TREND MICRO™

4.4.0 TippingPoint™ Security Management System (SMS)

User Guide

Enterprise network security management system for centralized global vision and security policy control.

Security Management System User Guide

Version 4.4.0

November 2016

Legal and notice information

© Copyright 2016 Trend Micro

Trend Micro 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 shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

This document contains proprietary information, which is protected by copyright. No part of this document may be photocopied, reproduced, or translated into another language without the prior written consent of Trend Micro. The information is provided "as is" without warranty of any kind and is subject to change without notice. The only warranties for Trend Micro 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 shall not be liable for technical or editorial errors or omissions contained herein.

TippingPoint®, the TippingPoint logo, and Digital Vaccine® are registered trademarks of Trend Micro. Vertica Copyright © 2016 Hewlett Packard Enterprise Development Company LP. All other company and product names may be trademarks of their respective holders. All rights reserved. This document contains confidential information, trade secrets or both, which are the property of Trend Micro. No part of this documentation may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from Trend Micro or one of its subsidiaries.

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

TippingPoint Security Management System (SMS) User Guide

Contents

About this guide....1

Target audience....1

Related documentation....1

Conventions....1

Product support....3

Getting started....4

SMS components....4

Installation....5

SMS server home page....5

Log in to the SMS server home page....5

Download SMS client software....6

View or download reports....6

View reports from the SMS website....6

View or download documentation....7

View or download exports and archives....7

View or save exported files....7

Connect to the TMC....7

SMS client....7

Install the SMS client....7

Install the SMS client....7

Important information when using a Mac OS X to host an SMS client....8

Log in to the SMS....9

Log in to the SMS....9

View notifications....9

SMS dashboard....10

Main user interface....10
Menu bar....12
SMS toolbar....12
Workspace....12
Navigation pane....13
Content pane....13
Features....13
Auto complete....13
Tabbed views....13
Table filtering....13
Expandable table columns....14
Table column controls....14
Realtime data....14
Named resources....14
IDResolver....14
Right-click menus....15
System preferences....15
Security preferences....15
Configure security preferences....15
Device SNMP....16
Configure device SNMP preferences....16
Device communication....17
Configure device communication preferences....17
Dashboard preferences....17
SSH client preferences....18
Change the SSH client setting....18
Banner message preferences....18
Configure banner message preferences....18
Configure PCAP download preferences....19
Report preferences....19

Software updates....19
Install TOS updates....20
Download a TOS update....20
Distribute a TOS update....20
Download, activate, and distribute Digital Vaccines....20
Download a Digital Vaccine from the TMC....21
Activate a Digital Vaccine....21
Distribute a Digital Vaccine to one or more devices....21
Install SMS updates....21
Download an SMS update from the TMC....22
Migrate to another SMS version....22
Manage your system....22
Add a device to the SMS....22
Tools....24
IP Lookup....24
Use the IP Lookup utility....25
TMC....25
Access the TMC....25
ThreatLinQ....26
Diagnostics....26
Log Utils....27
Create a logs zip file....27
Edit logging levels....27
Hotfixes....28
Install a hotfix....28
Rolling back to a previous software hotfix....28
Bookmarks....28
Generate bookmark string....28

Users on LDAP....29
IDResolver....29
Configure and enable IDResolver....29
Query IDResolver....29
Dashboard....30
Dashboard palette....30
Default dashboard configuration....31
Dashboard gadgets....31
Health and Status gadgets....32
Task Status gadgets....33
Inspection Event gadgets....33
Event Rate gadget....33
Security gadgets....34
Reputation gadgets....35
Application gadgets....35
User gadgets....36
Firewall gadgets....37
Customize the SMS dashboard....38
Select a dashboard theme....39
Change the dashboard layout....39
Restore dashboard defaults....39
Add or remove a gadget....39
Configure a gadget....40
Events....41
Navigate the Events workspace....41
Inspection events....42
Criteria panels....42
Inspection Events table....42

Firewall events....44
Monitor events....46
Monitor inspection or firewall events....46
Right-click options from the events table....47
Customizing display options....50
Events display....50
Severity level....51
Table properties....51
Customize table property settings....51
Add a comment....51
Edit a comment....52
Viewing event details....52
Edit a geographic filter....55
View geographic filter description....55
View event details....56
Reputation information....56
TMC ThreatLinQ charts and graphs....56
Packet trace....57
Packet trace options....57
Right-click packet trace menu options....57
External packet trace viewer....57
View the packet trace....58
Save packet trace files....58
Download packet trace files to the SMS....58
Configure packet trace view settings....58
Exporting query results....59
Export query results....59
ThreatLinQ....59
Saving queries....59
Open a saved query....60
Edit a saved query....60
Delete a saved query....60
Filter criteria....60
Create an inspection query with filter criteria....61

Filter taxonomy criteria..... 62
Create a query with filter taxonomy criteria..... 63
Network criteria (Inspection Events)..... 63
Create a query with network criteria..... 64
User info criteria (Inspection Event viewer)..... 65
Create a query with user information criteria..... 66
Device/segment/rule criteria..... 66
Create a query with device segment criteria..... 67
Tuning event filters (Inspection events)..... 67
Filter modifications..... 67
Application, transaction, and user criteria (Firewall Events)..... 68
Add application, transaction, and user criteria..... 69
Edit application criteria..... 69
Firewall policy criteria..... 70
Create a firewall query with filter criteria..... 70
Device, Segment/Interface criteria..... 70
Network criteria (Firewall Events)..... 71
Create a firewall query with network criteria..... 71
Schedule, Service Criteria..... 71
Create a query with schedule or service criteria..... 71
Network Address Translation criteria..... 72
Users criteria (Firewall Events)..... 72
Event criteria (Firewall Events)..... 72
Threshold filter state..... 72
Right-click options..... 72
Edit a traffic threshold filter..... 73
Reset a traffic threshold filter..... 73
Reset all traffic threshold filters..... 74
SSL Inspection Logs..... 74

Reports..... 75

Navigate the Reports workspace..... 75

Templates..... 76

Report permissions..... 76

AD User reports..... 76

Inspection criteria panels..... 76

Firewall templates..... 78

Firewall criteria panels..... 79

Reputation templates..... 80

Reputation criteria panels..... 81

Rate Limit templates..... 82

Rate Limit criteria panels..... 82

Device Traffic templates..... 83

Device Traffic criteria panels..... 83

Traffic Threshold templates..... 84

Traffic Threshold criteria panels..... 84

Advanced DDoS templates..... 86

Advanced DDoS criteria panels..... 86

Executive reports templates..... 87

Executive report criteria panels..... 87

Traffic Analysis templates..... 89

Traffic Analysis criteria panels..... 89

Run a report..... 90

Run a report..... 91

Clear filters..... 92

Customize the criteria panels..... 92

Change the criteria panels that display on a report....92
Customize a query....93
Create a custom query for a report....93
Saved reports....93
Create a saved report....94
Run a saved report....95
Edit a saved report....96
Save as a rew report....96
Report results....96
Open a saved report....96
Edit result settings and permissions....97
Delete a saved report....97
Export report results....98
Export a report result....98
Report schedules....99
Create a new schedule....99
Edit an existing schedule....100
Delete a schedule....100
All schedules....100
Edit a report schedule....100
Delete a report schedule....101
Profiles....102
Profile support areas....103
Planning and using profiles....103
Navigation and menu options....103
Global search....105
Shared settings....105

