Source domain name</td>
</tr>
<tr>
<td>42</td>
<td>sourceTranslatedAddress</td>
<td>Client IPv4 address</td>
</tr>
<tr>
<td>43</td>
<td>spt</td>
<td>Source port</td>
</tr>
<tr>
<td>44</td>
<td>src</td>
<td>Source IPv4 address</td>
</tr>
<tr>
<td>45</td>
<td>suser</td>
<td>Source user name</td>
</tr>
</tbody>
</table>

**Event sample data**

The following is a log message for one event, as it would appear on the syslog:

```
CEF:0|TippingPoint|UnityOne|1.0.0.17|3701|3701:
HTTP: PayPal Login Phish Site|4|app=TCP
cnt=1
dst=168.187.175.20
dpt=1185
act=Block
cn1=0 cn1Label=VLAN ID
cn2=33885180 cn2Label=Taxonomy
cn3=0 cn3Label=Packet Trace
cs1=URI Profile cs1Label=Profile Name
cs2=00000002-0002-0002-0002-000000003701
cs2Label=Policy UUID
cs3=00000001-0001-0001-0001-000000003701
cs3Label=Signature UUID
cs4=6A 6B
```
Create or edit a custom syslog format

1. Go to Admin > Server Properties > Syslog.
2. On the Syslog Formats panel, click New or select a custom syslog format, and then click Edit. All of the custom syslog formats display after the default syslog formats.
3. Type a name for the custom syslog format in the Name field.
4. (Optional) Type a description that identifies the syslog format in the Description field.
5. Click Insert Field, and then select the field elements that you want to include in the syslog format. For an explanation of the available fields, see Available fields in a syslog format on page 618. The fields that you select appear in the Pattern area.

   Note: The maximum size of a syslog message is 9K.

6. (Optional) Provide (or modify) the event fields in syslog format as needed in the Pattern area.
7. Specify whether a syslog that exceeds the size limit (1024 bytes) is RFC 3164 compliant (messages are truncated) or RFC 5424 compliant (messages are split into multiple messages).
8. Click OK to save the custom format.

Available fields in a syslog format

The following table describes the supported fields that compose a syslog format.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>actionType</td>
<td>Action type that is used on the filter associated with the event. Supported action types include the following:</td>
<td>Integer</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
<td>Type</td>
</tr>
<tr>
<td>--------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------</td>
</tr>
<tr>
<td>arcSightFilterName</td>
<td>Name of the filter associated with the event</td>
<td>String</td>
</tr>
<tr>
<td>arcSightSeverity</td>
<td>Severity — 0 is Normal, 1 is Low, 2 is Minor, 3 is Major, 4 is Critical</td>
<td>Integer</td>
</tr>
<tr>
<td>categoryName</td>
<td>Name of the filter category</td>
<td>String</td>
</tr>
<tr>
<td>clientAddress</td>
<td>TCIP/XFF client IP address in IPv4 (for example, 10.0.0.1) or IPv6 format from HTTP traffic when configured in the profile settings.</td>
<td>IPv4 or IPv6 address</td>
</tr>
</tbody>
</table>

**Note:** This field matches the `srcAddress` field when TCIP/XFF collection is enabled but TCIP/XFF is unavailable for the traffic flow associated with the event.

This field will be empty in the following situations:

- The profile configured on the segment does not have TCIP/XFF enabled
- The IPS device is running a version of TOS that doesn’t support the feature

- 7 — IPS Alert
- 8 — IPS Block
- 9 — P2P
- 12 — Quarantine
- 33 — NGFW Block
- 34 — NGFW Alert
- 35 — NGFW VPN
- 36 — NGFW Visibility
- 37 — Reputation Alert
- 38 — Reputation Block
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>clientAddressv4</td>
<td>TCIP/ XFF client IP address in IPv4 format (for example, 10.0.0.1) from HTTP traffic when configured in the profile settings.</td>
<td>IPv4 address</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>This field matches the srcAddress field when TCIP/XFF collection is enabled but TCIP/XFF is unavailable for the traffic flow associated with the event.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>This field will be empty in the following situations:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• The profile configured on the segment does not have TCIP/XFF enabled</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• The IPS device is running a version of TOS that doesn't support the feature</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• An IPv6 address was captured</td>
<td></td>
</tr>
<tr>
<td>clientAddressv6</td>
<td>TCIP/XFF client IPv6 address in IPv6 format (for example, 2001:db8:85a3:8a2e:370:7334) from HTTP traffic when configured in the profile settings.</td>
<td>IPv6 address</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>This field matches the srcAddress field when TCIP/XFF collection is enabled but TCIP/XFF is unavailable for the traffic flow associated with the event.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>This field will be empty in the following situations:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• The profile configured on the segment does not have TCIP/XFF enabled</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• The IPS device is running a version of TOS that doesn't support the feature</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• An IPv4 address was captured</td>
<td></td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
<td>Type</td>
</tr>
<tr>
<td>--------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>correlationId</td>
<td>Session identifier for an event coming from an NGFW appliance. It can be used to correlate all the NGFW events for a single session.</td>
<td>Long</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This field will only be available from NGFW appliances.</td>
<td></td>
</tr>
<tr>
<td>cveIds</td>
<td>CVE ID</td>
<td>String</td>
</tr>
<tr>
<td></td>
<td><strong>When creating a custom syslog format, note the following:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Because commas are used to separate multiple CVEs in a syslog entry, define and manually insert an escape character when you use comma delimiters in your custom syslog. These characters will properly separate the CVE ID field so that the receiving server can parse the custom fields.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> You might also need to adjust the settings for your syslog server so that it recognizes the defined escape character.</td>
<td></td>
</tr>
<tr>
<td>destAddress</td>
<td>Destination address of the event (for example, 10.0.0.2)</td>
<td>IPv4 or IPv6 address</td>
</tr>
<tr>
<td>destAddressv4</td>
<td>Destination IPv4 address (for example, 10.0.0.2)</td>
<td>IPv4 address</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This field will be empty if the destAddress is an IPv6 address.</td>
<td></td>
</tr>
<tr>
<td>destAddressv6</td>
<td>Destination IPv6 address (for example, 2001:db8:85a3::8a2e:370:7335)</td>
<td>IPv6 address</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This field will be empty if the destAddress is an IPv4 address.</td>
<td></td>
</tr>
<tr>
<td>destPort</td>
<td>Destination port number</td>
<td>Integer</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
<td>Type</td>
</tr>
<tr>
<td>---------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>--------</td>
</tr>
<tr>
<td>destUserDomain</td>
<td>Active Directory domain name of the user at the destination IP address</td>
<td>String</td>
</tr>
<tr>
<td></td>
<td>(for example, marketing.acme.net)</td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>In order for this field to display, the Identity Agent</td>
<td></td>
</tr>
<tr>
<td></td>
<td>must be configured for the SMS.</td>
<td></td>
</tr>
<tr>
<td>destUserMachine</td>
<td>Computer name for the user at the destination IP address (for example,</td>
<td>String</td>
</tr>
<tr>
<td></td>
<td>computername.marketing.acme.net)</td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>In order for this field to display, the Identity Agent</td>
<td></td>
</tr>
<tr>
<td></td>
<td>must be configured for the SMS.</td>
<td></td>
</tr>
<tr>
<td>destUserName</td>
<td>Active Directory logged in username at the destination IP address (for</td>
<td>String</td>
</tr>
<tr>
<td></td>
<td>example, johndoe.marketing.acme.net)</td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>In order for this field to display, the Identity Agent</td>
<td></td>
</tr>
<tr>
<td></td>
<td>must be configured for the SMS.</td>
<td></td>
</tr>
<tr>
<td>destZone</td>
<td>Destination zone name (for example, 1-2B)</td>
<td>String</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>This field will only be available from NGFW appliances.</td>
<td></td>
</tr>
<tr>
<td>deviceName</td>
<td>User-provided name of the device event was received from</td>
<td>String</td>
</tr>
<tr>
<td>deviceSegment</td>
<td>Segment on the device where the event occurred (for example, 2)</td>
<td>Integer</td>
</tr>
<tr>
<td>deviceSlot</td>
<td>Device Slot (for example, 11)</td>
<td>Integer</td>
</tr>
<tr>
<td>deviceTimezone</td>
<td>Device time zone (for example, CST)</td>
<td>String</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
<td>Type</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------</td>
</tr>
<tr>
<td>eventID</td>
<td>SMS event identifier</td>
<td>Long</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> In the SMS, this is the Event No. field, which is available on the Event Details for Inspection and Firewall events.</td>
<td></td>
</tr>
<tr>
<td>eventTimestamp</td>
<td>Event timestamp in milliseconds since epoch (for example, 1445012290091)</td>
<td>Long</td>
</tr>
<tr>
<td>filterName</td>
<td>Name of the filter associated with the event</td>
<td>String</td>
</tr>
<tr>
<td>filterNameV2</td>
<td>Name of the filter associated with the event and contains the same information as the filterName field except for the colon (:) and semi-colon (;) punctuation</td>
<td>String</td>
</tr>
<tr>
<td>firewallRuleUUID</td>
<td>UUID of the Firewall rule that is applied to the traffic (for example, DEFAULT will appear for the default block rule)</td>
<td>String</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This field will only be available from NGFW appliances.</td>
<td></td>
</tr>
<tr>
<td>flowControl</td>
<td>Flow control of the filter (for example, block or permit)</td>
<td>String</td>
</tr>
<tr>
<td>hitCount</td>
<td>Number of times this event occurred during aggregation period</td>
<td>Integer</td>
</tr>
<tr>
<td>inInterfaceName</td>
<td>Inbound interface name</td>
<td>String</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This field will only be available from NGFW appliances.</td>
<td></td>
</tr>
<tr>
<td>inspectionProfileUUID</td>
<td>Profile UUID (for example, c6da0827-798b-49ad-85e8-bb8e0ae531b5)</td>
<td>String</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This field will only be available from NGFW appliances.</td>
<td></td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
<td>Type</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>msgParameters</td>
<td>Message parameters used for certain filters, such as DDoS filters and Reputation filters. Each parameter is separated by pipes (for example, 10.1.4.80/32</td>
<td>exceeds</td>
</tr>
<tr>
<td>Example</td>
<td>If a signature has a message (e.g., 7202 is 7202: SYN flood against [1] [2] [3] SYNs/sec (current rate = [4], the numbers in brackets refer to the data in the message parameters. The complete message results when the signature message is combined with the message parameters. For example: 7202: SYN flood against 10.1.4.80/32 exceeds 1 SYNs/sec (current rate = 3)</td>
<td></td>
</tr>
<tr>
<td>outInterfaceName</td>
<td>Outbound interface name</td>
<td>String</td>
</tr>
<tr>
<td>Note</td>
<td>This field will only be available from NGFW appliances.</td>
<td></td>
</tr>
<tr>
<td>packetTrace</td>
<td>Packet trace associated with the event — 0 is if there is no packet trace, 1 is if there is a packet trace</td>
<td>Boolean</td>
</tr>
<tr>
<td>Note</td>
<td>This field will not be available from TPS devices and NGFW appliances.</td>
<td></td>
</tr>
<tr>
<td>physicalPortIn</td>
<td>Physical port in</td>
<td>Integer</td>
</tr>
<tr>
<td>policyUUID</td>
<td>UUID for the policy (for example, c6da0827-798b-49ad-85e8-bb8e0ae531b5)</td>
<td>String</td>
</tr>
<tr>
<td>Note</td>
<td>You can also use this field in conjunction with the SMS Web Services API.</td>
<td></td>
</tr>
<tr>
<td>profileName</td>
<td>Name of the profile on the device segment/interface where the event occurred</td>
<td>String</td>
</tr>
<tr>
<td>protocol</td>
<td>Name of the protocol (for example, HTTP, ICMP, etc.)</td>
<td>String</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
<td>Type</td>
</tr>
<tr>
<td>---------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>protocolLower</td>
<td>Name of the protocol in lowercase letters (for example, http, icmp, etc.)</td>
<td>String</td>
</tr>
<tr>
<td>severity</td>
<td>Severity — 0 is Normal, 1 is Low, 2 is Minor, 3 is Major, 4 is Critical</td>
<td>Integer</td>
</tr>
<tr>
<td>severityType</td>
<td>Text of the severity (for example, Low, Minor, Major, etc.)</td>
<td>String</td>
</tr>
<tr>
<td>signatureName</td>
<td>User-friendly name for the filter (for example, 0027: IP Options: Record Route (RR))</td>
<td>String</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> You can also use this field in conjunction with the SMS Web Services API.</td>
<td></td>
</tr>
<tr>
<td>signatureNumber</td>
<td>Filter number (for example, 27)</td>
<td>Integer</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> You can also use this field in conjunction with the SMS Web Services API.</td>
<td></td>
</tr>
<tr>
<td>signatureUUID</td>
<td>UUID for the filter (for example, 00000001-0001-0001-0001-000000000027)</td>
<td>String</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> You can also use this field in conjunction with the SMS Web Services API.</td>
<td></td>
</tr>
<tr>
<td>smsName</td>
<td>User-provided name of the SMS (hostname)</td>
<td>String</td>
</tr>
<tr>
<td>snortClass [deprecated]</td>
<td>Snort Classification (for example, Misc Attack)</td>
<td>String</td>
</tr>
<tr>
<td>snortDate [deprecated]</td>
<td>Event timestamp (for example, Oct 16 10:20:35)</td>
<td>Date</td>
</tr>
<tr>
<td>snortDestAddress [deprecated]</td>
<td>Destination address and port of the event (for example, 10.0.0.2:1368)</td>
<td>IP address: Port</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
<td>Type</td>
</tr>
<tr>
<td>---------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>snortName [deprecated]</td>
<td>Name of the filter associated with the event</td>
<td>String</td>
</tr>
<tr>
<td>snortNameV2 [deprecated]</td>
<td>Name of the filter associated with the event</td>
<td>String</td>
</tr>
<tr>
<td>snortPriority [deprecated]</td>
<td>Severity — 0 is Normal, 1 is Low, 2 is Minor, 3 is Major, 4 is Critical</td>
<td>Integer</td>
</tr>
<tr>
<td>snortProtocol [deprecated]</td>
<td>Name of the protocol (for example, HTTP, ICMP, etc.)</td>
<td>String</td>
</tr>
<tr>
<td>snortProtocolV2 [deprecated]</td>
<td>Name of the protocol (for example, HTTP, ICMP, etc.)</td>
<td>String</td>
</tr>
<tr>
<td>snortSid [deprecated]</td>
<td>Snort rule identifier (for example, [1:0:1])</td>
<td>String</td>
</tr>
<tr>
<td>snortSrcAddress [deprecated]</td>
<td>Source address and port of the event (for example, 10.0.0.3:80)</td>
<td>IP address: Port</td>
</tr>
<tr>
<td>srcAddress</td>
<td>Source address of the event (for example, 10.0.0.3)</td>
<td>IP address</td>
</tr>
<tr>
<td>srcAddressv4</td>
<td>Source IPv4 address (for example, 10.0.0.3). This field will be empty if the srcAddress is an IPv6 address.</td>
<td>IPv4 address</td>
</tr>
<tr>
<td>srcAddressv6</td>
<td>Source IPv6 address (for example, 2001:db8:85a3::8a2e:370:7336). This field will be empty if the srcAddress is an IPv4 address.</td>
<td>IPv6 address</td>
</tr>
<tr>
<td>srcPort</td>
<td>Source port number</td>
<td>Integer</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
<td>Type</td>
</tr>
<tr>
<td>--------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>srcUserDomain</td>
<td>Active Directory domain name of the user at the source IP address (for example, marketing.acme.net)</td>
<td>String</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> In order for this field to display, the Identity Agent must be configured for the SMS.</td>
<td></td>
</tr>
<tr>
<td>srcUserMachine</td>
<td>Computer name for the user at the source IP address (for example, computernamemarketing.acme.net)</td>
<td>String</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> In order for this field to display, the Identity Agent must be configured for the SMS.</td>
<td></td>
</tr>
<tr>
<td>srcZone</td>
<td>Source zone name</td>
<td>String</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This field will only be available from NGFW appliances.</td>
<td></td>
</tr>
<tr>
<td>taxonomyID</td>
<td>Category ID assigned to the signature</td>
<td>Long</td>
</tr>
<tr>
<td>uriHost</td>
<td>HTTP hostname from the HTTP header when HTTP context is configured for the profile and reported by the IPS device (for example, example.com)</td>
<td>String</td>
</tr>
<tr>
<td>uriMethod</td>
<td>HTTP method from the HTTP header when HTTP context is configured for the profile and reported by the IPS device (for example, GET)</td>
<td>String</td>
</tr>
<tr>
<td>uriString</td>
<td>URI from the HTTP header when HTTP context is configured for the profile and reported by the IPS device (for example, /path/to/resource/resource.txt)</td>
<td>String (8k limit)</td>
</tr>
<tr>
<td>vlanTag</td>
<td>Vlan ID</td>
<td>Integer</td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delimiter</td>
<td>Determines the character the SMS uses as a delimiter for event data in the syslog (tab, comma, semi-colon, or pipe)</td>
<td></td>
</tr>
</tbody>
</table>

### Copy an existing syslog format to create a custom format

1. On the Syslog tab, select the syslog entry you want to copy. For descriptions and examples of the SMS and device syslog formats, see *Syslog format options* on page 600.
2. Click **Copy**.
3. In the Edit Syslog Format dialog, you can do the following:
   - Edit the **Name** and **Description**.
   - Modify the Pattern as needed.
   - Click **Insert Field**, and then select the field elements that you want to include in the syslog format. For an explanation of the available fields, see *Available fields in a syslog format* on page 618. The fields that you select appear in the Pattern area.
4. Click **OK** to save the custom format.

   The custom syslog format will display after the default syslog formats on the Syslog Formats table.

### Delete a user-defined syslog format

1. On the Syslog tab, select the syslog entry you want to delete.
2. Click **Delete**.
3. Click **Yes**.

### Remote syslog for events

The **Remote Syslog for Events** panel on the Syslog tab enables you to configure remote syslog notification settings.

To control the number of events that are sent to a remote syslog server, the SMS allows you to filter the events that are sent. In addition, when you initially configure a connection to a remote syslog server, you can choose to send only future events, excluding what could be a sizable number of historical events.

The following table describes the information the SMS requires to send syslog events to a remote syslog server.
<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syslog Server</td>
<td>Hostname or IP address of the remote syslog server</td>
</tr>
<tr>
<td>Protocol</td>
<td>Transport protocol used in sending event notifications to the remote syslog server. Valid options are UDP, TCP, and Encrypted TCP.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> When URI information that includes URI strings is sent using the UDP protocol, data loss can result. For best results in logging URI string information, use either the TCP or Encrypted TCP protocol.</td>
</tr>
<tr>
<td>Port</td>
<td>Port on the remote syslog server used for communicating syslog events.</td>
</tr>
<tr>
<td>Log Type</td>
<td>Syslog format the SMS uses when sending event notifications to the remote syslog server. The format varies depending on the version of the SMS and the event itself. The format is important because the receiving server must know how to interpret the data. The SMS provides the following syslog format options:</td>
</tr>
<tr>
<td></td>
<td>• <strong>SMS System:</strong> SMS system logging</td>
</tr>
<tr>
<td></td>
<td>• <strong>SMS Audit:</strong> SMS audit logging</td>
</tr>
<tr>
<td></td>
<td>• <strong>Device System:</strong> Device system logging</td>
</tr>
<tr>
<td></td>
<td>• <strong>Device Audit:</strong> Device audit logging</td>
</tr>
<tr>
<td></td>
<td>• <strong>Snort Syslog (MARS) [Deprecated]:</strong> Send Snort-configured-for-MARS events</td>
</tr>
<tr>
<td></td>
<td>• <strong>Snort Syslog V2 [Deprecated]:</strong> Send Snort Version 2 events</td>
</tr>
<tr>
<td></td>
<td>• <strong>SMS 2.0 / 2.1 Syslog Format:</strong> Send SMS v2.0 / 2.1 log events</td>
</tr>
<tr>
<td></td>
<td>• <strong>SMS 2.5 Syslog Format:</strong> Send SMS v2.5 log events</td>
</tr>
<tr>
<td></td>
<td>• <strong>ArcSight CEF Format v3.5 [Deprecated]:</strong> Send events to an ArcSight connector (Deprecated – does not support IPv6)</td>
</tr>
<tr>
<td></td>
<td>• <strong>ArcSight CEF Format v4.1 [Deprecated]:</strong> Send events to an ArcSight connector (Deprecated – adds HTTP context information and IPv6 support)</td>
</tr>
</tbody>
</table>
### Setting | Description
--- | ---
- **ArcSight CEF Format v4.2**: Send events to an ArcSight connector (Recommended – adds HTTP context information, TCIP/XFF client IP, and user information)

**Note**: SMS and device syslog formats cannot be modified. See *Syslog format options* on page 600 for descriptions and examples of the syslog formats.

| Event Query | Determines whether the SMS sends all events or a select set of events to the remote syslog server. |
| Facility | Limits the events send to the remote syslog server to a specific facility level. Facilities are defined by the BSD Syslog Protocol. Refer to RFC 3164. |
| Severity | Limits the events sent to the remote syslog server to events that match the specified severity. |
| Delimiter | Determines the character the SMS uses as a delimiter for event data in the syslog. Options include tab, comma, semi-colon, pipe, or space. |
| Timestamp | Determines the timestamp the SMS includes in headers in messages sent to the remote syslog: |
  - **None** – No timestamp is included in the message header
  - **SMS current timestamp** – Timestamp when the SMS sends the message to the remote syslog server
  - **Event timestamp** – Original timestamp of the event that is being reported

**Configure remote syslog notification settings**

1. On the Remote Syslog for Events panel, click **New**.
2. In the Create Remote Syslog Notification Settings dialog, select **Enable** to enable the sending of events to the remote syslog server.
3. Provide the host name or IP address of the remote syslog server.
4. Select the protocol the SMS is to use to send notifications to the remote syslog server. Options include UDP, TCP, and Encrypted TCP.
If you select Encrypted TCP, you must import an x509 certificate. The certificate is generated on the remote syslog server, and must be imported to the SMS. Click Import to select the x509 certificate file from your local drive or storage media. If you have already imported a certificate into the SMS certificate repository, simply choose the one you want. For more information about certificate management, see Viewing Certificate Authority (CA) certificates on page 573.

**Note:** When URI information that includes URI strings is sent using the UDP protocol, data loss can result. When logging URI string information, use either the TCP or Encrypted TCP protocol.

5. Provide the port number for the listener port on the remote syslog server.

6. Click **Log Type**, and select a log type format. See Remote syslog for events on page 628 for available options.

7. Select an Event Query option, if this field is available.

8. Click **Facility**, and select an option.

9. Select a **Severity** to limit events sent to the remote syslog server to a specific severity level.

10. Select a **Delimiter** for event data in the syslog.

11. On the Include Timestamp in Header panel, select an option as described in Table on page 628.

12. Do the following:
   - Select or clear **Include SMS Hostname in Header** to determine whether the message header includes the hostname of the SMS.
   - Select or clear **Send New Events/Log Only** to determine whether the SMS will send only new events and log entries, not those already received by the SMS.

13. Click **OK**.

**Edit syslog server settings**

1. On the Remote Syslog for Events panel, select an entry, and then click **Edit**.

2. In the Edit Syslog Notification Settings dialog, adjust settings as needed, and click **OK**.

**Delete a syslog server**

1. On the Remote Syslog for Events panel, select the syslog server configuration that you want to delete, and click **Delete**.

2. In the Delete Syslog dialog, click **Yes**.

**Configuring SNMP properties**

SNMP is an application-layer protocol that monitors network devices for conditions that warrant administrative attention. Items typically monitored include servers, workstations, routers, switches and hubs. You can configure SMS to be a managed device that is monitored by an SNMP server. The SNMP server periodically requests information from the SMS server. You can also configure SMS to send trap
information to the SNMP server. The SNMP server is also referred to as a network management system (NMS) and come in a variety of products, including OpenView.

SMS supports SNMP v2 and the latest version, SNMP v3, which has additional security and remote configuration capabilities.

The SNMP tab enables you to configure SNMP request settings and NMS trap destinations.

**Request settings**

SNMP request settings determine how the SMS handles SNMP requests. To configure communications between the SMS server and the SNMP server, as well as to correctly identify the SMS server SNMP information, you must configure SNMP request settings.

**Note:** SNMP request settings do not affect SMS communication with IPS devices.

**Enable SNMP requests**

1. On the Admin (Server Properties) screen, select the **SNMP** tab.
2. Click **Edit** on the Request Settings panel.
3. In the SNMP Request Settings dialog, select **Enable SNMP Requests**.
4. Do one of the following:
   a. Select **SNMP Version v2**, and use the Community String field to restrict access. By default, the Community String is “public.”
   b. Select **SNMP Version v3**, and provide the following information:
      • User name required for the SNMP application
      • Protocol used for authentication (None, MD5, or SHA)
      • Key used with the authentication protocol (you must verify the key)
      • Protocol (encryption method) used for privacy (DES, AES-128, AES-192, AES-256, or Triple_DES)
      • Key used with privacy protocol (you must verify the key)

**Note:** The Engine ID is a read-only, SMS-generated identifier for the SNMP application.

**Note:** If no protocol is selected, the Key field is disabled.

• Select **Both**, and provide the information for both v2 and v3.

5. Click **OK**.

**Disable SNMP requests**

1. On the Admin (Server Properties) screen, select the **SNMP** tab.
2. Click **Edit** on the Request Settings panel.
3. In the SNMP Request Settings dialog, clear the **Enable SNMP Requests** check box.
4. Click **OK**.

**NMS trap destinations**

To configure the SMS to send SNMP trap information to an SMTP server you must identify one or more NMS trap destination.

Configure the SMS to send NMS traps to a destination

1. On the Admin (Server Properties) screen, select the **SNMP** tab.
2. Click **Add** on the NMS Trap Destinations panel.
3. In the NMS Trap Destination dialog, provide an IP address and port for the trap destination.
4. Do one of the following:
   a. Select v2, and use the Community String field to restrict access. By default, the Community String is “public.”
   b. Select v3, and provide the following information:
      • User name required for the SNMP application
      • Protocol used for authentication (None, MD5, or SHA)
      • Key used with the authentication protocol (you must verify the key)
      • Protocol (encryption method) used for privacy (DES, AES-128, AES-192, AES-256, or Triple DES)
      • Key used with privacy protocol (you must verify the key)

**Note:** The Engine ID is a read-only, SMS-generated identifier for the SNMP application.

**Note:** If no protocol is selected, the Key field is disabled.

5. Click **Test** to send a test trap to the specified destination.
6. When you are finished, click **OK**.

**Edit an NMS trap destination**

1. Click **Edit** on the NMS Trap Destinations panel.
2. Edit the NMS trap destination settings as needed.
3. Click **Test** to send a test trap to the specified destination.
4. When you are finished, click **OK**.

**Delete an NMS trap destination**

1. On the NMS Trap Destinations panel, select one or more entries.
2. Click **Delete**.

3. In the Delete Selected Trap Destination dialog, click **Yes**.

## Configuring TLS settings

Use this page to define which TLS versions (v1.0, v1.1, and v1.2) will be enabled for the various SMS communication categories.

- **Web Server**— allows access to the SMS web server using a Web browser or the SMS Web API. The TLS version on your client (e.g., Web browser) must be compatible with the TLS versions enabled in this section.

- **IPS Remote Authentication** — used by the IPS devices when the SMS is used as the authentication source. If the device doesn't support the TLS version, the SMS will not be able to communicate with the device.

- **SMS Client Communication** — used for communication between the SMS client and the SMS server.

- **SMS connecting to Devices/TMC/LDAP**— used for communication between the SMS and remote servers, such as LDAP, TMC, Identity Agent, and managed devices. You can enable SSLv3.0 if your remote server requires this protocol.

### SMS connecting to Devices/TMC/LDAP

If the SSLv3.0 protocol is not required in your network environment, we recommend that you disable it as it is the least secure TLS version.

The TLS versions enabled on a TPS device must be compatible with the TLS versions enabled in this section. To review the TLS settings on the TPS device, go to the TPS device, and then select **Device Configuration > Services**.

If TLS v1.2 is enabled and you are using the Identity Agent with TLS v1.2 enabled, the SMS must be running with the 2K key. For more information, see *SMS certificate key* on page 537.

If you have trouble managing a TippingPoint SSL appliance 1500S, set the TLS version to 1.0 only.

Before you edit the TLS versions, note the following caveats:

- You must select at least one TLS version for each communication category. Due to security reasons, we recommend that you disable TLS v1.0 and SSLv3.0 if they are not required in your network environment.

- The TLS versions for some devices are incompatible with the SMS. Before you configure the TLS versions settings, review the list of unsupported devices available on the **TMC**.

- Editing the TLS versions requires a restart of the SMS.

For more information on the supported cipher suites for the TLS versions, see *SMS encryption protocols, algorithms, and cipher support* on page 694.
Edit TLS versions

1. On the Admin (Server Properties) screen, select the TLS tab.
2. Review the current state for each communication type. A check mark indicates if a TLS version is enabled. If it is not, the radio button is unselected and the current state displays as Disabled.
3. Click Edit to edit the TLS versions.
4. Select one or more TLS versions for the communication categories:
   
   Note: You must select at least one TLS version for each communication category.

   - Click Select All Settings to quickly select all versions for all communication categories. Clear the check box to quickly remove all version selections for the communication categories.
   - Click All TLS v1.0 to quickly select all v1.0 versions for all communication categories.
   - Click All TLS v1.1 to quickly select all v1.1 versions for all communication categories.
   - Click All TLS v1.2 to quickly select all v1.2 versions for all communication categories.
   - Click All SSL v2Hello to quickly select the SSL v2Hello versions for the Web Server and IPS Remote Authentication communication categories.
5. If there are incompatibilities between the SMS TLS versions and the managed device TLS versions, the SMS will display warnings and/or errors. Click Details to review the severity and descriptions. If there are any errors, you cannot save your changes until you select compatible TLS versions.
6. Click OK. Editing the TLS versions requires a restart of the SMS. Click Yes to immediately reboot the SMS and commit the TLS versions.

High Availability

The SMS can be configured to operate in an active-passive, high availability (HA) cluster, increasing availability of the SMS in case an unexpected event causes the primary SMS to fail or become inaccessible. The SMS HA cluster consists of two nodes, one designated as the primary SMS, the other designated as the secondary SMS. Under normal operation, the state of the primary SMS is Active, and the state of the secondary SMS is Passive, unless the primary SMS becomes unavailable. When the primary SMS is unavailable, the state of the secondary SMS changes to Active.

During initial HA configuration, the SMS cluster performs a synchronization of the database from the active SMS to the passive SMS. To keep the passive SMS current, the active SMS replicates critical SMS data to the passive SMS, including database and SMS configuration.

In the Admin workspace, select High Availability in the navigation pane to display the Admin (High Availability) screen. This screen displays HA-related information and enables you to configure and adjust the SMS HA settings, synchronize the two nodes, and monitor the HA cluster status.
SMS HA cluster compatibility requirements

The active and passive systems must meet the following compatibility requirements to configure the SMS HA cluster:

- **Version number** – Both systems must be running the same version number (including patch number). Both systems should be the same model and have similar disk memory and disk space.

- **Partition number** – Both systems must use the identical partition version.

- **FIPS mode** – Both systems must have FIPS mode disabled.