Action sets....106
Create or edit an action set....107
Default action sets....108
Manage action sets....108
Flow control....108
Notifications....109
Packet trace....110
Quarantine settings....110
Quarantine exceptions....110
Application groups....111
Create or edit an application group....111
Notification contacts....112
Create or edit an email notification contact....113
Create or edit an SNMP notification contact....114
Alert aggregation for notifications....114
Aggregation period....115
Set aggregation settings for global contacts....115
Schedules....115
Create a schedule....115
Edit a schedule....116
Delete a schedule....116
Security zones....116
Create and edit security zones....117
Services....117
Add a non-standard port....118
Delete a non-standard port....118
Add a new service....118
Service groups....119
Create and edit service groups....119
SSL Servers....120
SSL servers....120
Add or edit an SSL server....120
Refresh certificate status....121

Refresh certificate status....121
Inspection profiles....121
Inventory pane....122
Distribution progress pane....123
Management tasks....123
Import profiles....124
Import a profile....125
Export profiles....126
Export a profile....126
Distribute inspection profiles....127
Segment groups....127
Required distributions....127
DV and DV Toolkit version verification....127
High/low priority distributions....128
Distributing profiles....128
Manual profile distribution....128
Distribute an inspection profile manually to inspection segments and firewall devices....128
Distribute multiple profiles....129
Distribute multiple profiles....129
Cancel a distribution in progress....130
Creating new profiles....130
Deployment mode....131
Inheritance....132
Create a new profile....132
Use the ‘Save As’ option to copy a profile....133
Deleting a profile....133
Compare profiles....133
Compare profiles....133
View profile details....134
Details view....134
Profile distribution schedule....135
Distribution details....135
Versions tab....136
View profile details and version options....137
Edit profile details....137
Create a snapshot of a profile version....138
View profile version details....138

Activate a profile version ... 138
Search options ... 139
Global search ... 139
Search ... 139
Find ... 140
Default inspection profile ... 140
Profile overview ... 140
Profile settings ... 140
Security filter ... 141
Create or edit a security filter profile restriction ... 141
Create or edit a security filter exception ... 142
Delete a security restriction or exception ... 142
Application filters ... 142
Application filter categories ... 144
View and edit application filter details ... 148
Edit the state or action set for application filter category settings ... 148
Custom filter exceptions ... 148
Create or edit application filter restrictions ... 149
Delete application restrictions ... 149
Create or edit application filter exceptions ... 149
User defined filters ... 150
Advanced DDoS filters ... 151
Advanced DDoS configuration ... 156
Create or edit an Advanced DDoS filter ... 157
Traffic Threshold filters ... 158
Create or edit a Traffic Threshold filter ... 159
Reputation filters ... 160
Geographic filters ... 160
Any country ... 161
Inclusions and exclusions ... 161
Reputation filters table ... 161
Management tasks ... 163
Right-click options ... 163
Reputation settings ... 164
Edit Reputation settings ... 164
Create a Reputation filter ... 165

Edit a Reputation filter 165
Create a Geographic filter 165
Edit a Geographic filter 167
Delete a Reputation or Geographic filter 167
Change the precedence of a Reputation or Geographic filter (move up/down) 168
Create or edit Reputation filter exceptions 168
Create or edit domain name exceptions 169
Traffic Management filters 169
Edit a Traffic Management filter 169
Firewall profiles 170
Manage firewall profiles 171
Import a firewall profile 172
Create a new profile 172
Create a snapshot of a firewall profile version 173
Activate a firewall profile version 173
Delete a firewall profile 173
Firewall rules 173
Add items to firewall rules 174
Create firewall rules 174
Captive portal rules 177
Create a captive portal rule 177
Special captive portal rules to allow blocked users to log out 178
NAT rules 178
Create source NAT rules 178
Create destination NAT rules 180
Distribute firewall profiles 181
Distribute profiles to firewall devices 181
Cancel a distribution in progress 182
Digital Vaccines 182
DV Inventory tab 182
Download and manage Digital Vaccine packages 185
Scheduled Distributions tab 185

Importing DV packages ... 186
Auto-download and distribute a DV, virtual DV, or Auxiliary DV ... 186
Import a DV, virtual DV, or Auxiliary DV package ... 187
Download a DV, virtual DV, or Auxiliary DV package ... 187
Managing DV packages ... 188
Delete a DV, virtual DV, or Auxiliary DV package ... 188
Activate a DV, virtual DV, or Auxiliary DV package ... 188
View details of a DV, virtual DV, or Auxiliary DV package ... 188
Search filters in a DV package ... 189
Distributing DV packages overview ... 189
Scheduled distributions ... 189
Distribute a DV, virtual DV, or Auxiliary DV package ... 189
Stop distribution of a DV, virtual DV, or Auxiliary DV ... 190
Create a new scheduled distribution ... 190
Edit a scheduled distribution ... 190
Auxiliary DV ... 191
ThreatDV ... 191
Auxiliary DV screen ... 191
Auxiliary Digital Vaccine tasks ... 193
Import Auxiliary DV packages ... 193
Manage Auxiliary DV packages ... 193
Uninstall an Auxiliary DV ... 193
Distribute Auxiliary DV packages ... 194
Clear an obsolete distribution listing for Auxiliary DVs ... 194
Digital Vaccine Toolkit ... 194
Associate DV Toolkit packages with devices and profiles in the SMS ... 194
Create DV Toolkit packages ... 195
Use multitenancy to limit access to DV Toolkit packages ... 195
DV Toolkit Packages screen ... 195
Import a DV Toolkit package ... 197

Activate a DV Toolkit package....198
Search for DV Toolkit packages from an Inspection Profile....198
Distribute a DV Toolkit package to the device....200
View DV Toolkit details....201
Remove DV Toolkit packages from the device and the SMS....201
Deactivate a DV Toolkit package on the SMS....201
Uninstall a DV Toolkit package from the device....202
Delete a DV Toolkit package from the SMS....203
Reputation database....203
Reputation database interface....203
Summary tab....203
Database summary....203
Activity tab....204
Sync progress....204
Tasks....204
View Reputation database details for distribution to device targets....205
Perform a full synchronization of the Reputation database....205
Stop a synchronization of the Reputation database....205
Clear obsolete distribution entries....206
Tag Categories tab....206
Import all tag categories....207
Export all tag categories....207
Add or edit a Reputation tag category....208
Delete a Reputation tag category....208
ThreatDV....208
View license details for a ThreatDV reputation filter....209
Enable or disable automatic DV download for a Reputation DV....209
Import a ThreatDV package....210
Reset a Reputation DV....210
User-provided entries....211
Import entries into the Reputation database....211

Import user-provided entries to the Reputation database from a file..... 211
Adding user-provided entries to the Reputation database..... 212
Add a user-provided entry (addresses only) to the Reputation Database..... 212
Add an address, tag category, or tag value to the Reputation database..... 212
Exporting user-provided Reputation entries..... 212
Export a user-provided entry from the Reputation Database..... 213
Reputation database search..... 213
Search criteria..... 213
Search results..... 214
Search for entries in the Reputation database..... 214
Edit bulk (all searched database entries)..... 215
Delete bulk (all searched database entries)..... 215
Edit a user-provided entry in the Reputation database..... 216
Edit multiple user-provided entries in the Reputation database..... 216
Scheduled distributions..... 216
Create a new profile distribution..... 217
View a profile schedule..... 217
Edit a profile schedule..... 217
Vulnerability Scans..... 217
Overview..... 218
Vulnerability scans..... 218
To import a CSV file..... 219
To import a file using a custom converter..... 219
Show CVEs..... 220
Profile Tuning..... 220
Functions of the Profile Tuning Wizard..... 220
Dialog Page 1..... 220
Dialog Page 2..... 220
Dialog Page 3..... 221
Dialog Page 4..... 221
Comments..... 221
Delete..... 222
CVE Search..... 222