- **SMS certificate key** – Both systems must have compatible SMS certificate key sizes. For example, the active SMS cannot be running a 1K key and the passive SMS be running a 2K key. You cannot install the 2K key in either SMS while the SMS is running in HA. To install a 2K key, disable the cluster, install the 2K key on each SMS, and then reconfigure the cluster.

- **SNMP** – You are not permitted to modify SNMP settings for the passive SMS server after SMS HA is configured. If you use SNMP to monitor and manage your SMS servers, you must configure the SMS's connectivity to an SNMP server before you configure the SMS HA cluster. To modify SNMP settings, disable the cluster, modify the SNMP settings, and then reconfigure the cluster.

Replication bandwidth requirements

The SMS has replication bandwidth requirements for heartbeat, digital vaccine (DV) and upgrade package download, and event traffic.

- Less than 10 Kbps bandwidth is required for heartbeat and system usage/administration operations, such as policy management.

- A minimum of 1 Mbps bandwidth is recommended for DV and upgrade package download. These operations consume as much bandwidth as is available between the two systems, but headroom of about 1 Mbps keeps the two systems reasonably synchronized.

- Event traffic requires approximately 1.5 Mbps per 1,000 events/second.

Configure the SMS HA cluster

Configure a SMS HA cluster from the SMS server that you intend to be the primary node in the cluster. Note that all of your managed devices must be managed by the SMS server that you will be designating as the active SMS server. After you configure SMS HA, the primary node is the Active SMS and the SMS client can no longer log in to the Passive SMS.

1. In the Admin workspace, select **High Availability** in the navigation pane.

2. Click **Configure** on the HA Cluster Status panel.

3. In the SMS High Availability wizard, click **Next**.
4. Select replication options:
   - **Enable Event Data Replication** – Allows event data to be replicated from the active SMS to the passive SMS. This option is already selected by default.
   - **Enable Encrypted Replication** – Enables encryption for the data being replicated. This option does not affect data replication during a synchronization operation which automatically occurs over a secure channel.

   **Note:** If you clear the **Enable Event Data Replication** check box, the new events are not replicated from the active server to the passive server. This option should only be turned off when the SMS is already configured to use an external log process server like the Reporting Server and SIEM.

5. Click **Next**, and then specify the parameters that the SMS server uses to determine the timeout values:
   - **Total Heartbeat Timeout** – Indicates the total time the passive SMS uses to recover from a heartbeat failure. This option is already set to three minutes by default but can be adjusted from two to four minutes.
   - **Mitigation Timeout** – Indicates the total time the passive SMS spends on mitigation. This option is already set to five minutes by default but can be adjusted from four to six minutes.

   When the passive SMS detects a health check failure, the maximum time the SMS spends on the recovery process is the sum of the total heartbeat and mitigation timeouts.

6. Click **Next**, and then choose the appropriate network configuration:
   - **Primary Only** – All communications occur over a single network interface.
   - **Primary and Secondary** – Replication and heartbeat signals occur over a secondary, intra-cluster, network path.

7. Click **Next**, and then do the following:
   - To use a Shared Virtual Management IP address, select the check box and enter the IP address.

     **Note:** The Shared Virtual Management IP address and the Maintenance IP addresses of the active and passive SMS servers must be in the same subnet.

   - Provide the maintenance IP address for the passive SMS server.

8. Click **Next**, and then do the following if you specified a Primary and Secondary network configuration:
   a. Provide the secondary IP addresses for the active and passive SMS.
   b. If you do not require the IP addresses to reside in the same subnet, clear the check box and provide gateway IP addresses for the active and passive SMS servers.
   c. Click **Next** again.

9. Enter the login credentials for the passive SMS server. The credentials must be those of a user with SuperUser permissions.

10. Click **Configure**.
The Configuration Status dialog box displays ongoing status. When the configuration finishes, the HA Cluster Synchronization dialog box opens.

11. Select **Synchronize the HA cluster**. To include all historical event data, select **Include historical event data**.

   **Note:** If you include historical event data, depending on the size of your event database, it can take several hours to synchronize the cluster.

12. Click **Finish**.

   All client connections are disconnected because access to the SMS database is prohibited during the synchronization process. To monitor progress, click **More**. The HA Synchronization Status dialog displays a progress bar, time elapsed, and so on.

   When synchronization finishes, the SMS client automatically attempts to reestablish a connection with the active SMS server. When the connection is reestablished, the SMS client opens to the Admin (High Availability) screen.

13. Verify the operational state of the cluster.

   The Active SMS status should display Active, and the Passive SMS status should display Passive.

   If you chose the Primary and Secondary network configuration, verify that the Heartbeat IP addresses for each SMS cluster node are performing as expected. The SMS monitors the needs to synchronize the cluster nodes. In typical operation, you do not need to initialize another synchronization. However, if you manually failover a cluster node or take one of the nodes offline, you need to re-synchronize the SMS cluster.

**How do I apply SMS software updates to a cluster?**

**Upgrades:** Disable the HA cluster before you apply software upgrades. To upgrade an HA cluster, upgrade each SMS server separately, and then reestablish the cluster. The passive SMS server cannot be upgraded while HA is enabled because:

1. The low-level services that are running on the passive node do not perform software upgrades or database updates.
2. Database updates on the passive node break database replication and as a result, data integrity.

**Patches:** Before applying a patch to an SMS HA cluster, determine whether the patch includes database updates:

- If the patch contains database changes, be sure to disable the SMS HA cluster, apply the patch to each SMS server separately, and then reestablish the cluster. Applying a database patch while under SMS HA breaks database replication and as a result, data integrity. The patch process does not prevent you from applying a database patch while under SMS HA.
- If the patch does not contain database changes, initiate the patch process from the active SMS server. The active SMS server automatically propagates the patch to the passive SMS server. If the patch
requires a restart of the SMS software or a reboot of the SMS server, the action takes place on both the active and passive SMS servers.

**Hotfixes:** Before applying a hotfix to an SMS HA cluster, determine whether the patch includes database updates, and follow the same installation procedure for applying a patch.

**View HA cluster status**

If the high availability feature is configured, the HA Cluster Status panel displays the current status of the SMS HA cluster and the configuration settings. Configuration settings include the management IP address and network, and event replication status data.

HA Cluster Status and HA Replication Delay metrics are displayed in graphs to help you track the status of the SMS HA cluster. The HA Replication Delay metrics show how many seconds the passive SMS is behind the active SMS in data replication.

The SMS displays information for the Active and Passive SMS.

- **Active SMS** – In the Active SMS area of the High Availability screen, the SMS displays the system name, status, maintenance IP address, and heartbeat IP address of the active SMS server.

- **Passive SMS** – In the Passive SMS area of the High Availability screen, the SMS displays the system name, status, maintenance IP address, and heartbeat IP address of the passive SMS server.

  From within this area you can manually activate the passive SMS server, which in turn deactivates the current active SMS server if it is operational, by invoking a failover. You can also swap roles of the active and passive SMS servers.

**Adjust HA timeout values**

After the SMS HA cluster is configured, you can adjust its timeout values. For example, if the primary and secondary servers are located in different geographic regions or if you experience intermittent connectivity issues, you can increase the HA timeout values to prevent a heartbeat failover. However, if the two SMS servers are collocated or are on a low latency network, we recommend that you use the default timeout configuration values (three minutes for the Total Heartbeat Timeout and five minutes for the Mitigation Timeout).

You can set the total time the passive SMS spends to recover from a heartbeat failure using the **Total Heartbeat Timeout** field.

If the passive and active server-to-server communication is lost, the passive SMS initiates a mitigation process, which may include restarting the SMS. You can set the time the passive SMS spends on mitigation using the **Mitigation Timeout** field.

When the passive SMS detects a health check failure, the maximum time the SMS spends on the recovery process is the sum of the Total Heartbeat Timeout and Mitigation Timeout fields.

1. Select **Admin > High Availability**.
2. Click **Timeouts**.
3. In the dialog box, adjust the total heartbeat and mitigation timeout values as needed.

### Synchronize the SMS HA cluster

Synchronize the SMS HA cluster to restore the cluster to a fully-functional state. Synchronizing the cluster synchronizes the database and configuration files to the passive server and restores the primary SMS to Active status. When you synchronize the SMS HA cluster, the SMS client is temporarily disconnected while the SMS server on each node in the cluster automatically restarts.

1. On the HA Cluster Status panel, click **Synchronize**.
   
   If the **Synchronize** button is disabled, it is not necessary to perform a synchronization.

2. In the dialog box, choose to include, or not include, historical event data in the synchronization.
   
   **Note:** If you include historical event data, depending on the size of your event database, it can take hours to synchronize the cluster.

3. Select the synchronization source, either the default source which is the most recent active SMS server or specify another source from the drop-down list.

4. Click **OK**.
   
   When the synchronization completes, the IP address of the original primary SMS appears under the **Active SMS** group with a status of **Active**.

### Deactivate the active SMS server

The most important aspects of the SMS HA cluster are the heartbeat connection and database replication. Periodically, verify that both activities are performing as expected.

If you need to perform maintenance on the active SMS server, for example to swap out a network card, you can invoke a failover on the active node, which deactivates it and activates the passive SMS server. When it is deactivated you can take the node offline, power it off, and perform maintenance on it.

Two methods are available in the Admin - High Availability screen to deactivate the active SMS server:

- **Swap** – Swaps the roles of the SMS HA cluster nodes so that the passive SMS server becomes the active SMS server and the active SMS server is re-configured as the passive server. This process re-synchronizes and restarts the nodes to ensure that HA status of the cluster is maintained. This process involves a temporary disconnect of the client and is temporarily more disruptive than failover. For more information, see *Swap the roles of the SMS HA cluster nodes* on page 641.

- **Failover** – Invokes a failover of the active node in the SMS HA cluster, thereby activating the passive SMS server making it immediately available for use. To bring the failed-over node back online and reinstate a fully functioning HA cluster, you must manually synchronize and restart the deactivated node. For more information, see *Invoke a failover* on page 641.
Swap the roles of the SMS HA cluster nodes

Swap the roles of the SMS HA cluster nodes to promote the Passive SMS to the Active SMS, and reconfigure the Active SMS to the Passive SMS.

1. On the Admin (High Availability) screen, click Swap.
2. Click OK to start the swap process.

Under HA Cluster Status, the IP addresses of the Passive SMS and Active SMS are swapped.

This process can take several minutes, during which time the SMS HA cluster is re-synchronized, nodes are restarted, and the SMS client is temporarily disconnected to reestablish the SMS HA cluster to a fully functional active-passive state. The operational state of the cluster is shown as Configured for the active SMS server and for the passive SMS server until the synchronization process finishes.

Invoke a failover

Invoke a failover to activate the secondary SMS server and deactivate the primary SMS. After you failover the SMS HA cluster, the secondary SMS is now the Active SMS, and the primary SMS becomes the Passive SMS. Failover the cluster when you want to:

- Verify that the initial configuration of the HA cluster works properly
- Perform maintenance on the primary SMS

1. On the Admin (High Availability) screen, click Failover.
2. Select OK

When the failover completes, Active SMS is now the secondary SMS, and the status of the Passive SMS is Failed: User requested. If necessary, perform maintenance on the Passive SMS.

To reactivate your primary node and reinstate the SMS HA cluster to a fully functioning high-availability state, make sure that the primary node is online and then synchronize the SMS HA cluster. See Synchronize the SMS HA cluster on page 640 for more information.

Disable the SMS HA cluster

1. Select Admin > High Availability.
2. Click Disable.

Because a device can be managed by only one SMS, the device always records the IP address and the certificate of the SMS in the HA cluster that manages it. This also prevents another SMS from taking control of the same device. Under normal HA failover conditions, the certificate from the active SMS is copied to the passive SMS and used to manage the devices. If the cluster fails-over or is swapped, then the devices are still seamlessly managed with the same certificate.
If the original passive SMS server becomes the active SMS server and you disable HA, then the SMS displays a dialog with two list panels.

- The left panel identifies devices that will continue to be managed by the currently active (original secondary) SMS.
- The right panel identifies devices that will be unmanaged by the currently active SMS. The devices in this right panel will be managed by the currently passive (original primary) SMS unless you unmanage them and remanage them on the currently active SMS.

3. Click Yes to disable the SMS HA cluster.

When you disable the SMS HA cluster, you break the cluster into separate, independent systems with identical configurations. Ensure one of the SMS servers is rendered inaccessible to SMS clients and devices so that the two servers do not compete with each other. To avoid device management conflicts after SMS HA is disabled, you can either power off the SMS that is not being used or perform a factory reset on it.

**Named resources**

To help you to group and manage the unique identification of resources, the SMS uses named resources. You can define and use named resources within the system for:

- **Devices** — Exception Rules, Servers, Management Routes
- **Events** — Inspection Events (Source and Destination Addresses)
- **Profiles** — Restrictions and Exceptions (Source and Destination Addresses)
- **Responder** — Policies (Inclusions and Exclusions)

Named resources are similar to aliases, and named resource groups are similar to groups of aliases. The SMS supports, and in some cases requires the creation of, named IP addresses, VLAN IDs, and named email addresses. For example, when you configure the SMS to deliver SMTP messages, you must create a named email address group for the recipient list. In another example, if you allow the creation of an external SMS database, you can restrict access to that database instance to only those members included in a specific named IP address group.

**Important:** Access to named resources functionality is based on user roles. Users with SuperUser capabilities can create or edit named resources; users with SuperUser or Admin capabilities can view named resources; users with Operator capabilities do not have access to named resources. See Managing user roles on page 558.

**Resource types**

The SMS uses three types of resources: unnamed, named, and permanent.
### User Capabilities

<table>
<thead>
<tr>
<th>Locked resource</th>
<th>Description</th>
<th>User Capabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unnamed resources</td>
<td>Automatically assigned and used for autocomplete when you enter a value in a field that supports named resources. Select the <strong>Show Unnamed Items</strong> check box to show or hide these values. If you create a filter exception without assigning the source or destination IP address to a named IP address group, then you have created an unnamed IP address group. The IP address group exists on the SMS, but the SMS does not have a way to identify the name of the group.</td>
<td>No</td>
</tr>
<tr>
<td>Named resources</td>
<td>Created by the user.</td>
<td>Yes</td>
</tr>
<tr>
<td>Permanent resources</td>
<td>Created by the SMS and not by the user.</td>
<td>No</td>
</tr>
</tbody>
</table>

**Note:** Named resources are used only on the SMS. In its communication with the device, the SMS sends only the constituent parts of a named resource (IP addresses, CIDR, and email address) to the device. The named resource itself is not sent.

**View whether a named resource is in use**

Click **Show References** to view whether the named resource is currently in use. If it is in use, the SMS displays the respective settings for the named resource.

**Save a copy of a named resource**

Click **Save As** to create a copy of the named resource or named resource group with a different name.

**Delete a named resource**

You cannot delete a named resource if it is currently in use on the SMS. When you click **Delete**, the SMS displays the respective settings for the named resource. You must first remove the named resource from these associated items before the named resource itself can be deleted.
Create or edit a named resource

A named resource is an individual resource, typically created to be included in a named resource group.

1. Select Admin > Named Resources.
2. Depending on the named resource you want to create (or edit), select either the Named IP Addresses tab, the Named VLAN IDs tab, or the Named Email Addresses tab.
3. Below the named resource table (located at the bottom of the screen), do one of the following:
   - Click New to create a new named resource.
   - Select an existing named resource, and click Edit. You cannot edit unnamed or permanent named resources. See Named resources on page 642.
4. Enter a Name for the named resource.
   **Note:** You cannot use special characters or spaces.
5. (Optional) To create a named IP Address:
   a. Select IP Host, and enter the single IP address.
   b. Select IP Subnet, and enter the IP address in CIDR notation.
   c. Select IP Range, and enter the range of IP addresses.
6. (Optional) To create a named VLAN ID:
   a. Select VLAN ID, and enter a VLAN ID from 1 to 4095.
   b. Select VLAN ID Range, and enter the range of VLAN IDs.
7. (Optional) To create a named email address, enter an Email Address.
8. Click OK.

Create or edit named resource groups

You can use named resource groups to simplify assigning actions or notifications to multiple resources on the SMS.

1. Select Admin > Named Resources.
2. Depending on the named resource group you want to create (or edit), select either the Named IP Addresses tab, the Named VLAN IDs tab, or the Named Email Addresses tab.
3. Below the Groups area (located at the top of the screen), do one of the following:
   - Click New to create a new named resource group.
• Select an existing named resource group, and click **Edit**. You cannot edit unnamed or permanent named resource groups. See *Named resources* on page 642.

Select the **Show Unnamed Items** check box to show or hide any unnamed resource groups that exist on the SMS.

4. Enter a **Name** for the named resource group.
    
    **Note:** You cannot use special characters or spaces.

5. To include a resource in the named resources group, select it in the left (Available) list panel, and click the right arrow to move it to the right (Selected) list panel.
    
    **Note:** If the Available list panel is empty, then no named resources of this type have been defined. Click **New** to create an individual named resource. See *Create or edit a named resource* on page 644.

6. (Optional) To remove a resource from the named resource group, select it in the right (Selected) list panel, and then click the left arrow to move it to the left (Available) list panel.

7. (Optional) Select the **Show Unnamed Items** check box to show or hide any unnamed resources that exist on the SMS.

8. Click **OK**.

### Import or export named resources

1. Select **Admin > Named Resources**.

2. Depending on the named resource you want to import (or export), select either the **Named IP Addresses** tab, the **Named VLAN IDs** tab, or the **Named Email Addresses** tab.

3. Below the named resource table (located at the bottom of the screen), do one of the following:
   
   • Click **Import**, browse to and select the file, and then click **Open**. If the file format is valid, the **Finish** button is enabled.
     
     **Note:** The imported file must contain only comma-separated values (CSV) or tab-separated values (TXT), without column headings or spaces in the names.

   • Select an existing named resource, and click **Export**. Browse to the directory in which you want to save the file, enter a filename, and click **Save**.

### Exports and archives

The Export and Archives screen provides a convenient location to store files on the SMS. In the Admin workspace, select Exports and Archives in the navigation pane to display this screen.

When you back up the SMS database or create a snapshot, the SMS client displays these files on the Export and Archives screen. This screen shows the following information for each file:
- Filename – File name, including the file extension.
- Size – File size in bytes.
- Last Modified – Date and time the file was last changed.

Export a file from the SMS exports and archives directory

1. On the Exports and Archives screen, select a file, and then click Export.
2. In the dialog, click Save.

Delete a file from the SMS exports and archives directory

1. On the Exports and Archives screen, select a file, and then click Delete.
2. In the Delete File dialog, click Yes.

To refresh the Exports and Archives list, click Refresh.

IP address identifier

The IP Address Identifier screen allows you to define address groups, enable event monitoring for IP addresses and address groups, and activate lookup services for a specified set of IP addresses. By default, all IP addresses in the network are monitored. You can modify the settings for any IP Address group that is configured for IP Address Identifier, or create new IP address groups containing one or more specific IP addresses to target for monitoring.

The IP Lookup Services enable you to specify and view selected metadata for monitored events associated with a given IP address or host. The IP Address Identifier screen lists address groups that the SMS is configured to monitor, which consists of the information described in the following table.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Order</td>
<td>Order of priority.</td>
</tr>
<tr>
<td>Icon</td>
<td>Icon that distinguishes the event when viewed.</td>
</tr>
<tr>
<td>Name</td>
<td>Name or identifier of the IP address group.</td>
</tr>
<tr>
<td>Address(es)</td>
<td>Addresses included in the IP address group; an asterisk (*) indicates all addresses.</td>
</tr>
<tr>
<td>Geo</td>
<td>Indicates whether Geo Locator lookup service is enabled for the address group.</td>
</tr>
</tbody>
</table>
### Column Description

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NR</td>
<td>Indicates whether Named Resources lookup service is enabled for the address group.</td>
</tr>
<tr>
<td>DNS</td>
<td>Indicates whether DNS lookup service is enabled for the address group.</td>
</tr>
<tr>
<td>User ID</td>
<td>Indicates whether User ID lookup service is enabled for the address group.</td>
</tr>
<tr>
<td>Rep</td>
<td>Indicates whether reputation filter lookup service is enabled for the address group.</td>
</tr>
<tr>
<td>End Point</td>
<td>Indicates whether End Point Attributes lookup service is enabled for the address group.</td>
</tr>
</tbody>
</table>

### Add or edit an IP address ID

1. On the IP Address Identifier screen, click **New**, or select a row, and then click **Edit**.
2. In the New/Edit Ip Addr Id Entry dialog, provide a name for this entry.
3. Leave the **All Addresses** option selected, or select **Specified Addresses**, and then do the following:
   a. Click **Add**, and then select one of the following options:
      1. **Host/Subnet/Range** – add one or more IP addresses, subnets, or ranges.
      2. **Named IP Address Groups** – select one or more named IP address groups.
      3. **Named IP Addresses** – select one or more named IP addresses.
   b. In the dialog, provide the required information, and then click **OK**.
4. Click **Next**, and then provide any custom metadata to be applied to the specified addresses.
   You can select the following options:
   - **End Point Attributes** – Specify operating system and manufacturer.
   - **Network Location** – Specify network location to apply end-point network location metadata.
   - **Custom Attributes** – Specify one or two custom attributes that you describe.
5. Click **Next**, and then choose from the following Decoration options:
   - Select **No Icon**, or click **Apply Icon** and select or import an icon.
   - Select **No Color**, or click **Apply Color** and choose a color.
Note: By default, no color and no icon is applied to the entry.

6. Click **Next**, and then select lookup services to activate for the specified addresses. See *IP Lookup* on page 32.

7. Click **Finish**.

8. Click **OK**.

Note: You can access all the IP Lookup services from the Tools menu. See *Tools* on page 32. You can also use the WhoIs utility to perform a WhoIs query from the Tools menu.

Delete an IP address ID

1. On the IP Address Identifier screen, select an entry in the list.
2. Click **Delete**.
3. In the Confirm Delete dialog, click **Yes**.

Change the priority order for IP address groups

1. On the IP Address Identifier screen, select an entry in the list.
2. Click **Move Up** or **Move Down** to change the order of priority.

   The list changes dynamically to show the new position of the entry in the IP Address Identifier table. The priority order helps you manage the Address Groups.

User ID IP Correlation

Once an Identity Agent is added to the SMS, the SMS will automatically poll the agent and will display the User ID to User IP correlation and security login events. With this data, you can search an IP address to view all historical information. When you first connect the Identity Agent in the SMS, the SMS will automatically poll the domain controller to get the last 15 minutes of historical information.

Note: When the SMS is in FIPS mode, it will not be able to communicate with the Identity Agent. For more information, see *FIPS mode* on page 591.

Polling times

The following table defines the polling times for the security login events and metadata and diagnostics.

<table>
<thead>
<tr>
<th>Item</th>
<th>Polling time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security login events</td>
<td>Every 4-5 seconds</td>
</tr>
<tr>
<td>Item</td>
<td>Polling time</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>----------------------</td>
</tr>
<tr>
<td>Metadata and diagnostics</td>
<td>Every 15 minutes</td>
</tr>
</tbody>
</table>

**Note:** These are the default times. You can update the polling settings in the Identity Agent.

**Note:** You can manage the User ID IP Correlation data maintained by the SMS when you perform Database Maintenance and specify retention parameters for the data. See Database maintenance on page 579.

**High level SMS and Identity Agent configuration process**

There are four steps to configure the Identity Agent in the SMS in order to retrieve User ID IP correlation.

1. **Add the Identity Agents** on page 649.
2. **Create an Agent Group** on page 649.
3. **Select an Identity Agent to be in a group** on page 650.
4. **Enable the Agent Group** on page 650 that will be actively used by the SMS to poll the Identity Agent for User ID IP correlation data.

**Add the Identity Agent**

1. Click **Admin** on the SMS toolbar, and then expand **User Id IP Correlation** in the navigation pane.
2. Click **Identity Agent Groups**.
3. Create an agent by opening the **Identity Agents** tab and clicking **New**.
4. Specify the following information of the Identity Agent:
   - IP address of the hostname
   - Port. The default port is 8443.
   - (Optional) Description or comments about the agent.
5. Click **OK**.

   The agent is added to the Identity Agent table.

**Create an Identity Agent Group**

Each Identity Agent must be added to a group before the SMS can retrieve events. Agents in a group can also be used for redundancy.

1. Click **Admin** on the SMS toolbar, and then expand **User Id IP Correlation** in the navigation pane.
2. Click **Identity Agent Groups**.
3. Create an agent group by opening the **Identity Agents Groups** tab and clicking **New**.

4. Specify the following information of the Identity Agent group:
   - Name of the agent group.
   - Domain name. This information gets automatically retrieved from the identity agent. All agents in a single group must belong to the same domain.
   - (Optional) Description or comments about the agent group.
   - Number of retries before the SMS attempts to contact the next agent in the group.
   - Number of seconds the SMS waits for a connection to the agent.
   - Number of seconds the SMS waits for a failed connection.

5. In the Identity Agents area, select from the available Identity Agents to add to the group.
   - Up to four agents can be added to a group. Use the Up and Down arrows to reorder the priority of the agents. The SMS attempts a connection to only one agent at a time, beginning with the first one in the list.

6. Click **OK**.
   - The Identity Agent group is added to the Identity Agent Group table. Click **Show References** to see which devices reference the group.

### Select an Identity Agent to be in a group

Select an Identity Agent group to use for the User ID IP Correlation.

1. Click **Admin** on the SMS toolbar, and then expand **User Id IP Correlation** in the navigation pane.
2. Click **User Id IP Configuration**.
3. Select an agent group by clicking **Add**.
4. In the User Id IP Configuration area, select from the available Identity Agent groups. Use the Right and Left arrows to add or remove a group. Alternatively, click **New Identity Agent Group** to create a new group.
5. Click **OK**.
   - The Identity Agent group is added to the Identity Agent Groups table.

### Enable Identity Agent group

Enable the Agent Group that will be actively used by the SMS to poll the Identity Agent for User ID IP correlation data.

1. Click **Admin** on the SMS toolbar, and then expand **User Id IP Correlation** in the navigation pane.
2. Click **User Id IP Configuration**.
3. Right-click on an agent group, and then click **Enable**. To disable an Identity Agent group, click **Disable**. A checkmark appears in the Enabled column.

**User ID IP Correlation events**

Once the SMS is configured with the Identity Agent, the SMS automatically polls the agent, and the user login and group information displays in the User ID IP Correlation table. You can use this data to correlate events to user information. This data is used for SMS reports.

You can also search an IP address to view historical information.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time</td>
<td>Specifies the date and time that the event was retrieved by the SMS.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Specifies the IP address of the security login event.</td>
</tr>
<tr>
<td>User Name</td>
<td>Specifies the user name.</td>
</tr>
<tr>
<td>Domain</td>
<td>Specifies the user domains.</td>
</tr>
<tr>
<td>Machine</td>
<td>Specifies the user machines.</td>
</tr>
<tr>
<td>Member of Groups</td>
<td>Specifies all of the groups for the user.</td>
</tr>
</tbody>
</table>

**Note:** You can manage the User ID IP Correlation data maintained by the SMS when you perform Database Maintenance and specify retention parameters for the data. See *Database maintenance* on page 579.

**Unknown user**

The SMS may display "unknown" for the following reasons:

- Any security event that happened before the Identity Agent was installed.
- The user is not logged into a domain that is monitored by an agent which SMS is using.
- The user is logged on a non Windows system
- The user is logged on a system that uses something other than Active Directory for authentication
• Any IPs that are listed in the **Unmapped IPs** area in the Identity Agent.

• A remote IP address outside of your corporate network that cannot be correlated by the Identity Agent.

**Configure a user resolver filter**

1. On the User Resolver panel, click **Configure a User Name Filter**.

2. In the Configure User Names dialog, select the check box to filter out all user names that end with a $ character.

   **Note:** The user name filter option is a convenient way to filter out recurring system events, such as Windows system service events. To filter out all system logons that end with “$$” select the associated check box.

3. Click **Add**.

4. In the Add User Name dialog, specify a User Name and Domain. When the specified user logs on or off, the associated events are ignored for Active Directory monitoring purposes.

5. Click **OK**.

**Geo Locator database**

The SMS uses a geolocation database developed by MaxMind based on their GeoLite City database. The Geo Locator database contains geographical information associated with IP addresses. The Geo Locator lookup service enables the SMS to do the following:

• Correlate the country of origin for host IP addresses associated with events.

• Query the database to view the country location for a specified host name or IP address.

• Display a map showing the country of origin for all IP addresses generating events.

The SMS uses the Geo Locator database to display event details, reporting information, and *IP Lookup results* on page 32.

The Geo Locator Database screen displays the following information:

• **Type** — Type of database file.

• **Date** — Date and timestamp of the current database file.

• **Version** — Version number of the current database file.

The SMS does not automatically download or install the Geo Locator databases. Instead, you must download and install the database files manually from the TMC. The Geo Locator database file available from the TMC is updated on a monthly basis.

**Note:** You can download updated Geo packages from MaxMind at [https://dev.maxmind.com/geoip/legacy/geolite/](https://dev.maxmind.com/geoip/legacy/geolite/). The SMS supports the GeoLite Legacy City database in CSV/zip format.
Download a Geo Locator database file from the TMC

2. Click Releases in the menu bar, and select Software > SMS > Geo Location.
3. Select the most current GeoIP package from the list.
4. On the Download Details page, note any release information in the Message field, and then click Download.
5. On the End User License Agreement page, click Accept.

Import a Geo Locator database file

1. On the Geo Locator Database screen, click Import.
2. In the dialog, locate the database file you downloaded.
3. Select the file, and click OK.
4. In the Import Completed dialog, click OK.

The Lookup button on the Geo Locator Database screen enables you to open the IP Lookup on page 32 utility from this screen.

Licensing

The Licensing page contains information about the status and the availability of Trend Micro TippingPoint products and services for licensed devices. If your SMS has TMC connectivity, you can configure the System Preferences to poll for license entitlement package updates. See TMC Information Share on page 41 for more information.

The TippingPoint License Package panel displays the following license information:

- **Status** – Top-level indicator of the status of your license entitlement package
- **Version** – License entitlement package version
- **Package Timestamp** – Day and time that the current license entitlement package was created
- **Notification Settings** – Current notification options for receiving results of the SMS daily check for license entitlement package issues. Options include email notifications and SMS system log notifications.

**Note:** If you receive license status errors, log in to your TMC account and check for a license entitlement package update. See Licensing details on page 656 and Import a license entitlement package on page 655.
The SMS runs a daily check for licensed capability expiration and other license entitlement package issues. The Notification Settings on the TippingPoint Licensing Package panel allow you to specify whether to receive the results of this check by email or by an entry in the SMS system log. You can specify one, both, or none of these options.

**Trend Micro TippingPoint License Manager**

The license manager, which is accessible from the TMC by navigating to **My Account > License Manager**, allows you to manage the licenses and certificates for your TPS products. This licensing model enables you to attach and detach speed and feature licenses for your TPS devices.

For more information, see the *License Manager User Guide* available from the license manager.

**Default and licensed inspection throughput for TPS devices**

Before a license entitlement package is installed on a device, each device has a limited, default inspection throughput. Contact your sales representative to purchase an inspection throughput license compatible with your device to increase the inspection rate.

Any TPS device inspection throughput license can be assigned to a compatible TPS device. For instance, a 1 Gbps inspection throughput license can be assigned to a 440T, 2200T, or vTPS device. The following table displays both the default inspection throughput and the inspection throughput options available for purchase for each device.