Scan Criteria pane..... 222
CVE Criteria pane..... 222
CVE Search Results..... 222
Details..... 223
Details Dialog..... 224
Vulnerability Criteria..... 224
Vulnerability Criteria search pane..... 224
Vulnerability Criteria Search Results..... 225
Edit Filter Dialog..... 225
System preferences..... 226
Responder..... 227
Before you begin..... 227
Responder configuration..... 228
Working with the Responder (Response History)..... 228
Monitoring and managing responses..... 230
Filter responses..... 230
Create a named resource..... 231
Close a response..... 231
View events for a response..... 232
Responder actions..... 232
Notification actions..... 233
Reputation entry (blacklist) actions..... 233
IPS Quarantine actions..... 234
Switch actions..... 234
Creating or editing response actions..... 235
Create or edit a response action..... 235
Email response action..... 235
Move quarantined host onto a VLAN response action..... 236
NMS trap response action..... 236
Reputation entry response action..... 237

SNMP trap response action....238
Syslog response action....238
Web response action....239
IPS quarantine response action....240
Delete a response action....241
Response action scripts....241
Import an active responder action script....241
Export an active responder action script....241
Delete an active responder action script....241
Policies....242
Policy setup options....242
Policy initiation....242
Policy remediation communication (timeout)....243
Inclusions and exclusions....243
IP correlation and thresholding....243
Actions....244
IPS destinations....244
Default response policy....244
Edit the default response policy....244
Manual response....246
Initiate a manual response....246
New response policies....246
Create or edit a new response policy....246
Delete a new response policy....248
Responder network devices....248
Auto discovery of switches....249
Configure auto discovery of network devices....249
Adding a switch....250
Add or edit a switch....250

RADIUS....251
Configure RADIUS....251
IP Correlation....252
Configuring IP Correlation....252
Network mapping using the GUI....253
Add/edit network mapping....253
Network mapping – bulk load via service mode....253
IP Correlation configuration – RFC1213....253
IP Correlation configuration – 3Com Network Director or 3Com Enterprise Management Suite....254
IP Correlation configuration – external Web API....254
IP Correlation query configuration....254
Build IP Correlation queries over HTTP(S)....254
IP Correlation web services....255
Add/edit web services....255
Control web service precedence....255
Testing IP Correlation....256
Perform a test of IP Correlation....256
Managing manual response policies....256
Managing responder through an external/third-party interface....257
Devices....258
The Devices workspace....258
Devices (All Devices)....259
Member Summary....260
Network summary....261
Events summary....261
Blocked and rate limited streams....262
Firewall sessions....263
Trusted streams....263
Quarantined hosts....264
Adaptive Filter....265
System health summary....266

Performance....266
Packet statistics....267
CPU....267
Device users....267
Traffic capture....269
Concurrent traffic capture....270
Device Details....272
Status indicators....273
Status indicator legends....273
Device Configuration wizard....275
System update and snapshots....276
System snapshots....277
TippingPoint Operating System....277
Virtual segments....279
Special notes....279
Migration....280
Limitations: 3.1 devices other than N-Platform or NX-Platform IPS devices....280
Virtual Segment table....281
Traffic flow analyzer....281
Segment groups....282
Common device tasks....282
Adding, editing, or deleting a device....283
Add a device....283
Editing one or more devices....284
Delete a device....285
Creating or deleting a device group....285
Create a device group....285
Delete a device group....286
Unmanaging or remanaging a device....286
Unmanage a Device....286
Manage a device....286
Importing or exporting device configuration....287

Export device settings....287
Import device settings....287
Viewing and searching events....288
View events for all devices....289
View events for a specific device....289
Flush events lists....289
Managing versions, updates, and snapshots....290
Rollback to a previous version....290
Delete a previous TOS version....290
Create a new system snapshot on the device....290
Import a system snapshot from a file....291
Export a system snapshot to a file....291
Archive a system snapshot to the SMS....291
Restore from a system snapshot....292
Delete a system snapshot....292
Importing and downloading the TOS....292
Download the TOS software....293
Import TOS software from a file....293
Managing TOS distribution....293
Distribute the TOS....294
Managing virtual segments....294
Create a virtual segment....294
Delete a virtual segment....295
Analyze traffic flow for virtual segments....295
Managing segment groups....296
View segment group details....296
Import a device profile....297
Create a segment group....297
Edit segment group membership....298
Edit the name and descriptions for a segment group member....298

Edit permissions for a segment group member....299
Editing device configurations....299
User activities....299
User access....299
Management information....300
Resetting IPS filters....302
Management network....302
Configure the management network for the N-Platform or NX-Platform IPS....303
Editing the management port settings for the S-Series devices....305
Management routes....305
NAT....305
Configure NAT....305
Host IP filters....306
Services....306
Services....308
AFC settings....309
HA (High Availability)....310
Configure network HA....311
Enable/disable the NX-Platform Bypass Mode on an installed Bypass module....312
Performance Protection....312
NMS....312
Configure NMS settings for IPS (SNMP v2)....313
Configure NMS for N-Platform or NX-Platform IPS (SNMP v3)....313
SNMP settings....313
Log Configuration....314
Remote syslog....314
Create/edit remote syslog servers....316
Servers....317
Email server....317
Time settings....317

Configure the time options for TPS devices....318
Configure the time options for the N-Platform or NX-Platform....319
TSE settings....323
Authentication preferences....324
Remote Authentication....325
Specify one or more RADIUS servers....325
Import an X509 certificate....327
Specify one or more TACACS+ servers....327
sFlow®....328
Create sFlow® collector for NX-Platform devices....329
Device settings....329
Application visibility....330
FIPS settings....330
Enable FIPS on IPS device using SMS....331
SSL Inspection....333
IPS network configuration and tasks (S-Series, N-Platform/NX-Platform)....333
Segments tab (S-Series and N-Platform)....334
Physical segments....334
Virtual segments....334
Modules & Segment tab (NX-Platform)....335
Link-Down Synchronization....336
Edit TPS segment details....336
Import IPS profile....337
Edit a virtual segment....337
Ports tab....338
Edit port details....339
Resolve out-of-service mode....339
VLAN translation tab (N-Platform and NX-Platform devices)....340
Create/edit VLAN translation for N-Platform or NX-Platform IPS devices....340
IPS events configuration (S-Series, N-Platform/NX-Platform)....341
Event monitoring....342
View realtime graph data....342
View log....342

Reset events/logs..... 342
System health..... 343
Health stats..... 344
Health threshold settings..... 344
System health graphs..... 344
Set health thresholds..... 345
Performance..... 345
Performance Data tab..... 345
Performance graphs..... 346
Tier Statistics tab..... 346
Port health..... 347
Port statistics..... 347
Traffic..... 347
Traffic graphs..... 347
System log..... 348
Device health event entries..... 348
Audit log..... 350
IPS traffic capture configuration (S-Series, N-Platform/NX-Platform)..... 351
Traffic capture expressions..... 353
Create a new traffic capture file..... 353
Export a traffic capture file..... 354
Transfer traffic capture files to the SMS..... 354
IPS distribution queue configuration (S-Series, N-Platform/NX-Platform)..... 354
View distribution queues for a device..... 355
Change or delete a distribution queue entry..... 355
Inspection Bypass configuration (N-Platform or NX-Platform)..... 355
Create/edit an inspection rule..... 357
Packet trace (S-Series, N-Platform/NX-Platform)..... 358
Save all packet trace information for a device..... 358
Download all packet trace files for a device to the SMS..... 358
SecBlade IPS configuration..... 358
Management port (SecBlade IPS)..... 359
Review or edit management port settings for the TP SecBlade..... 360
Physical ports and physical segments (SecBlade IPS)..... 360
Review/edit segment mapping for physical ports on the SecBlade..... 360

Edit segment details for an IPS (includes TP SecBlade)....361
Edit data port details for an IPS (includes TP SecBlade)....361
Backplane Port 5 on the TippingPoint SecBlade....362
VLAN translation on a single port....362
Replacing a device....362
Device replacement limitations....363
Port configuration considerations....363
IPS device replacement considerations....364
Segments....364
DDoS....364
Different models....365
Replace a device....365
NGFW network configuration and tasks....366
Interfaces tab (NGFW)....366
Segments tab (NGFW)....366
Ports tab (NGFW)....367
Anti-Spoofing FIlters tab (NGFW)....367
Add an anti-spoofing filter....367
DNS/DHCP....367
ARP/NDP....368
NGFW routing....368
NGFW VPN configuration....368
NGFW authentication....369
NGFW events....369
NGFW distribution queue....369
Create a device HA cluster....370
Create a device HA cluster....370
Synchronize a cluster configuration....373
Force state change....374
Remove a cluster from the SMS....374
Advanced DDoS tasks....374
Advanced DDoS supported models....375

Advanced DDoS filter configuration....375
Edit Advanced DDoS filters....375
Create/edit a DDoS filter exception....376
DDoS preferences....376
Set DDoS preferences....376
SMS managed devices....377
Threat Protection System devices....377
440T device....378
2200T device....378
Virtual Threat Protection System....378
IPS devices....379
S-Series devices....379
N-Platform IPS devices....379
NX-Platform IPS devices....380
SecBlade IPS devices....381
Configurable ports....381
Next Generation Firewall appliances....381
Core Controller....382
Core Controller segment (10G)....382
Core Controller iLinks....382
Flow management....383
Core Controller configuration....383
Configuring Core Controller mappings....383
Use the Core Controller Mapping wizard to configure mappings....384
Configuring the Core Controller....385
Management information....385
Services....385
HA (High Availability)....386
NMS....387
Remote syslog....387
Servers....387
Time settings....387
Core controller network configuration....388

Segments....388
Link down synchronization....389
Change link down synchronization....389
iLinks....390
Core Controller system health....390
Core Controller performance....391
Performance Data tab....391
Tier Statistics tab....392
Core Controller port health....392
Statistics....392
System log....393
Reset logs....393
Audit log (Core Controller)....393
Exception rules (Core Controller)....395
Create/edit exception rules....395
Flow management (Core Controller)....396
Flow management....396
Packet processing....396
Flow management device settings....396
Maximum frame size....398
Learning mode....399
Edit flow management global settings....400
Flow management methods....400
Flow Management Methods table....401
Flow management method graphs....402
View variable flow management stats....403
Determine the best flow management method....404
Reassign flow management methods....405
Flow management rules....405
Configure Core Controller flow management rules....406
TippingPoint vController....406
Access the TippingPoint vController from the SMS....406
SSL appliance....407
Setting up an SSL appliance....407
Install the SSL appliance....408

Configure the SSL appliance..... 408
Configure SNMP on the SSL appliance.....408
Configure SNMPv3 on the SSL appliance..... 408
Add the SSL appliance to the SMS..... 408
Add the SSL appliance to the SMS.....408
SSL appliance configuration..... 409
Device configuration..... 409
Network configuration..... 410
Ports tab.....410
Event monitoring (SSL appliance).....410
System health..... 411
Performance.....411
Port health.....412
Port statistics.....412
Traffic.....412
Server tab.....412
Net tab.....412
SSL tab..... 413
Switch tab.....413
System log..... 415

Administration..... 416

General administration.....416

Working with the Admin (General) screen..... 416

SMS server.....416

SMS software..... 416
Download and install SMS software..... 417
Import and install SMS software from a CD or the TMC..... 417

SMS patches..... 418
Install an SMS patch..... 419
Roll back an SMS patch..... 419

SMS node count license..... 419
Upgrade your SMS license key.....420

TippingPoint license package.....420
Edit notification settings.....421
Import a license package..... 421
View license status details..... 421

SMS web security SSL certificate.....422

Reset the SMS web security SSL certificate..... 422
Import a custom Web security SSL certificate..... 422
SMS certificate key..... 423
Update the SMS certificate key..... 424
Viewing system health..... 425
Viewing port health..... 425
Viewing the SMS system log..... 426
View the SMS system log..... 427
Export SMS system log entries..... 427
Viewing the SMS audit log..... 427
Authentication and authorization..... 428
Managing active sessions..... 428
Set or change a new resource group for a user account..... 429
Terminate an active session..... 429
Configuring authentication..... 430
Authentication source..... 431
Edit the SMS server authentication source..... 431
Authentication configuration..... 431
Configure RADIUS authentication..... 432
Edit the RADIUS server configuration..... 432
Import an X509 certificate..... 433
Configure Active Directory authentication..... 433
Allowing remote users with Active Directory authentication..... 434
Edit the Active Directory server configuration..... 434
Edit Active Directory global group mapping..... 435
Import an Active Directory SSL certificate..... 437
Configure TACACS+ authentication..... 437
Edit the TACACS+ server configuration..... 437
Configure CAC authentication..... 438
CAC authentication overview..... 440
Prerequisites..... 440
Import CA Certificates..... 441
Add, edit, import, or delete personal identifiers..... 441
Enable CAC authentication..... 442
Log in to the SMS using CAC authentication..... 442
Managing user roles..... 443

Create a user role....443
Edit a user role....444
Managing user groups....445
Create a user group....445
Edit a user group....446
Delete a user group....446
Managing user accounts....447
User accounts....448
Specify user name....448
Specify a password....449
Assign the user to a group....449
Create a user account....449
Edit a user account....451
Delete a user account....451
Database....451
Working with the Admin (Database) screen....451
Database maintenance....451
Edit data retention settings....454
Reset data statistics....455
Initiate an immediate clean up of data statistics....455
External database settings....455
Backup and restore....456
Backup....456
Backup the SMS database....456
Edit a scheduled backup....458
Delete a scheduled backup....458
Restore....458
Restore the SMS database....460
Server properties....460
Configuring management properties....460
System information....460
Update system information....461
FIPS mode....461
Enable or disable FIPS Crypto Core mode....462