**Table 123. Default and licensed inspection throughput**

<table>
<thead>
<tr>
<th>Device</th>
<th>Default inspection throughput</th>
<th>Purchasable inspection throughput</th>
</tr>
</thead>
<tbody>
<tr>
<td>440T</td>
<td>100 Mbps</td>
<td>250 Mbps, 500 Mbps, 1 Gbps</td>
</tr>
<tr>
<td>2200T</td>
<td>200 Mbps</td>
<td>1 Gbps, 2 Gbps</td>
</tr>
<tr>
<td>8200TX</td>
<td>1 Gbps</td>
<td>3 Gbps, 5 Gbps, 10 Gbps, 15 Gbps, 20 Gbps, 30 Gbps, 40 Gbps</td>
</tr>
<tr>
<td>8400TX</td>
<td>1 Gbps</td>
<td>3 Gbps, 5 Gbps, 10 Gbps, 15 Gbps, 20 Gbps, 30 Gbps, 40 Gbps</td>
</tr>
</tbody>
</table>
### Device Default inspection throughput Purchasable inspection throughput

<table>
<thead>
<tr>
<th>Device</th>
<th>Default inspection throughput</th>
<th>Purchasable inspection throughput</th>
</tr>
</thead>
<tbody>
<tr>
<td>vTPS</td>
<td>100 Mbps</td>
<td>250 Mbps, 500 Mbps, 1 Gbps</td>
</tr>
</tbody>
</table>

**Note:** You must install a vTPS certificate package on a vTPS to activate the capabilities purchased with the vTPS device license package. See vTPS deployment and licensing on page 403 for more information about vTPS license certificate installation.

### SSL inspection licenses

With TOS v5.0.0 and later, SSL inspection is supported on TX Series (8200TX and 8400TX), 2200T, and Virtual TPS (vTPS) security devices. SSL inspection is not supported on the TippingPoint 440T TPS security device.

For more information, see SSL inspection on page 658.

### Edit notification settings

1. On the TippingPoint Licensing Package panel, click **Edit** next to the Notification Settings field.
2. In the License Package Status Notification Settings dialog, select an option to enable it, or clear a selection to disable it.
3. Click **OK**.

### Import a license entitlement package

Complete the following steps to manually import a device license entitlement package.

If your SMS is connected to the TMC, you do not need to manually import the entitlement file. The SMS automatically downloads the entitlement files from the TMC any time there is an update. See TMC Information Share on page 41 for more information.

**Note:** It might take up to 30 minutes for a new license entitlement package to automatically update on the TMC database and for the SMS to reflect the change on the managed devices. Changes to the software, DV, and ThreatDV licenses are made automatically, but changes to the license-designated throughput speed require a device reboot to take effect.

#### To manually import a device license entitlement package

1. Download the entitlement package from the TMC.
   a. Log on to the TMC at [https://tmc.tippingpoint.com](https://tmc.tippingpoint.com).
   b. From the TMC, navigate to **My Account > TippingPoint License Package**.
   c. Download and save the appropriate license entitlement package file to your local system.
2. In the SMS client, open the Admin Workspace.
3. In the left navigation pane, click **Licensing**.

4. On the TippingPoint Licensing Package panel, click **Import**.

5. Select the license entitlement package file to import, and then click **Open**.

   **Note:** You can only import license entitlement files that match a valid device managed by the SMS and visible in the Licensing Details panel. An error message appears if you try to import an invalid entitlement package.

6. Click **OK**.

   The SMS displays the imported license entitlement package in the Licensing Details panel. See *Licensing details* on page 656 for more information.

**Licensing details**

The Licensing Details panel displays status and information for the license on each managed device.

The following information is displayed in the Licensing Details table:

<table>
<thead>
<tr>
<th><strong>Column</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Device/Capability</td>
<td>Displays the devices currently managed by the SMS. Click the expand button next to each device to view the device feature details, including DV updates, maintenance, SSL Inspection, TOS updates, Threat DV, and throughput speed.</td>
</tr>
<tr>
<td>Expiration Date</td>
<td>The license expiration date of each device feature.</td>
</tr>
<tr>
<td>Activation Code</td>
<td>The unique identification number assigned to the hardware, inspection throughput speed, Threat DV, and SSL license components.</td>
</tr>
<tr>
<td>Action</td>
<td>Displays whether a feature is set to ALLOW or DENY.</td>
</tr>
<tr>
<td>Details</td>
<td>Displays detailed information about the feature, including any errors.</td>
</tr>
<tr>
<td>Certificate</td>
<td>The software certificate number.</td>
</tr>
<tr>
<td>Hardware Serial Number</td>
<td>The device hardware serial number.</td>
</tr>
</tbody>
</table>
Expires within

Use the Expires Within field to sort the results in the Licensing Details panel by the expiration dates of the device licenses. Select the drop down list to choose a time range from **One Week** to **Never** or select the start and end time to manually sort the table information by specific dates and times.
SSL inspection

The TippingPoint Threat Protection System (TPS) provides in-line, real-time threat protection for inbound SSL traffic. The TPS manages its own private keys and certificates from the servers it is securing; these can either be stored on the device itself or accessed at run-time from the Security Management System (SMS).

With access to the server certificate and private key, the TPS is a transparent proxy that receives and decrypts SSL data, inspects it by using the Threat Suppression Engine, and then encrypts it before sending it to the actual destination.

Additional considerations

When deploying SSL inspection, consider the following:

<table>
<thead>
<tr>
<th>Consideration</th>
<th>Description</th>
</tr>
</thead>
</table>
| Inbound IPv4 traffic only | The TPS inspects inbound IPv4 traffic, including HTTP and HTTPS traffic. Inbound SSL inspection does not support:  
  • IPv6 traffic, including IPv4 over IPv6 tunneling.  
  • Outbound IPv4 traffic and IPv6 traffic. |
| Tunneled traffic    | Supported SSL encapsulations:  
  • GRE (Generic Routing Encapsulation)  
  • IPv4 (IP-in-IP)  
  • One layer of tunneling only for both GRE and IPv4-in-IPv4  
  SSL inspection does not include support for GTP or IPv6 encapsulations. |
<table>
<thead>
<tr>
<th>Consideration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GRE support includes the mandatory GRE fields. Optional GRE key configuration is also supported, but the key needs to be the same value for both directions. Other optional GRE fields, such as GRE sequence number, are not supported.</td>
<td></td>
</tr>
<tr>
<td>Quarantine hosts and redirecting HTTP traffic to another site</td>
<td>When configuring an Action Set to quarantine hosts, if you also configure the response to HTTP traffic sent from quarantined host to &quot;redirect to the following site,&quot; HTTP traffic from the quarantined host is redirected but HTTPS traffic is not redirected.</td>
</tr>
</tbody>
</table>
| Filter Precedence | The TPS processes filters in the following order of precedence:  
1. Inspection Bypass Rules  
2. Traffic Management Filters  
3. RepDV  
4. Quarantine  
5. Digital Vaccine Filters  
When encrypted traffic is routed through the device and:  
• SSL inspection is configured, the TPS order of precedence applies to the decrypted traffic. The TPS does not quarantine or Digital Vaccine filter traffic without first decrypting the traffic.  
• SSL inspection is not configured, the device performs Inspection Bypass, Traffic Management, RepDV, and quarantine filtering against the encrypted traffic. Digital Vaccine filters are applied, but do not match against encrypted payload. |
<p>| Non-encrypted traffic when SSL is configured | • The TPS will drop non-encrypted traffic flows that match a configured SSL server tuple (destination port and destination IP address) in the SSL profile but send cleartext traffic before starting an SSL handshake (as some protocols allow via <code>STARTTLS</code>). |</p>
<table>
<thead>
<tr>
<th>Consideration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traffic Management filters - Trust action</td>
<td>The TPS continues to proxy the SSL session between the client and the server when HTTPS traffic matches a traffic management filter which is set to Trust (incoming traffic is trusted and not inspected).</td>
</tr>
<tr>
<td>Packet trace</td>
<td>Packet Trace as an action includes the decrypted traffic.</td>
</tr>
<tr>
<td>Traffic capture</td>
<td>Traffic capture by tcpdump does not include the decrypted contents.</td>
</tr>
<tr>
<td>L2FB/ZPHA</td>
<td>When the TPS enters Layer-2 Fallback (L2FB) or Zero Power High Availability (ZPHA), the proxied SSL sessions are cleared.</td>
</tr>
</tbody>
</table>

**Requirements**

Make sure your environment meets the following requirements:

- SSL certificate and private key from the server that hosts the SSL/TLS compliant application.

- A supported TippingPoint TPS device with an SSL Inspection license. With TOS v5.0.0 and later, SSL inspection is supported on TX Series (8200TX and 8400TX), 2200T, and Virtual TPS (performance image only, with RDRAND instruction recommended) security devices. For information about how to deploy the vTPS for SSL inspection, see the vTPS Deployment Guide on the TMC at [https://tmc.tippingpoint.com](https://tmc.tippingpoint.com).

**Note:** SSL inspection is not supported on the TippingPoint 440T TPS security device.

- Cipher suite support – SMS v5.0.0 and later is capable of configuring the following ciphers if your TOS supports them. Older versions of the TOS may have limited cipher support. Profile distribution extended status alerts you to any errors:
  - Protocols:
    - TLS v1.2 (enabled by default)
    - TLS v1.1 (enabled by default)
- TLS v1.0 (enabled by default)
- SSL v3.0 (disabled by default)


- Key exchange:
  - Ephemeral Elliptic Curve Diffie-Hellman with RSA signatures (ECDHE-RSA).
    The ECDHE-RSA cipher suite extends SSL inspection capability to Perfect Forward Secrecy (PFS). ECDHE-RSA is enabled by default.
- RSA (enabled by default)

- Authentication:
  - RSA (enabled by default)

- Encryption:
  - AES256 (enabled by default)
  - AES128 (enabled by default)
  - 3DES (enabled by default)
  - DES (disabled by default)

- MAC:
  - SHA384 (enabled by default)
  - SHA256 (enabled by default)
  - SHA1 (enabled by default)

- VLAN translation cannot be used in conjunction with SSL inspection.

### Manage SSL inspection from the SMS

From the SMS, you can set up and manage SSL inspection. For more information, see the following sections.

### Before you configure SSL inspection

Before you configure SSL inspection, update the SMS settings for SSL inspection.

**Important:** To inspect SSL sessions, the device must be licensed for SSL inspection.

The process is:
The following information provides more details:

- **Update the license package** on page 662
- **Import the license package** on page 662
- **Verify the license package** on page 663
- **Enable SSL inspection** on page 663

### Update the license package

Update the license package to assign an available SSL inspection license to any supported TPS security device. SSL inspection is licensed separately. To request an SSL Inspection license, contact your sales representative.

**Note:** Manage your license package by using the License Manager on the TMC at [https://tmc.tippingpoint.com/TMC/](https://tmc.tippingpoint.com/TMC/). When you log on to the TMC, the License Manager is under **My Account > License Manager**.

### Import the license package

If the SMS is configured to automatically download Digital Vaccine (DV) filters from the TippingPoint TMC, the SMS also downloads the most recent license package within 30 minutes. If your SMS is connected to the TMC, you do not need to manually import the license package.

**To manually import the license package**

1. Log on to the TMC at [https://tmc.tippingpoint.com](https://tmc.tippingpoint.com).
2. In the navigation bar, click **My Account** and select **TippingPoint License Package**.
3. Download and save the license package to your local system.
4. Log in to the SMS.
5. In SMS tools, click Admin.
6. In the left navigation pane, click Licensing.
7. On the TippingPoint Licensing Package panel, click Import.

**Verify the license package**

Verify the SSL inspection license is enabled on each TPS device.

**Important:** To enable the SSL inspection license, you must reboot the device.

**To verify the license package**

1. In the SMS client, open the Licensing screen in the Admin Workspace.
   From the Licensing screen, you can view the Licensing Details panel.
   The Licensing Details panel displays status and information for the license on each managed device.
   Details include device name and IP address, next license expiration date, and license status.

2. To view licensed capabilities for an individual device, select the expand button next to the device.
   If the SSL Inspection feature indicates:
   - **Reboot required**, reboot the device to complete the installation.
   - **Deny**, install a license package with SSL inspection assigned to the device. See Update the license package on page 662 for more information.

**Enable SSL inspection**

From the SMS, enable SSL inspection to activate SSL inspection on the device. While SSL inspection is disabled, you can configure SSL inspection on the device.

**Important:** To enable SSL inspection, the license package on the device must allow SSL inspection. If the device is not licensed for SSL inspection, the SMS displays a notification.

**To enable SSL inspection**

1. Select Devices > All Devices > device-name > Device Configuration.
2. Click the Edit > Device Configuration.
   The Device Configuration dialog opens.
3. Click the SSL Inspection property sheet.
4. To view the SSL ciphers that are supported by a device, click View Supported SSL Ciphers.
   The Supported SSL Ciphers dialog box is displayed.
5. Configure the following options:
SSL Inspection. Select this option to enable the device to inspect SSL sessions. If the checkbox is grayed, verify the license package assigns an SSL inspection license to the device.

Persist Private Keys. Select this option to persist private key information in the system keystore of the device. By default, a managed device automatically retrieves private key information from the SMS but does not persist the information when the device reboots.

**Configure SSL inspection**

Configure SSL inspection to specify the SSL sessions you want the TPS device to inspect. The TPS cannot effectively inspect the encrypted payload of SSL traffic that does not match the SSL inspection profile.

The process is:

1. Secure the SMS certificate repository
2. Import the SSL server certificate and private key
3. Add or edit an SSL server
4. Add or edit an SSL inspection policy
5. Distribute the inspection profile

The following information provides more details:

- Secure the SMS certificate repository on page 664
- Add or edit an SSL server on page 666
- Add or edit an SSL inspection policy on page 667
- Distribute the inspection profile on page 668

**Secure the SMS certificate repository**

Secure the SMS certificate repository by providing a password. If a password already exists for the SMS certificate repository, you can skip this step.

The SMS certificate password protects the private keys in the SMS certificate repository with encryption. When you import certificates with private keys into the SMS certificate repository, the SMS always prompts for the SMS certificate password.
Once you set up the SMS certificate password, keep in mind:

- The SMS does not store the SMS certificate password. You must enter this password every time the SMS server restarts.

- There is no way to recover a lost password. If you lose your password, you must reset your password. Resetting your password deletes all of your private keys in the SMS certificate repository. To resolve this issue, reimport all of your private keys.

**To secure the SMS certificate repository**

1. Go to **Admin > Certificate Management**.
2. Click **Setup Encryption**.
3. Enter and confirm a password.
4. Click **OK**.

   A new RSA key pair is generated after password validation. The new password encrypts the private key of this key pair which encrypts your private keys in your SMS certificate repository.

**Import the SSL server certificate and private key**

From the SMS, import both the SSL server certificate and its private key from the server of interest. The SMS performs basic validation on the status of the certificate itself.

The SMS copies the device certificate to each device that is configured to use the certificate along with the corresponding private key.

Optionally, you can configure each device to persist private key information in the system keystore. For more information, see *Enable SSL inspection* on page 663.

**To import the SSL certificate and private key**

1. Select **Admin > Certificate Management > Certificates**.
2. In the Certificates panel, click **Import** to import a new SSL certificate.

   To update an existing SSL certificate, select the certificate from the list, then click **Import**.
3. Enter the certificate name.

   (Best Practice) Follow a naming convention so that you can easily and reliably assign the correct certificate to an SSL server.
4. Click **Browse** to locate the file.
5. Select the certificate format, either **Base64 Encoded Certificate (PEM)** or **Encrypted Private Key and Certificate (PKCS12)**.