Services....463
Enable or disable the SMS services....463
Configuring network properties....464
Network interface....464
Update network interface information....465
Date/Time....465
Enable Network Time Protocol....465
Enable SMS Network Time Protocol authentication settings....465
Manually set the time and date....466
SMTP server....466
Edit SMTP server settings....466
TMC proxy....467
Configure a proxy TMC connection....467
Domain Name Service (DNS)....468
Configure DNS....468
Configuring NAT properties....468
SMS NAT....468
Enable SMS global NAT....468
Disable SMS global NAT....469
SMS per network NAT....469
Enable SMS per network NAT....469
Add or edit an SMS per network NAT address....469
Delete SMS per network NAT addresses....469
Address determination....470
Configuring integration properties....470
IDResolver....470
Configuring SNMP properties....470
Request settings....470
Enable SNMP requests....471
Disable SNMP requests....471
NMS trap destinations....471
Configure the SMS to send NMS traps to a destination....471
Edit an NMS trap destination....472
Delete an NMS trap destination....472
Configuring syslog properties....472

Syslog format options....473
SMS system syslog....473
SMS audit syslog....474
Device system syslog....474
Device audit syslog....475
Snort syslog for MARS [Deprecated]....476
Snort syslog for V2 [Deprecated]....477
SMS 2.0/2.1 syslog....477
SMS 2.5 syslog....479
ArcSight CEF Format v3.5 [Deprecated]....481
ArcSight CEF Format v4.1 [Deprecated]....484
ArcSight CEF Format v4.2....487
Create or edit a custom syslog format....490
Available fields in a syslog format....491
Copy an existing syslog format to create a custom format....500
Delete a user-defined syslog format....500
Remote syslog for events....500
Configure remote syslog notification settings....502
Edit syslog server settings....503
Delete a syslog server....503
Configuring TLS settings....503
Edit TLS versions....504
High Availability....505
Configuring an SMS HA cluster....506
Configure an SMS HA cluster....507
Synchronize the SMS HA cluster....508
Disable the SMS HA cluster....509
Adjust HA timeout values....509
Viewing active and passive SMS details....509
Swap HA cluster nodes....510
Invoke failover to activate a passive SMS....510
Named resources....510
Create, edit, and delete named resource groups....511
Create a new named resource group....511

Show users of an existing named resource group....512
Edit a new named resource group....512
Save As a named resource group....512
Delete a named resource group....512
Create, edit, and delete named resources....513
Import a list of named resources from a file....513
Export a list of named resources to a file....513
Configure a user resolver filter....513
Define a new named resource....514
Show users of a named resource....514
Edit a named resource....514
Delete a named resource....514
Exports and archives....514
Export a file from the SMS exports and archives directory....515
Delete a file from the SMS exports and archives directory....515
IP address identifier....515
Add or edit an IP address ID....516
Delete an IP address ID....517
Change the priority order for IP address groups....517
User ID IP Correlation....517
Add the Identity Agent....518
Create an Identity Agent Group....519
Select an Identity Agent to be in a group....519
Enable Identity Agent group....520
User ID IP Correlation events....520
Geo Locator database....521
Download a Geo Locator database file from the TMC....522
Import a Geo Locator database file....522
SSL Inspection....523

Overview ... 523
Additional considerations ... 523
Requirements ... 525
Manage SSL inspection from the SMS ... 526
Before you configure SSL inspection ... 526
Update the license package on TMC ... 527
Secure the SMS certificate repository ... 527
Import the license package ... 528
Verify the license package ... 528
Enable SSL inspection ... 528
Configure SSL inspection ... 529
Import the SSL server certificate and private key ... 529
SSL servers ... 530
Add or edit an SSL server ... 530
Refresh certificate status ... 531
Add or edit an SSL inspection policy ... 531
Distribute the inspection profile ... 532
After you configure SSL inspection ... 533
Verify SSL inspection activity ... 533
Replace a certificate ... 534
Give permissions for SSL inspection ... 534
Give access to SSL servers ... 535
Manage SSL inspection from the LSM ... 535
Before you configure SSL inspection ... 535
Update the license package on TMC ... 536
Import the license package ... 536
Verify the license package ... 537
Enable SSL inspection ... 537
Configure SSL inspection ... 537

Import the SSL server certificate and private key 538
Add or edit an SSL server 539
Add or edit an SSL inspection profile 540
Assign the SSL inspection profile to a virtual segment 541
Commit changes to the Running configuration 542
After you configure SSL inspection 542
Verify SSL inspection activity 542
Give permissions for SSL inspection 543
Best Practices 544
Troubleshoot SSL inspection 544
Basic troubleshooting 544
Advanced troubleshooting 546
CLI Reference for the 2200T device 547
Troubleshoot 547
show license 547
display conf 548
show tse 549
debug 550
show np tier-stats 559
show ssl-inspection congestion 560
keystore 561
Configure 561
ips{running-certificates}certificate 562
ips{running-certificates}private-key 562
ips{running-sslinsp} Context Commands 563
ips{running-sslinsp}enable 564
ips{running-sslinsp}log sslInspection 564
ips{running-sslinsp}server 565
ips{running-sslinsp}profile 567
ips{running-vsegs-VSEG_NAME}ssl-profile 569

commit....569
save-config....570
Troubleshooting....572
Login error messages....572
Password recovery....572
Reset your password....572
Network changes....573
IPS port out-of-service....574
SMS error messages....574
Modifying filters....575
Modifying filter action settings....575
Adding exceptions....575
Distributing profiles....576
TMC connectivity....576
Geo Locator maps do not display correctly....577
Port information....579
Required ports....579
Active Response ports....581
HA ports....582
Optional ports....583
Filters....587
Device replace table....589
Replacing a previous IPS model with an NX model....592
Replacing an existing NX model with another NX model....592

General clarifications..... 592

Reputation information..... 593

Reputation import rules..... 593

Format rules..... 593

Tag category rules..... 594

Address rules..... 594

SMS encryption protocols, algorithms, and cipher support..... 596

About this guide

The *Security Management System User Guide* provides information to help you quickly get started configuring your TippingPoint system and using the Security Management System (SMS) to manage 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*

Target audience

This guide is intended for security network administrators and specialists that have the responsibility of monitoring, managing, and improving system security. The audience for this material is expected to be familiar with the 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 product documentation for the Security Management System is available online. The product document set generally includes conceptual and deployment information, installation and user guides, CLI command references, safety and compliance information, and release notes.

For information about how to access the online product documentation, refer to the *Read Me First* document in your product shipment.

Conventions

This information uses the following conventions.

Typefaces

TippingPoint uses the following typographic conventions for structuring information:

Convention	Element
Bold font	• Key names • Text typed into a GUI element, such as into a box • GUI elements that are clicked or selected, such as menu and list items, buttons, and check boxes. Example: Click **OK** to accept.
Italics font	Text emphasis, important terms, variables, and publication titles
`Monospace font`	• File and directory names • System output • Code • Text typed at the command-line
`Monospace, italic font`	• Code variables • Command-line variables
`Monospace, bold font`	Emphasis of file and directory names, system output, code, and text typed at the command line

Messages

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

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

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

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

Important: Provides significant information or specific instructions.

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

Product support

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

Email support

tippingpoint.support@trendmicro.com

Phone support

North America: +1 866 681 8324

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

Getting started

The TippingPoint Security Management System (SMS) is the control center for managing large-scale deployments of all TippingPoint products. 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 hardware appliance is available as a rack-mountable management server or as a virtual product (vSMS). Both include the SMS client, which provides an easy interface for performing secure management tasks for multiple devices.

The core of the SMS is the ability to create multiple filter profiles which are distributed to specific devices. Organizing devices in groups or security zones makes it easier to distribute and update security profiles than doing it for each device. You can also use the SMS to keep your devices updated with the latest TippingPoint Operating System (TOS) software and Digital Vaccine packages.

SMS components

The main components of the system are the **SMS secure server** 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 SMS server provides two interfaces:

- SMS client, a web-based interface with links to client software, documentation, and the Threat Management Center (TMC).
- SMS command line interface (CLI), which enables users with SuperUser rights to log on to and configure the SMS server.

The SMS client is a Java-based application for Windows, Linux, or Mac workstations. The SMS client consists of a graphical user interface and a dashboard to enable users to manage the TippingPoint system and interacts with the following services and components:

- **Threat Management Center (TMC)** — Centralized service center that monitors global threats and distributes up-to-date attack filter packages, software updates, and product documentation.
- **ThreatLinQ** — TippingPoint service that works with the TMC to collect and analyze information about the security posture of the Internet.
- **Digital Vaccine (DV)** — Update service that includes up-to-date filter packages for protecting your network.
- **Managed devices** — TippingPoint devices installed on your network, such as the Threat Protection System (TPS), Intrusion Prevention System (IPS), and Next Generation Firewall (NGFW). Each SMS can manage multiple TippingPoint devices; the maximum number depends on usage, network, and other environmental conditions.

Installation

Prior to using the SMS server, you need to install and configure the components of the SMS system. See the installation documents for your SMS platform.

To install an SMS appliance, refer to the Quick Start guide that came with it. The guide will describe the steps to mount the appliance in a rack, connect it to your network, and configure the server.

To install vSMS, refer to the *vSMS Getting Started Guide*, which provides installation and setup information for the Virtual Security Management System (vSMS).

Important: For the most up-to-date information, download the latest SMS documentation from the TippingPoint Threat Management Center (TMC) website at *https://tmc.tippingpoint.com*.

After you set up the SMS hardware and connect to your network, you must configure the server and install the client. You must also complete certain initial management tasks.

Important: Make sure your system meets TMC port requirements. See *Port information* on page 579.

SMS server home page

Your SMS home page is located on your SMS server. This Web-based interface enables you to install or upgrade SMS client software, and it provides quick access to SMS System Log and saved reports, documentation, exported or archived files, and the TippingPoint Threat Management Center (TMC).

After you log in to SMS (see *Log in to the SMS server home page* on page 5), the following links are available in the navigation menu at the left of the page:

- *Download SMS client software* on page 6
- *View or download reports* on page 6
- *View or download documentation* on page 7
- *View or download exports and archives* on page 7
- *Connect to the TMC* on page 7

Log in to the SMS server home page

After the SMS server is configured and your user account has been defined, you can connect to the SMS home page.

1. Open a supported Web browser.
2. Provide the IP address configured as the management address for the SMS (for example, `https://<sms-server>`), and press **Enter**.
3. On the Login page, enter your username and password, and click **Login**.

Depending on your user account roles and security settings, logging in to the site may enable options such as displayed reports and archived files.

Note: If the website does not prompt you for a login, you can log in to the SMS using the **Login** link, which is located in the upper-right corner.

Download SMS client software

The Client Installation page on the SMS Server provides details, such as system requirements and version number, and gives instructions for installing, upgrading, or uninstalling the client. From this page, you can download the appropriate installer for your Windows, Linux, or Mac system.

If a patch is available for the SMS client, it is noted under the installer buttons.

View or download reports

The Reports page on the SMS server contains links to the SMS System Log and to saved reports that are available on the server. In addition, the SMS home page contains a Reports panel that displays a condensed view of reports. If you are not logged on to the SMS, you must log in to view the reports or ensure the Web View Permissions for each individual report is configured to allow anonymous users to view results.

View reports from the SMS website

1. On the SMS home page, click **Reports** in the navigation menu.
2. Click on a report listed in the Saved Reports area. Report details are loaded into the table.
3. Select a file type for the report output:
   - html — HTML file
   - pdf — PDF file
   - csv — Comma-delimited file
   - xml — XML-formatted data
   - docx — Word document
   - xls — Excel spreadsheet

   Depending on the file type and your browser settings, the report either displays in your browser window or is downloaded to your local drive.

   Note: When you use the save a report using the CSV or XML option, certain reports might add an additional column that contains two parts of the IPv6 address.

View or download documentation

The Documentation page on the SMS Server contains links to the PDF documents that were included with your SMS release. For the most recent documents and updates, check the TMC at *https://tmc.tippingpoint.com.*

View or download exports and archives

The Exports and Archives page on the SMS Server displays links to files that have been exported or archived from an SMS client.

To save a file locally, right click on the file and save it to your hard drive.

View or save exported files

1. Select **Exports and Archives** from the left navigational menu.
2. To open a file, click the file name.
3. To download a file, right-click the file and select **Save As**.

Connect to the TMC

The **TMC** link in the navigation menu of the SMS Server is a direct link to the Threat Management Center at *https://tmc.tippingpoint.com*.

SMS client

The SMS client interface enables you to manage your TippingPoint system. You can download, install, and run the SMS client on a Windows, Mac, or Linux-based computer.

Install the SMS client

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 579.

For information on hardware and software requirements, consult the SMS Release Notes or the SMS installation documentation.

Install the SMS client

1. Open a Web browser, and connect to your SMS server home page (see *Log in to the SMS server home page* on page 5).
2. On the Welcome page, select the appropriate SMS client installer for your platform and download it.
3. 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.

After you install the SMS client, you should download, install, and activate the latest Digital Vaccine from the TMC website. See *Configure security preferences* on page 15.

Important information when using a 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 4.4.0 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.

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

1. Temporarily make the following changes to the JRE on your local Mac OS X. - OR -
2. 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 423.

Review the SMS certificate key compatibility matrix for your device.

Log in to the SMS

When you launch the SMS client application, you may see a splash screen, and then the **SMS Login** screen is displayed. Use this screen to log in to the SMS client or for distributed management. This screen enables you to log in to a single SMS client or, for distributed management, you can log in to multiple SMS clients.

Log in to the SMS

1. Launch the TippingPoint SMS client.
2. Do one of the following:
   - To log into a single SMS server client, specify the IP address or fully qualified hostname in the **SMS Server** field.
   - To log into multiple SMS server clients, click **More**, and then click **Add** next to the **SMS Servers** field. Specify the IP address or fully qualified hostname in the **SMS Server** field, and click **OK**. Repeat for each SMS server.

     Note: When you log in to multiple clients, the **SMS Login** screen saves each address you enter. The **SMS Login** screen does not list all active servers. For information on account settings, see *Authentication and authorization* on page 428.
3. Provide the user name and password for a user account defined on the SMS.

   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.

   After you successfully log in, typically the SMS dashboard is displayed in front of the client interface, depending on how your SMS client is configured. If you are unable to log in, see *Troubleshooting* on page 572.

   When you log in to multiple SMS server clients, the client for each server is displayed on a separate tab. For information about tabbed dashboard options, see *Dashboard* on page 30.

   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 443.

View notifications

After you log in, a Notifications window might be displayed. After reading the message(s), click the **OK** button to close the window. Click the notifications icon in the bottom right corner of the client interface to access the View Notifications screen at any time.

The following are types of notifications that might be displayed:

- **System Notification** — Indicates that an event triggered a message.
- **DV Notification** — Indicates a new Digital Vaccine 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.

SMS dashboard

After you log into the client, the SMS dashboard is displayed. The dashboard provides centralized access for monitoring the status of the SMS. This window offers a quick review of the SMS, according to the types of filters on the system.