   When selecting:
666

- **PEM/DER** format, the private key must be imported in a separate file. Be sure to select the Include a Private Key checkbox, and then browse to the private key file. If the private key is encrypted, you must also enter the appropriate password in the Password box.

- **PKCS12** format, you must enter the appropriate password in the Password box.

6. Click **OK**.

The appliance imports the certificate and associated private key, and the certificate is displayed in the Device Certificates table.

### Add or edit an SSL server

From the SMS, add an SSL server to specify the SSL server configuration, including the SSL service that is accepted on the SSL detection port.

**Tip:** To view a summary of the existing SSL server configurations, click **Profiles** on the SMS toolbar. Then, in the navigation pane, select **Profiles > Shared Settings > SSL Servers**.

For secure HTTP, IMAP, and POP3 traffic, create a separate SSL server to enable DV filtering on the decrypted SSL service. For example, if the web server accepts POP3S traffic on port 2000, add an SSL server with a Detection Port of 2000 and a Decrypted Service of **POP3** to enable DV filters for POP3.

For other SSL services, such as SMTPS, create an SSL server with a Detection Port that identifies the secure traffic, and a Decrypted Service of **Other**. The TPS applies DV filters to the incoming traffic, but does not apply DV filters to the decrypted SSL service.

To inspect more than one decrypted service on a particular SSL server, define the same server IP for each service you want. For example, you can define a server with IP 1.1.1.1 and port 443 (HTTPS), and another server with IP 1.1.1.1 and port 995 (POP3S), and associate them with the same SSL inspection profile.

**To add or edit an SSL server**

1. Select **Profiles > Shared Settings > SSL Servers**.
2. In the SSL Server tab of the SSL Servers panel, click **New** or **Edit**.
3. In the **SSL Server** tab, specify the following settings:
   - **Name**: Enter the server name, for example, **myapp_pop3**.
     
     (Best Practice) Name the server so that you easily associate it with your web server.
   - **Destinations**: Specify the server IPv4 address or CIDR range.
   - **Detection Ports**: Specify the port range of the encrypted application traffic. For example, if the web server accepts POP3S traffic on port 2000, specify **2000**.
   - **Certificate**: Select the SSL certificate for your web server. You can import a certificate now, or if you have already imported a certificate into the SMS certificate repository, simply choose the one you want.
Decrypted Service: Choose the SSL service that is accepted on the SSL Detection Port to enable filtering for that particular service. If the SSL service you want is not listed, choose Other.

Rekey Interval: Specify the interval, in seconds, that your web server forces renegotiation of the shared SSL key. If your web server does not offer renegotiation of the shared SSL key, leave this blank.

Enable logging: Select this option to enable the TPS to write log information about SSL inspection to the external user disk (CFast or SSD). This option collects detailed logging information and should only be enabled for troubleshooting purposes. For example, enable this option if, after you set up SSL inspection, the TPS device does not see SSL session activity. By default, this option is disabled. For information about viewing log information, see Verify SSL inspection activity on page 669.

Allow compression: Select this option to allow the SSL compression algorithm to be negotiated during the SSL handshake. If your web server does not offer negotiation of SSL compression, disable this option. By default, this option is disabled. If you select this option, and your web server does not offer SSL compression, this setting is ignored.

Send TCP reset to server for blocked sessions: Select this option to always send a TCP reset to the server whenever the TPS blocks an SSL session. This option overrides the TCP reset action set, if enabled, on a DV filter.

(Best Practice) Enable this option so that protected servers can release network resources quickly if flows are blocked. When this option is disabled, the TCP reset action, if enabled on a DV filter, still applies.

4. In the Cipher Suites tab, choose the protocols and algorithms that are supported by your web server.

The Cipher Suite list automatically updates based on your selections. Deselect any cipher suites that you do not want.

5. Click OK.

6. Assign the SSL Server to an SSL inspection policy. See the next section for more information.

Add or edit an SSL inspection policy

On the SMS, update an inspection profile to add an SSL inspection policy. The SSL inspection policy specifies each SSL server that you want to protect, and any SSL client exceptions.

Important: Always distribute an inspection profile with an SSL inspection policy to the inbound virtual segment that receives SSL client requests. When assigned properly, the SSL inspection policy enables the device to proxy (and decrypt) the SSL session between both the SSL client and the device, and between the SSL server and the device. If necessary, update the inspection profile on the corresponding outbound virtual segment to properly filter the decrypted server responses. For more information, see Distribute the inspection profile on page 668.
Tip: To view a summary of the existing SSL server policies, select Profiles > Inspection Profiles > profile name > SSL Inspection Policy.

To add or edit an SSL inspection policy

1. Select Profiles > Inspection Profiles > inspection_profile_name > SSL Inspection Policy.
2. Select Locked to prevent an SMS user from changing the SSL inspection policy directly, or as a child instance in another policy.

   When you select this option, only users with the Lock SSL Filter capability (under Profiles > Profile Management > Profile Filter Management > SSL Filter Management > Lock SSL Filter) can change the SSL inspection policy.

3. In the SSL Inspection Policy panel, click New or Edit.

   The SSL Profile Editor opens.

4. Enter the SSL profile name, for example, myapp_SSLprofile.

   The Add SSL Server Policy dialog box opens.

6. Specify the following settings:
   • **Enable**: Deselect the checkbox to exclude this SSL Server Policy from the SSL inspection profile. By default, this option is selected.
   • **Name**: Specify a policy name, for example, that corresponds to the SSL server configuration.
   • **SSL Server**: Choose a server to include in SSL inspection.
   • **Source Address Exception**: Specify any SSL client IPv4 addresses to exclude from SSL inspection.

7. Click OK.

   You are now ready to distribute the SSL inspection profile. See the next section for more information.

Distribute the inspection profile

From the SMS, distribute the inspection profile to the virtual segment that receives SSL client requests. Make sure that the inspection profile includes an SSL server policy, and that the SSL server policy specifies the SSL server to which the SSL clients connect.

**Important**: The SSL server policy enables the device to proxy (and decrypt) the SSL session between both the SSL client and the device, and between the SSL server and the device. If necessary, update the inspection profile on the corresponding outbound virtual segment to properly filter the decrypted server responses.

For example, if you do not want the device to inspect the decrypted payload in the SSL server response, perform the following steps:
1. Add a user-defined virtual segment that meets the following criteria:
   ◦ Source IP address - Specify the SSL server IP address.
   ◦ Physical segment - Specify the corresponding outbound physical segment. For example, if Segment1 (A > B) receives SSL client requests, specify Segment1 (A < B).
2. Distribute an inspection profile to the virtual segment that disables the Application filters and the Security filters. Or, you can disable all filter categories and filter overrides to maximize the available inspection resources.

To distribute the inspection profile
1. On the Profiles navigation pane, expand Profiles, and then click Inspection Profiles.
2. Select a profile on the Inventory pane, and then click Distribute.
3. To distribute the profile to Inspection Segments:
   • In the Targets section, select the Inspection Segments tab.
   • To Allow Segment Selection, choose one of the following items from the Organize By drop-down box:
     ◦ Segment Group
     ◦ Device
   • Select the appropriate group(s).
4. For a high priority distribution, select the High Priority check box.
5. Click OK.

Note: When you enter a significant number of changes to the filters within a profile, the period of time that is required to distribute the profile increases. If the profile distribution takes too long, a time-out can occur. For assistance with extending the time-out setting to meet your profile distribution needs, contact TippingPoint product support.

After you configure SSL inspection

After you configure SSL inspection, monitor SSL inspection activity to verify the device is inspecting the SSL sessions you want. If you want to restrict access to the SSL configuration, give permissions to SSL inspection.

Verify SSL inspection activity

From the SMS, monitor SSL inspection on the TPS device.

View event information about SSL inspection activity by choosing from the following:
• **Devices > All Devices > device-name > Events > SSL Sessions** displays active session count information for up to 50 SSL sessions. Filter the list to view details for the sessions you want.

• **Devices > All Devices > device-name > Events > Traffic > SSL Decrypted Traffic** displays overall SSL traffic seen and amount inspected.

• **Devices > All Devices > device-name > Events > Traffic > Active SSL Connection Rate** displays the total number of new SSL connections that were created during the 1-minute reporting interval.

• **Devices > All Devices > device-name > Events > Traffic > New SSL Connection Rate** displays the average number of new SSL connections created per second during the 1-minute reporting interval.

To view logging information about SSL inspection, choose **Events > SSL Inspection Logs**. The SSL Inspection log displays SSL session information for the SSL servers with logging enabled, including information about SSL sessions that failed to negotiate SSL parameters. By default, when you add an SSL server, logging is disabled. The SSL inspection log does not contain SSL system errors; check the System log.

**Note:** When you delete an SSL inspection profile or policy, corresponding SSL connections continue to be inspected until the SSL connection closes, but the SSL inspection log incorrectly indicates that the SSL connections have an unknown profile or policy. You can disregard these entries. The device stops logging these connections after the SSL connections close.

If you do not see SSL sessions for a particular server, edit the SSL server to enable logging and then review this log for useful troubleshooting information. When you finish troubleshooting, disable logging on the server.

The SSL Inspection log does not log SSL sessions that are Blocked or Quarantined:

• Both the IPS Block and Alert logs (**Monitor > IPS**) and the Quarantine log (**Monitor > Quarantine**) have an “SSL Inspected” (y/n) column to report on SSL sessions.

  **Note:** If you see an unexpected alert on a profile that inspects outbound SSL traffic, keep in mind that the device proxies (and decrypts) the SSL session between both the SSL client and the device (inbound segment), and between the SSL server and the device (outbound segment). If necessary, update the inspection profile on the corresponding outbound virtual segment to properly filter the decrypted server responses.

• The Reputation Block and Alert logs (**Monitor > Reputation**) do not report on SSL sessions because Reputation is analyzed prior to SSL Inspection.

**Replace a certificate**

Replace an SSL server certificate before it expires. When you replace a certificate, keep these points in mind:

• A certificate with a private key should always be replaced by another certificate with a private key.

• A certificate without a private key should always be replaced by another certificate without a private key.

• The replacement certificate is always new to the SMS certificate repository.
• You must have the *Device X509 Certification Configuration* capability in your user role for all of the devices where the certificate is replaced.

• The SMS replaces the certificate on any applicable devices. If the SMS cannot communicate with a particular managed device, the SMS displays an error message.

**Note:** Certificate replacement requires the *Admin X509 Certificate Management* capability in your user role.

**To replace a certificate**

1. In SMS tools, click **Admin**.
2. In the left navigation pane, click **Certificate Management > Certificates**.
3. Click **Replace**.
   - For certificates with a private key, browse to and open a certificate.
   - For PEM/DER certificates, browse to and open the associated private key.
4. (Optional) Provide a password to encrypt the private key.
5. Click **OK**.

The replaced certificate is saved under the original name with `_REPLACED` appended.

**Add SSL inspection to the user role**

From the SMS, grant permissions to SSL inspection so that an assigned user group can configure SSL inspection. By default, SSL inspection permissions are granted to the Administrator role.

Grant role-based permissions to:

• SSL inspection profiles
• SSL servers
• SSL global settings
• SSL log
• SSL event information

**Note:** Only custom user roles can be edited; the default user roles cannot be edited.

**To update the user role**

1. In SMS tools, click **Admin**.
2. In the left navigation pane, click **Authentication and Authorization > Roles**.
3. Click **New** to create a user role or **Edit** to change an existing role. When creating a new role, select one of the default roles to use as a template base role for the new role.
4. In the Role dialog box, click the **Capabilities** property sheet.
5. In the Capabilities property sheet, under:
   - Profiles > Shared Settings Management, check or uncheck SSL Server Management.
   - Devices > Device Section > Device Management > Event Management, check or uncheck View SSL inspection log.

Grant the user group access to the SSL server

In the SMS, grant the user group access to the SSL servers that you have defined as part of your SSL inspection configuration. By default, a user group has access to all SSL servers, including new SSL servers that have yet to be defined.

To give access to SSL servers

1. In SMS tools, click Admin.
2. In the left navigation pane, click Authentication and Authorization > Groups.
3. Click New to create a group or Edit to change an existing group.
4. In the Group dialog box, click the SSL Servers property sheet.
5. Check or uncheck the SSL servers to which the group has access.
6. Click the Profiles property sheet.
7. Check or uncheck the SSL inspection profiles to which the group has access.

Best Practices

Use this checklist to verify that your SSL inspection configuration conforms to the recommended best practices.

<table>
<thead>
<tr>
<th></th>
<th>To help avoid assigning the wrong certificate and private key to a server, use a naming convention for the certificate, private key, and SSL server. The device does not validate the certificate and private key.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Set role-based access controls to limit access to SSL inspection.</td>
</tr>
<tr>
<td></td>
<td>Check the System log for errors.</td>
</tr>
<tr>
<td></td>
<td>Keep your certificates up-to-date. Whenever you update a certificate on your server, be sure to also import the updated certificate into the device or the SMS. If a certificate expires, the System log generates an error.</td>
</tr>
</tbody>
</table>
Troubleshoot SSL inspection

If SSL clients cannot reach the server, check Traffic Management and Reputation filters to verify the sessions of interest are not being blocked. Traffic Management and Reputation filters are applied before SSL inspection. See the following sections for additional troubleshooting information.

Basic troubleshooting

If SSL clients are reaching the server but the TPS device is not inspecting some or all of the encrypted sessions of interest, perform the following basic troubleshooting steps:

- Check the System Log to determine whether the TPS device is bypassing SSL sessions.
- Check the SSL Server IP and ports.
- Check the server policies on the SSL Profile to verify a source IP exception is not bypassing SSL inspection.
- Check the virtual segments that have been assigned the SSL profile:
  a. If the virtual segment designates a segment, is it the correct segment? For example, is it supposed to be interface 1A or 3A? If it is only one direction, is it the correct direction, such as \( A > B \) or \( A < B \)?
  b. If the virtual segment defines VLANs, are they correct for the SSL Servers?
  c. If the virtual segment defines Source IP Addresses, are the SSL clients coming from those addresses?
  d. Finally, if the virtual segment defines Destination IP Addresses, are the SSL servers in those addresses?

<table>
<thead>
<tr>
<th>To verify</th>
<th>Do this</th>
</tr>
</thead>
<tbody>
<tr>
<td>The TPS is not bypassing SSL sessions</td>
<td>On the device, check the System Log for an entry similar to the following: SSL Inspection reached Critical threshold of Max Concurrent Connections. Action: Allow but bypass Inspection. If the number of concurrent SSL sessions exceeds the maximum threshold as specified by the entry in the System Log, the TPS device does not inspect them. If necessary, reconfigure SSL inspection to reduce the number of concurrent SSL connections.</td>
</tr>
<tr>
<td>To verify</td>
<td>Do this</td>
</tr>
<tr>
<td>--------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>For information about configuring SSL inspection to block SSL sessions that exceed the maximum threshold, contact TippingPoint product support.</td>
<td></td>
</tr>
<tr>
<td>SSL inspection license is installed and valid</td>
<td>For a managed device, see Verify the license package on page 663 for more information.</td>
</tr>
<tr>
<td>SSL inspection is enabled</td>
<td>For a managed device, see Enable SSL inspection on page 663 for more information.</td>
</tr>
<tr>
<td>The correct certificate and key are installed</td>
<td>For a managed device, see Import the SSL server certificate and private key on page 665 for more information.</td>
</tr>
<tr>
<td>The SSL server matches the correct IP address and port</td>
<td>For a managed device, see Add or edit an SSL server on page 666 for more information.</td>
</tr>
<tr>
<td>The profile is applied to the correct virtual segments</td>
<td>For a managed device, see Distribute the inspection profile on page 668 for more information.</td>
</tr>
<tr>
<td>The virtual segment includes the desired SSL server IP addresses and ports</td>
<td>Verify the SSL clients are reaching the SSL server.</td>
</tr>
</tbody>
</table>

**Advanced troubleshooting**

If the basic troubleshooting does not resolve your issue, perform the following steps on the device:

1. Verify the list of inspected SSL sessions. In the LSM, click Monitor > Sessions > SSL Sessions or, from the CLI run the show tse ssl-inspection command.
   