The dashboard provides gadgets that track and display event data, performance, and system health and status. The SMS is polled approximately every five minutes to collect data for display in the historical charts.

Health and Status gadgets (for example, Charting, Geo, Top gadgets) provide a high-level warning system for potential health and performance problems with your devices.

To enhance the quick view statistics, you can configure the dashboard to display specific reports.

For detailed information about the SMS dashboard, see *Dashboard* on page 30.

Main user interface

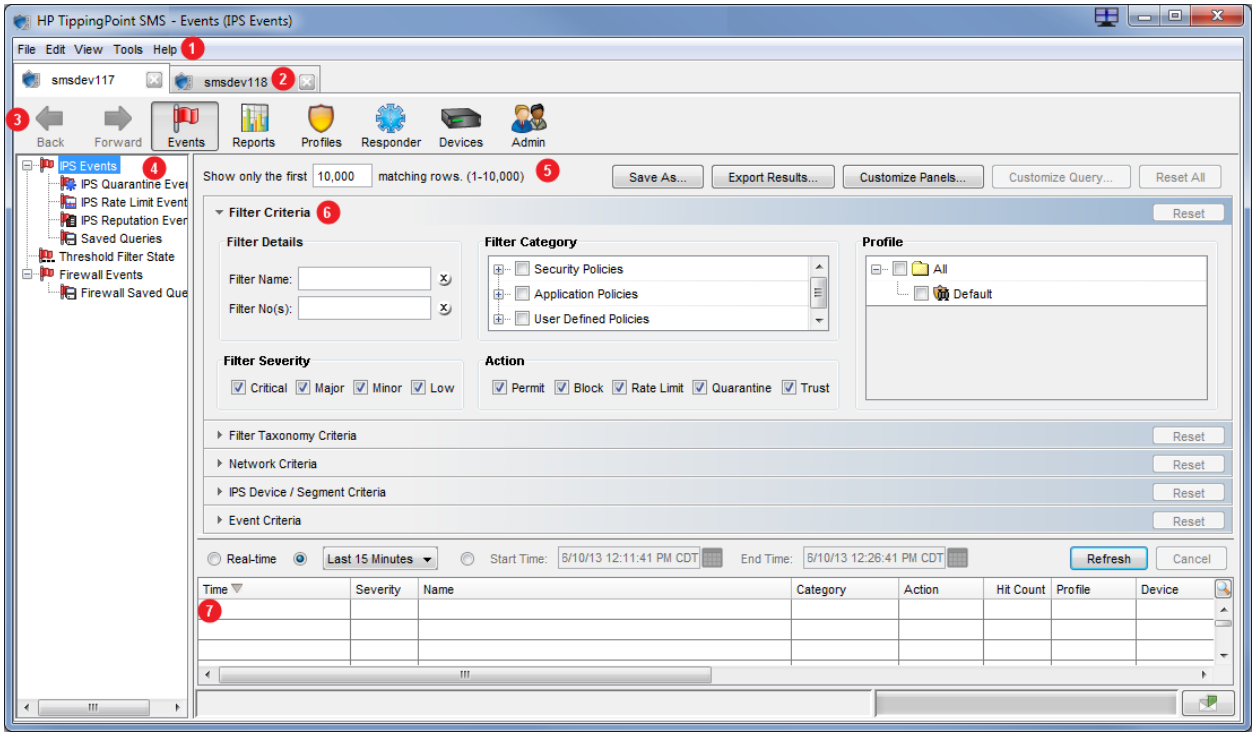
The SMS client main user interface provides controls that enable you to manage and maintain your TippingPoint system. The interface includes a menu bar, the SMS toolbar, a navigation pane, and a content pane. If you log into multiple SMS servers, the client displays a tab for each server.

Certain interface controls launch a dialog box or wizard, as appropriate, for creating, editing, and validating changes in system data. A wizard is a collection of screens that walk you through a multiple step task or process. A dialog box is a secondary window that enables you to perform a command or prompts you for specific feedback.

When you click a button, the system performs the action displayed in text. For buttons such as **Apply**, **Save**, and **OK**, you save and accept the changes or actions you entered. Buttons with **Cancel** end without saving changes. Some buttons may also open new screens and dialog boxes, such as **New**, **Create**, or **Edit**. You must conclude your actions on those screens and dialog boxes to return to the previous screen.

Right-click menus display a list of options that differs according to workspace, screen, and the entry or object you selected to display the menu.

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



Number	Object	Description
1	Menu Bar	Some menu options may vary based on screen.
2	Tab	When you are connected to multiple SMS servers, each tab displays a complete client interface for the selected SMS.
3	SMS Toolbar	Navigate to each SMS workspace.
4	Navigation Pane	Displays nodes of the navigation tree; click the plus (+) symbol to expand a node.
5	Content Pane	The content depends on your selection in the navigation pane. Content may consist of criteria for queries, lists of entries, display options, details, and so on.
6	Panel	Defined, named area or section of a screen displayed in the content pane.

Number	Object	Description
7	List	Rows of data displayed in a table view. Typically, you can select a row to act on (edit, delete, etc.).

Menu bar

The menu bar contains five top-level menus: **File**, **Edit**, **View**, **Tools**, and **Help**. 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.

SMS toolbar

The SMS toolbar enables you to navigate to the primary functional areas of the SMS client. As you click on a button on the toolbar, the navigation and content panes display the corresponding workspace: **Events**, **Reports**, **Profiles**, **Responder**, **Devices**, or **Admin**.

Workspace

Each functional area in the SMS client has a corresponding workspace. A workspace consists of the elements in content and navigation panes that enable you to view, query, configure, or act on your TippingPoint system.

Click one of the buttons on the SMS toolbar to display the corresponding workspace:

Events on page 41 — Manage and view system behavior and events. The application provides two categories of events called attack and health events. Attack events are events that occur when the system receives malicious attacks. Health events are events of system performance problems, such as lost or rerouted network traffic.

Reports on page 75 — Generate, download, and view reports that provide details of threats encountered by the entire system and show processing trends. The Reports workspace also provides real-time assessments of the IPS network statistics.

Profiles on page 102 — Tune the behavior of your TippingPoint system by managing, editing, and applying profiles, filters, action sets, Digital Vaccine packages, and so on.

Responder on page 227 — 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.

Devices on page 258 — Configure, monitor, and manage devices, device groups, network configuration, traffic capture, and so on. You can also download TOS updates and distribute them to managed devices from this workspace.

Administration on page 416 — Manage user access, system and audit logs, and system settings. Only users with the correct role and access can manage settings on the Admin screen.

Navigation pane

The navigation pane enables you to 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.

Content pane

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.

Features

The SMS provides the following features.

Auto complete

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.

Tabbed views

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.

Table filtering

When a table displays a vertical scroll bar (that is, the number of rows exceeds the maximum number that fit into the display area), the SMS client enables you to filter the table by matching text.

To use the filtering feature, click the magnifying glass icon at the top right of the table, directly above the scroll bar. This opens a Filter text box below the table. Provide filter criteria in the text box, and click **Refresh**. When the table is refreshed, is displays rows with data that match your filter criteria. To close the Filter area, either click the close (x) icon, or use the magnifying glass icon to toggle the Filter field.

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`.

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.

Table column controls

Click the drop-down arrow in a table column heading to display the following options:

- **Sorting** — Sort the column ion ascending or descending order, based on the column entry.
- **Aggregation** — Summarize similar column entries.
- **Hide Column** — Hide the selected column from your view.
- **Table Properties** — 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.