   Entries are only present for the life of the session. If necessary, use the debug np ssl-clear command to forcibly close the SSL sessions. If an entry does not exist, proceed to the next step.

2. Run the debug np stats show npSslInspStats command to check the connection counters. If they are all zero, then it is likely that you have a configuration issue. If there are refused connections, it is also a configuration issue, but there are likely incompatible ciphers or it is trying to use compression when the profile does not support it. For more information, see Basic troubleshooting on page 673.
3. Run the `debug np stats show npSslInspProtocolStats` command and keep the following points in mind:
   - Non-zero entries in "other cipher" indicate a possible unsupported cipher. The other error counters narrow the source of the problem to at least the server or the client.
   - Server connection failures, it is the same possibility, but with the added chance that the server might be asking for a client certificate, which the proxy does not support with this release.

4. Run the `debug np stats show npTcpProxyStats` command to confirm whether the profile and server is configured to correctly match traffic. If the results are all zero, then no traffic is being sent for inspection. If there is any TCP traffic matching a profile, the results are non-zero.
General troubleshooting

The SMS is a complex system. If you cannot find the information you need in SMS documentation, contact your TippingPoint customer support representative. Common issues include:

Login error messages on page 676
Password recovery on page 676
Network changes on page 677
IPS port out-of-service on page 678
SMS error messages on page 678
Modifying filters on page 679
Distributing profiles on page 679
TMC connectivity on page 680
Geo Locator maps do not display correctly on page 681
Export a Tech Support Report on page 681

Login error messages

To recover from errors that occur in the Login dialog box, see the following items.

<table>
<thead>
<tr>
<th>Error message</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connect Failed</td>
<td>• Verify that you entered the correct IP address or fully qualified hostname for the server.</td>
</tr>
<tr>
<td></td>
<td>• Verify that the server is properly connected to the network and that the network is up.</td>
</tr>
<tr>
<td>Can't authenticate! Retype and try again</td>
<td>Verify that you typed the correct username and password.</td>
</tr>
</tbody>
</table>

Password recovery

The SMS provides two ways to reset your password: menu and hotkey. Both methods reset the password for the factory SuperUser account to your SMS serial number.
Reset your password

1. Attach a console to the SMS, and reboot the system.

2. Do one of the following:
   
   • At the prompt, “Press any key to enter the menu,” press a key before the countdown timer reaches 0. The prompt might appear for only a couple seconds during the boot process.
   
   • At the GRUB screen, press an arrow key to select Password Recovery, and then press the Enter key.

   **Note:** The console arrow keys might not work with some KVM equipment. If the arrow keys do not function, try the next method.

   • For SMS version 3.1 and higher, during the boot sequence, when the Starting mgmt startup task is displayed, press the P key (not case sensitive). You must press P within three seconds to trigger password recovery. Starting mgmt occurs shortly after Synchronizing with time server.

   If password recovery is successfully initiated, the console displays the message, “Password recovery enabled.”

   After the SMS completes the boot sequence, the factory SuperUser account is reactivated and the password reset to the serial number of your SMS.

3. While in the console, display the serial number for the SMS:
   
   • Press the ALT + F12 key combination to view the serial number of the SMS. See Managing user accounts on page 562

   • Press the ALT + F1 key combination to return to the previous screen.

4. Log on to the SMS as SuperUser (using the SMS serial number as password) and change your password:
   
   • To change your password through the SMS client, see Managing user accounts on page 562

   • To change your password using the SMS command line interface, see the SMS CLI Reference Guide.

**Network changes**

To change the IP address and gateway for the SMS server, use the CLI and issue the following command: mgmtsettings

1. Change the IP address:

   ```
   set net.ipaddr = SMSipaddr
   ```

   where SMSipaddr is the new IP address.

2. Change the gateway:

   ```
   set net.gateway = gateway
   ```
where `gateway` is the IP address of the new gateway.

3. Restart the network stack:

   ```
   set net.restart = yes
   ```

   The system prompts you to confirm that you want to restart the network stack. Your changes are applied when the network stack is restarted.

   **Note:** You must issue the `set net.restart=yes` command after you modify the IP address or gateway using the `set net` command. Changes to these attributes do not take effect until you issue this command. For more information, see the *SMS CLI Reference Guide*.

### IPS port out-of-service

If the SMS has errors and refuses to locate the device, check the connections on the IPS device. If you use a copper-fiber translator (such as Netgear) and it is disconnected or loose, the IPS device driver will attempt to re-initialize the port several times before timing out and placing the port in an Out-of-Service mode. Netgear does not support auto-negotiation. When you remove the copper cable or the cable is loose, Netgear does not attempt to auto-negotiate with the IPS device.

1. In the SMS client, go to the **Devices** screen.
2. In the **Devices** navigation pane, expand and select a segment on the device.
3. On the **Segments - Segment** screen, locate the auto-negotiation feature for each port.
4. For **Auto-Negotiation**, clear the **Enabled** check box to disable the option.
5. Click **Apply**.

   Leave auto-negotiation disabled. The port should reset.

### SMS error messages

When you modify filters and distribute them to devices, you may encounter error messages. This section describes error messages you may receive and what they mean.

When dealing with error messages, consider the following actions to successfully modify, save, and distribute profiles:

- **Category Settings:** Use category settings if several filters are being set to the same action set. Even if filters in a category have different action sets, you can improve performance by setting the majority of the filters to use the category settings and minority of the filters to use a specific action set.

- **Shared Settings:** When adding exceptions to a large number of filters, you should use Shared Settings where possible.

**Note:** If you continue to have issues distributing profiles with error messages, contact a TippingPoint technical support representative.
Modifying filters

The SMS has a set limit for the number of filters you may change for a profile. This limit promotes better performance for your system. Saving and distributing too many filter changes to a device at one time can cause problems with performance, out of memory errors, and fallback mode for High Availability. You receive these messages when the amount of filters you want to modify and save, be it many or one, exceeds the limit. These filter changes include editing the filter or adding an exception.

**Note:** We recommend modifying and distributing smaller amounts of filters using Category Settings and Shared Settings to help improve performance and distribution of profiles. See *Security filters* on page 169 and *Traffic Management filters* on page 185.

When you modify several filters at one time, you may receive the following error message:

Unable to save these Filters. Saving causes the Profile to exceed the total number of recommended updates.

When you modify and save one filter, you may also receive an error message:

Unable to save these Filters. Saving causes the Profile to exceed the total number of recommended updates.

Distributing profiles

When you modify a number of filters in a profile and distribute it, you may encounter errors with the device. The SMS and IPS devices have limits set for the number of modified filters that you can distribute. This limit promotes better performance for your system. Saving and distributing too many filter changes to a device at one time can cause problems with performance, out of memory errors, and fallback mode for High Availability. You receive these messages in regards to the device.

**Note:** We recommend modifying and distributing smaller amounts of filters, using Category Settings, and Shared Settings to help improve performance and distribution of profiles. See *Profiles* on page 122 and *Traffic Management filters* on page 185.

You may receive the first error message when the total amount of filters you want to distribute exceeds the object receiving limit for the device:

Load failed - Total number of filter updates exceeds recommended limit for this device.

You may receive the second error message when the device fails during distribution. This occurs when the profile installation polling fails due to the device terminating the loading of filters. The loading fails if the amount of filters allowed by the device and the amount sent from the SMS exceed limits:

Load failed - Total number of filter objects exceeds limit for this device. Device terminated filter loading.
These error messages display on the Devices screen

**Note:** Occasionally an IPS device may be busy when the SMS distributes a profile and you receive an error message indicating that the Install failed. In those instances, wait a few moments and try again.

### TMC connectivity

When the SMS attempts to connect to the TMC, the system log displays one of the following messages. The following error messages may appear when you issue the `get health,tmc-valid` command from the CLI.

<table>
<thead>
<tr>
<th>Message</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>OK</td>
<td>SMS was able to connect to both the TMC server and TMC package server</td>
</tr>
<tr>
<td>Cannot connect to server <code>&lt;hostname&gt;</code>: host unreachable</td>
<td>Network error prevented the SMS from contacting TMC</td>
</tr>
<tr>
<td>DNS lookup failure for server <code>&lt;hostname&gt;</code></td>
<td>TMC server hostname could not be resolved</td>
</tr>
<tr>
<td>This SMS is not registered on TMC</td>
<td>TMC is rejecting the SMS connection because the SMS has not been registered with the TMC</td>
</tr>
<tr>
<td>TMC connection error: <code>&lt;error&gt;</code></td>
<td>Other errors connecting to TMC</td>
</tr>
<tr>
<td>TMC Proxy authentication error</td>
<td>TMC proxy is rejecting your authentication</td>
</tr>
<tr>
<td>TMC Proxy: DNS lookup failure for TMC server <code>&lt;hostname&gt;</code></td>
<td>TMC proxy failed the DNS lookup for the TMC server</td>
</tr>
<tr>
<td>TMC Proxy: host <code>&lt;hostname&gt;</code> unreachable</td>
<td>TMC proxy could not contact the TMC server</td>
</tr>
<tr>
<td>Possible proxy DNS lookup error on package server <code>&lt;hostname&gt;</code></td>
<td>TMC package server proxy is likely failing with a DNS error</td>
</tr>
<tr>
<td>TMC package server error: <code>&lt;error&gt;</code></td>
<td>Other errors from the TMC package server</td>
</tr>
<tr>
<td>Message</td>
<td>Meaning</td>
</tr>
<tr>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>Network error connecting to TMC package server &lt;hostname&gt;</td>
<td>SMS could not reach the TMC package server</td>
</tr>
<tr>
<td>DNS lookup failure for TMC package server &lt;hostname&gt;</td>
<td>TMC package server hostname could not be resolved</td>
</tr>
</tbody>
</table>

**Geo Locator maps do not display correctly**

If Geo Locator maps do not display properly, you might need to enable a proxy server for outbound access to TCP connections from your client workstation.

To adjust the proxy settings for your SMS client, add the following lines to the net.properties file at C:\Program Files\TippingPoint SMS Client\jre\lib\net.properties:

- http.proxyHost=yourproxyhostname.com
- http.proxyPort=proxyhostlisteningport (for example: 8080)
- http.nonProxyHosts=localhost|ipaddress

If you need additional assistance, contact TippingPoint customer support (TAC).

**Export a Tech Support Report**

In the SMS, you can collect diagnostic information from an IPS or TPS device by exporting a Tech Support Report (TSR). The TSR collects information from diagnostic commands and log files into a report that TippingPoint product support can use to diagnose issues with the device.

Unlike a TSR created on the device by using the Local Security Manager, the TSR exported by the SMS does not include snapshot information. However, you can create a snapshot from the SMS. For more information about creating a TSR from the Local Security Manager, see the Local Security Manager User Guide.

**Important:** The SMS exports a TSR from TippingPoint IPS and TPS devices only. To create a TSR for another type of TippingPoint security device, use the Local Security Manager.

**To collect diagnostic information for the stack**

1. Use the SMS to export a TSR from each device in the stack.
2. After the report is created, you can save it to your local system.
3. You can then email the file to TippingPoint product support for assistance. For contact information, go to [https://tmc.tippingpoint.com](https://tmc.tippingpoint.com).
To create a Tech Support Report

1. In the SMS tools, click **Devices**.
   - If the device is not a member of a stack:
     a. In the **All Devices** workspace, right-click the shelf-level graphic for the standalone IPS or TPS device and select **Export TSR**.
     b. Click **Export** to download a `tar.zip` file of the report to your local Downloads directory.
   - If the device is a member of a stack:
     a. In the **All Devices** workspace, double-click the stack.
     b. In the left navigation pane, expand the stack to select the stacking device.
     c. Right-click the shelf-level graphic for the stacking device and select **Export TSR**.
     d. Click **Export** to download a `tar.zip` file of the report to your local Downloads directory.
Port information

The SMS requires certain ports to be available for it to perform its tasks. You can make other ports available for optional tasks.

**Required ports**

<table>
<thead>
<tr>
<th>Port</th>
<th>Service</th>
<th>From</th>
<th>To</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>22/TCP</td>
<td>SSH</td>
<td>SMS client</td>
<td>SMS server</td>
<td>CLI management of SMS</td>
</tr>
<tr>
<td>9033/TCP</td>
<td>SMS</td>
<td>SMS client</td>
<td>SMS server</td>
<td>Required for the SMS client to connect to the SMS server</td>
</tr>
<tr>
<td>10042/TCP</td>
<td>SMS</td>
<td>SMS client</td>
<td>SMS server</td>
<td>Required for the SMS client to connect to the SMS server</td>
</tr>
<tr>
<td>443/TCP</td>
<td>HTTPS</td>
<td>SMS client</td>
<td>SMS server</td>
<td>File downloads, such as client installation, exported reports, Web services (if configured)</td>
</tr>
</tbody>
</table>

**Network ports required for the SMS to manage TippingPoint devices**

<table>
<thead>
<tr>
<th>Port</th>
<th>Service</th>
<th>From</th>
<th>To</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>161/UDP</td>
<td>SNMP (agent)</td>
<td>SMS server</td>
<td>IPS</td>
<td>SMS management</td>
</tr>
<tr>
<td>Port</td>
<td>Service</td>
<td>From</td>
<td>To</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>------------</td>
<td>--------------</td>
<td>-------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>443/TCP</td>
<td>HTTPS</td>
<td>SMS server</td>
<td>TPS, IPS, NGFW, DD Analyzer</td>
<td>SMS management</td>
</tr>
<tr>
<td>8162/UDP</td>
<td>SNMP (trap)</td>
<td>IPS</td>
<td>SMS server</td>
<td>SNMP traps from device to SMS</td>
</tr>
<tr>
<td>8163/UDP</td>
<td>SNMP (trap)</td>
<td>IPS</td>
<td>SMS server</td>
<td>SNMP traps from device to SMS</td>
</tr>
</tbody>
</table>

Network ports required for the SMS to access the TMC for software and security updates

<table>
<thead>
<tr>
<th>Port</th>
<th>Service</th>
<th>From</th>
<th>To</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>80/TCP</td>
<td>HTTP</td>
<td>SMS server</td>
<td>Outbound</td>
<td>Digital Vaccine updates from TMC</td>
</tr>
<tr>
<td>443/TCP</td>
<td>HTTPS</td>
<td>SMS server</td>
<td>TMC</td>
<td>Updates from TMC</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>For new SMS installations, this port is the <strong>NEW</strong> default for communication with the TMC</td>
</tr>
<tr>
<td>4043/TCP</td>
<td>HTTPS</td>
<td>SMS server</td>
<td>TMC</td>
<td>Updates from TMC</td>
</tr>
</tbody>
</table>

Network ports required for the SMS to perform WhoIs lookups

<table>
<thead>
<tr>
<th>Port</th>
<th>Service</th>
<th>From</th>
<th>To</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>43/TCP</td>
<td>WhoIs</td>
<td>SMS server</td>
<td>whois.arin.net whois.apnic.net whois.ripe.net whois.lacnic.net</td>
<td>Perform WhoIs lookups</td>
</tr>
</tbody>
</table>
1) The TMC is also available at https://tmc.tippingpoint.com for manual package download. Network ports are not required when you configure the Proxy Server Port to access the TMC for software and security updates.

**Note:** If your security policy requires you to restrict access by hostname, contact TippingPoint for a current list of required hosts.

### Proxy server port information

A proxy server can be used for TMC access if required in your network. To update the TMC proxy connection, go to **Admin > Server Properties > Network > TMC Proxy.**

### Active Response ports

The following tables list and describe the Active Response ports that you should make available. These ports are determined by the use of Active Response on SMS.

<table>
<thead>
<tr>
<th>Port</th>
<th>Service</th>
<th>From</th>
<th>To</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>23/TCP</td>
<td>Telnet</td>
<td>SMS server</td>
<td>External switch</td>
<td>Active Response switch disconnect action</td>
</tr>
<tr>
<td>25/TCP</td>
<td>SMTP</td>
<td>SMS server</td>
<td>Mail server</td>
<td>Active Response email action</td>
</tr>
<tr>
<td>80/TCP</td>
<td>HTTP</td>
<td>SMS server</td>
<td>Remote host</td>
<td>Active Response Web action</td>
</tr>
<tr>
<td>162/UDP</td>
<td>SNMP</td>
<td>SMS server</td>
<td>Remote host</td>
<td>Active Response SNMP action</td>
</tr>
<tr>
<td>162/UDP</td>
<td>SNMP</td>
<td>SMS server</td>
<td>Remote host</td>
<td>Active Response NMS action</td>
</tr>
<tr>
<td>514/UDP</td>
<td>Syslog</td>
<td>SMS server</td>
<td>Syslog server</td>
<td>Active Response Syslog action</td>
</tr>
<tr>
<td>Port</td>
<td>Service</td>
<td>From</td>
<td>To</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>---------</td>
<td>-----------------</td>
<td>-----------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>1812/UDP</td>
<td>RADIUS</td>
<td>External switch</td>
<td>SMS server</td>
<td>RADIUS proxy (required for Active Response switch disconnect action)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>80/TCP</td>
<td>HTTP</td>
<td>External host</td>
<td>SMS server</td>
<td>Trigger Active Response/ via URL, IP correlation lookup, IP or MAC lookup</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>162/UDP</td>
<td>SNMP</td>
<td>NMS server</td>
<td>SMS server</td>
<td>SNMP traps from an SNMP client or NMS server, such as 3Com Network Directory (3ND) to Active Response</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>443/TCP</td>
<td>HTTPS</td>
<td>External host</td>
<td>SMS server</td>
<td>Trigger Active Response via URL, IP correlation lookup, IP or MAC lookup</td>
</tr>
</tbody>
</table>

**Active Response (triggers) for the port availability**

**Note:** Additional ports may need to be opened if they are defined in a Active Response action script.

**HA ports**

The following table lists and describes the High Availability ports that you must make available. In addition to these HA ports, all of the ports listed in Table on page 683 must be open for both primary and secondary SMS servers.

The SMS provides command options that allow you to disable or re-enable HA ports. By default all SMS devices are set to yes or enabled. See “High Availability” in the SMS CLI Reference Guide.
<table>
<thead>
<tr>
<th>Port</th>
<th>Service</th>
<th>From</th>
<th>To</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>22/TCP</td>
<td>SSH</td>
<td>SMS primary</td>
<td>SMS secondary</td>
<td>Secure remote command execution and file replication</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SMS secondary</td>
<td>SMS primary</td>
<td></td>
</tr>
<tr>
<td>1098/TCP</td>
<td>RMI</td>
<td>SMS primary</td>
<td>SMS secondary</td>
<td>JAVA RMI for HA configuration and remote peer administration</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SMS secondary</td>
<td>SMS primary</td>
<td></td>
</tr>
<tr>
<td>1099/TCP</td>
<td>RMI registry</td>
<td>SMS primary</td>
<td>SMS secondary</td>
<td>JAVA RMI for HA configuration and remote peer administration</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SMS secondary</td>
<td>SMS primary</td>
<td></td>
</tr>
<tr>
<td>3306/TCP</td>
<td>MySQL</td>
<td>SMS primary</td>
<td>SMS secondary</td>
<td>Database replication</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SMS secondary</td>
<td>SMS primary</td>
<td></td>
</tr>
<tr>
<td>4444/TCP</td>
<td>RMI</td>
<td>SMS primary</td>
<td>SMS secondary</td>
<td>JAVA RMI for HA configuration and remote peer administration</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SMS secondary</td>
<td>SMS primary</td>
<td></td>
</tr>
<tr>
<td>10042/TCP</td>
<td>SMS</td>
<td>SMS primary</td>
<td>SMS secondary</td>
<td>CLI command replication</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SMS secondary</td>
<td>SMS primary</td>
<td></td>
</tr>
</tbody>
</table>

**Optional ports**

The following table lists and describes the optional ports that you can make available.
<table>
<thead>
<tr>
<th>Port</th>
<th>Service</th>
<th>From</th>
<th>To</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SMS client port</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>23/TCP</td>
<td>Telnet</td>
<td>SMS client</td>
<td>SMS server</td>
<td>CLI</td>
</tr>
<tr>
<td>10042/TCP</td>
<td>SMS</td>
<td>SMS client</td>
<td>SMS server</td>
<td>SMS backup restore</td>
</tr>
<tr>
<td><strong>SMS client browser port</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>80/TCP</td>
<td>HTTP</td>
<td>SMS client</td>
<td>SMS server</td>
<td>File downloads, such as client installation, exported reports, Web services</td>
</tr>
<tr>
<td><strong>SNMP client port</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>161/UDP</td>
<td>SNMP</td>
<td>SNMP client</td>
<td>SMS server</td>
<td>To query SMS SNMP MIBs</td>
</tr>
<tr>
<td><strong>Device ports</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>123/UDP</td>
<td>NTP</td>
<td>IPS</td>
<td>SMS server</td>
<td>Required only if IPS uses SMS for NTP time synchronization</td>
</tr>
<tr>
<td>6343/UDP</td>
<td>sFlow®</td>
<td>IPS</td>
<td>sFlow server</td>
<td>Send sFlow data from TPS devices running TOS v5.0.0 or later and NX-platform IPS devices to one or more sFlow servers</td>
</tr>
<tr>
<td>Port</td>
<td>Service</td>
<td>From</td>
<td>To</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>--------------------------</td>
<td>----------------</td>
<td>----------------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>10043/TCP</td>
<td>SMS provision</td>
<td>IPS</td>
<td>SMS server</td>
<td>Remote Authentication</td>
</tr>
<tr>
<td>443/TCP</td>
<td>URL Threat Analysis</td>
<td>SMS server</td>
<td>DD Analyzer</td>
<td>Send URL data from the SMS to the DD Analyzer</td>
</tr>
<tr>
<td></td>
<td><strong>SMS server ports</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>389/TCP</td>
<td>Active Directory</td>
<td>SMS server</td>
<td>AD server</td>
<td>SMS AD LDAP authentication</td>
</tr>
<tr>
<td>636/TCP</td>
<td>Active Directory</td>
<td>SMS server</td>
<td>AD server</td>
<td>SMS AD LDAP over SSL authentication</td>
</tr>
<tr>
<td>3306/TCP</td>
<td>Database</td>
<td>SMS server</td>
<td>Any</td>
<td>External database access</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>External server</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>External replication</td>
</tr>
<tr>
<td>53/TCP/UDP</td>
<td>DNS</td>
<td>SMS server</td>
<td>Name server</td>
<td>Name resolution</td>
</tr>
<tr>
<td>135/TCP</td>
<td>ID correlation</td>
<td>SMS server</td>
<td>AD server</td>
<td>SMS AD authentication</td>
</tr>
<tr>
<td>239/UDP</td>
<td>IP2ID</td>
<td>SMS server</td>
<td>IPS (A10)</td>
<td>IDsentrie</td>
</tr>
<tr>
<td>111/TCP/UDP</td>
<td>NFS</td>
<td>SMS server</td>
<td>File server</td>
<td>Report export, database backup</td>
</tr>
<tr>
<td>369/TCP/UDP</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2039/TCP/UDP</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Port</td>
<td>Service</td>
<td>From</td>
<td>To</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>---------</td>
<td>----------------</td>
<td>-----------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>123/UDP</td>
<td>NTP</td>
<td>SMS server</td>
<td>NTP server (time source)</td>
<td>Time synchronization from external NTP server</td>
</tr>
<tr>
<td>1812/UDP</td>
<td>RADIUS</td>
<td>SMS server</td>
<td>RADIUS server</td>
<td>SMS user authentication</td>
</tr>
<tr>
<td>49/TCP</td>
<td>TACACS+</td>
<td>SMS server</td>
<td>TACACS+ server</td>
<td>SMS user authentication</td>
</tr>
<tr>
<td>137/TCP/UDP</td>
<td>Samba</td>
<td>SMS server</td>
<td>File server</td>
<td>Report export, database backup</td>
</tr>
<tr>
<td>138/TCP/UDP</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>139/TCP/UDP</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1512/TCP/UDP</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>25/TCP</td>
<td>SMTP</td>
<td>SMS server</td>
<td>Mail server</td>
<td>Email notifications, such IPS events, Active Response</td>
</tr>
<tr>
<td>514/UDP</td>
<td>Syslog</td>
<td>SMS server</td>
<td>Syslog server</td>
<td>SMS audit and syslog</td>
</tr>
</tbody>
</table>
Reputation information

The TippingPoint Reputation Database contains records of suspect IP addresses, domain addresses, and URLs with tagged entries such as reputation score and geographic location.

Database entries are added manually by users, automatically by ThreatDV, or they are imported from CSV files. See Reputation filters on page 175 and Reputation database on page 210.

Reputation import rules

The SMS enables you to enter data in the Reputation Database by importing a file. This section describes rules you must follow when importing data to the Reputation Database.

Note: The examples assume that Country, Approved, and Comment tag categories are defined and that China, Mexico, and United States are defined values for the Country tag category.

Format rules

• For IP and DNS entries, the import file must be in comma-separated value (CSV) format; each line consists of one or more fields separated by commas.

• For URL entries, the import file must be delimited by pipes (|) instead of commas. Limit the number of URL entries to 100,000 per TPS device.

• Each line represents one entry, and entries must not span lines.

• Any line that has a first non-white space character of “#” is considered a comment. Comment lines are discarded during import. There is no support for inline comments.

• The import file may not contain any blank lines within the body; blank lines after the last line are ignored.

• A field may be enclosed in double-quotes; this is mandatory when a value contains a comma that should not be treated as a field separator.

• To represent a double-quote character within a quoted value, use two double-quotes.

RIGHT

1.2.3.0/24,Country,United States,Approved,yes
2.3.0.0/16,Country,Mexico,Approved,no,Comment,"This comment ""contains"" quotes"

WRONG

1.2.3.0/24|Country|United States|Approved|yes
1.2.3.0/24,Country,United States,Approved,yes,2.3.0.0/16,Country,Mexico,Approved,no
#2.3.0.0/16,Country,Mexico,Approved,no
2.3.0.0/16,Country,Mexico,Approved,no,Comment,"This comment "contains" quotes"

Tag category rules

• Any tag categories that appear in the import file must exist on the SMS prior to the import.
• Except for yes/no tag categories, character case is significant in all tag category names and tag values.
• For yes/no tag categories, the text “yes”, regardless of case, denotes a yes value. All other values are considered no.
• Empty pairs of fields are ignored. If a tag category field is empty, an error occurs and the entry is not imported. If a tag value field is empty, the corresponding tag category is discarded and the next field of the entry is processed; it is equivalent to the tag category not appearing on that line at all.
• Tag category/value pairs need not appear in the same order on each line. It is not necessary that every entry specify every tag category, or even the same tag categories as other entries in the file.

RIGHT
2.3.0.0/16,Country,Mexico,Approved,no
2.3.0.0/16,Approved,no,Country,Mexico

WRONG
1.2.3.0/24,COUNTRY,united states,Approved,yes
3.4.5.0/24,Country,China,Approved,y
1.2.3.0/24,,United States,Approved,yes
2.3.0.0/16,Country,Mexico,,yes

Address rules

• The first field on each line must be the IPv4 address, IPv6 address, DNS name, or URL for that entry. The remaining fields on a line are optional. If present, remaining fields are processed as tag category/tag value pairs.
• Only one type of address (IPv4, IPv6, DNS domain name, or URL) can be contained in the file; mixing of types within a file is not allowed.
• A DNS entry matches any lookups that contain the specified string. For example, foo.com matches foo.com, www.foo.com, and images.foo.com.

**Note:** To specify an exact DNS entry match, enclose the DNS name in square brackets. For example, [foo.com] matches only foo.com, and does NOT match www.foo.com or images.foo.com.

• CIDR values are normalized. That is, any bits outside the portion of the address specified by the prefix length are changed to zero. For example, 192.168.66.127/24 are stored as 192.168.66.0/24.

**RIGHT**

foo.com,Country,United States,Approved,yes
1.2.3.0/24,Country,United States,Approved,yes
2001:0db8:85a3:0042:1000:8a2e:0370:7334

**WRONG**

Country,United States,foo.com,Approved,yes
1.2.3.0/24,Country,United States,Approved,yes
fc01:a63:1::/64,Country,China,Approved,yes
## SMS encryption protocols, algorithms, and cipher support

The following table lists the SMS encryption protocols, algorithms, and supported ciphers.

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Ciphers/Algorithms</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>443</td>
<td>TLSv1.0</td>
<td>TLS_RSA_WITH_AES_128_CBC_SHA</td>
<td>HTTPS service</td>
</tr>
<tr>
<td></td>
<td>TLSv1.1</td>
<td>TLS_RSA_WITH_AES_128_CBC_SHA256 (only supported with TLSv1.2)</td>
<td>• SSL provided by SunJSE</td>
</tr>
<tr>
<td></td>
<td>TLSv1.2</td>
<td></td>
<td>• Encryption algorithms provided by SunJCE (Non-FIPS) and NSS (FIPS)</td>
</tr>
<tr>
<td></td>
<td>SSLv2Hello</td>
<td>TLS_RSA_WITH_AES_128_CBC_SHA256 (only supported with TLSv1.2)</td>
<td>• SSL provided by SunJSE</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Encryption algorithms provided by SunJCE (Non-FIPS) and NSS (FIPS)</td>
</tr>
<tr>
<td>10042</td>
<td>TLSv1.0</td>
<td>TLS_RSA_WITH_AES_128_CBC_SHA</td>
<td>Client-server communication</td>
</tr>
<tr>
<td>9033</td>
<td>TLSv1.1</td>
<td>TLS_RSA_WITH_AES_128_CBC_SHA256 (only supported with TLSv1.2)</td>
<td>• SSL provided by SunJSE</td>
</tr>
<tr>
<td></td>
<td>TLSv1.2</td>
<td></td>
<td>• Encryption algorithms provided by SunJCE (Non-FIPS) and NSS (FIPS)</td>
</tr>
<tr>
<td>10043</td>
<td>TLSv1.0</td>
<td>TLS_RSA_WITH_AES_128_CBC_SHA</td>
<td>Device provision manager (device remote authorization)</td>
</tr>
<tr>
<td></td>
<td>TLSv1.1</td>
<td>TLS_RSA_WITH_AES_128_CBC_SHA256 (only supported with TLSv1.2)</td>
<td>• SSL provided by SunJSE</td>
</tr>
<tr>
<td></td>
<td>TLSv1.2</td>
<td></td>
<td>• Encryption algorithms provided by SunJCE (Non-FIPS) and NSS (FIPS)</td>
</tr>
<tr>
<td></td>
<td>SSLv2Hello</td>
<td></td>
<td>• SSL provided by SunJSE</td>
</tr>
<tr>
<td>22</td>
<td>SSH-2</td>
<td>aes128-ctr</td>
<td>• SSH provided by OpenSSH</td>
</tr>
<tr>
<td></td>
<td></td>
<td>aes192-ctr</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>aes256-ctr</td>
<td></td>
</tr>
</tbody>
</table>
When the SMS is in FIPS mode, it does not support SSLv2 formatted hello, SSLv3, and TLSv1.2. The SMS does not support SSLv2 protocol at any time.

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Ciphers/Algorithms</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Encryption algorithms provided by OpenSSL</td>
</tr>
</tbody>
</table>