Realtime data

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.

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 **Pause** to freeze and resume statistical polling. Use the **Polling Interval** drop-down menu to adjust the polling interval.

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.
3. Click **Refresh** to filter events and show matching events in realtime.

Named resources

The SMS uses *named resources* 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 *Named resources*.

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.

Right-click menus

Right-click a selected entry to display a list of options. These options differ according to entry type and screen.

System preferences

The SMS client allows users, depending on their access and authorization levels, to configure certain system preferences that affect how the client and the dashboard look and operate.

To view or change the preferences, click the **Edit** menu in the SMS client, and select **Preferences**. The navigation pane at the left of the System Preferences window contains the following configuration options:

- *Configure security preferences* on page 15
- *Configure device SNMP preferences* on page 16
- *Configure device communication preferences* on page 17
- *Dashboard preferences* on page 17
- *Change the SSH client setting* on page 18
- *Configure banner message preferences* on page 18
- *Configure PCAP download preferences* on page 19
- *Report preferences* on page 19

Security preferences

Security preferences enable you to control aspects of SMS login passwords, information sharing between the TMC and your SMS, and client preferences related to storing user login information and session timeout.

Configure security preferences

1. Select **Security** in the System Preferences navigation menu.
2. In the Password Preferences area, configure the following options:
   - Select a Security Level: **0 - Low**, **1 - Medium**, or **2 - High** (default).
   - Select or clear **Require Login for Web Access** to determine whether the SMS home page requires a separate login from the client.

- Select or clear **Require Password to be different from user ID** to determine whether the SMS client allows a user to have a password that is the same as the user ID.
- Select or clear **Lock User after failed login attempts** to determine whether the SMS client locks a user out after a specified number of unsuccessful login attempts. If enabled, use **Threshold** to set the number of unsuccessful consecutive attempts a user can make before the account is locked out.

3. In the TMC Information Share area, configure the following options:
   - Select or clear **Enable update tracking on TMC** to determine whether the TMC can track updates made form the client.
   - Select or clear **Enable TMC Polling for DV, OS, and License Package updates** to determine whether the SMS client periodically checks the TMC for updates.
   - Select or clear **Enable ThreatLinQ Event Sharing** 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:
     - Hide All IP Addresses in ThreatLinQ
     - Don't Hide IP Addresses in ThreatLinQ
     - Hide the Following Addresses in ThreatLinQ (Allows you to specify IP Addresses, CIDR, or address ranges to keep private or hide)
4. In the Client Preferences area, configure the following options:
   - Select or clear **Allow storing the username and server used to login to this SMS** to allow or prevent the client from caching login information.
   - Select or clear **Timeout client session after inactivity** to allow or prevent the client from ending a session after a specified period of inactivity. If enabled, use the Time field to set the number of minutes (10–600) a user can be inactive before the session is ended.
5. Click **OK**.

Device SNMP

The Device SNMP preferences enable you to specify SNMP settings.

Configure device SNMP preferences

1. Select **Device SNMP** in the System Preferences navigation pane.
2. (Optional) Select the **v2** check box to enable the SMS to communicate with managed devices using SNMPv2. When you select this check box, you can enter and confirm the SNMPv2 community string.
3. (Optional) Select **v3** to enable the SMS to communicate with managed devices using SNMPv3. When you select this check box, do the following:
   a. Enter the SNMPv3 user name in the **User Name** field.

b. Select an authentication protocol from the **Protocol** drop-down list.

c. Enter and confirm the key.

d. Select a privacy protocol from the **Protocol** drop-down list.

4. (Optional) Select the **Use SNMP v3 when possible** check box to enable the SMS to automatically use SNMPv3 to communicate with managed devices when available.
5. Click **OK**.

Device communication

The device communication preferences enable you to specify the device communication and data retrieval settings.

Configure device communication preferences

1. Select **Device Communication** in the System Preferences navigation pane.
2. Select the **Enable Device Communication Check** check box to enable the SMS to perform communication checks with managed devices. If enabled, specify values for the following options:
   a. Failure threshold: maximum number of failures. This only applies to IPS devices that are using SNMP traps to send alert logs.
   b. Comm check interval: interval (in seconds or minutes) between communication checks. This does not apply to IPS devices using the Encrypted Alert Channel.
3. Specify **Data Retrieval Polling Interval** options in minutes, 1–30 for the following:
   - Device history statistics (Profile reports)
   - Device health and performance
   - Device port statistics
   - Overall SMS health and performance
4. Click **OK**.

Dashboard preferences

The Dashboard preferences determine whether the dashboard is actively displayed for all users when they log on to the SMS.

Note: Only administrators with the SuperUser role can disable the dashboard globally.

If **Enable Dashboard** is selected, you can specify the time interval (5–60 minutes) at which the dashboard information is updated.

If you clear the **Enable Dashboard** check box, the dashboard will not automatically be displayed when a user logs into the SMS. A user can still manually open the Dashboard view, but the information is not updated.

You can select the font family, style, and size.

SSH client preferences

The SSH Client preferences enable you to specify an external SSH client application to launch from the SMS client.

Change the SSH client setting

1. Select **SSH Client** in the System Preferences navigation menu.
2. Click **Browse**, and choose the local program to use as SSH client.
3. In the Choose File dialog, click **OK**.
4. Click **OK**.

Banner message preferences

The Banner Message preferences enable you to enable or disable the banner message feature, specify a banner message, and choose whether to display the message in the client or in the command line interface (CLI) at login.

Configure banner message preferences

A banner is a message presented to a user; examples of banner messages include temporary notices, reminders, or permanent messages, such as authorized access and legal notices. If enabled, the banner message will always display until you disable it.

1. Select **Banner Message** in the System Preferences navigation pane.
2. Select or clear **Enable Banner Message** to enable or disable the banner message.
3. If enabled, enter a title and a message in the appropriate fields, and then choose from the following options:
   - **Display on client toolbar** to display the message on the SMS toolbar, located to the right of the Admin button.
   - **Display on client login** to display the message when a user accesses the client login screen.
   - **Display on web login** to display the message when a user accesses the client from a web page.
   - **Display on console/CLI login** to display the message when a user logs in at the command line.
   - **Display on remote/SSH login** to display the message when a user logs in remotely using SSH.
4. Click **OK**.

Configure PCAP download preferences

The PCAP Download preferences enable you to provide remote storage information (e.g., 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 will generate 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 416.
- Sufficient storage space for the PCAP files.
- PCAP management application.

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

1. Select **PCAP Download** in the System Preferences navigation pane.
2. Select an **External Source** from the following: IPS, NFS, or SMB.
3. Enter the remote directory and server name in the appropriate fields.
4. If you select SMB as the external source, enter a user name and password in the appropriate fields. You have the option to specify a **Domain** to access.
5. Click **OK**.

See also *Packet trace* on page 57.

Report preferences

The Reports system preferences allow you to do the following:

- Specify a time interval (in minutes) for the SMS to run an extract, transform, and load (ETL) process.
- Click **Run ETL Process Now** to run the ETL process immediately.

Software updates

When TippingPoint identifies new attacks or improves methods of detecting existing attacks, the TMC makes protection available to customers in the form of TippingPoint Operating System (TOS) updates, Digital Vaccines, 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* on page 20
- *Download, activate, and distribute Digital Vaccines* on page 20
- *Install SMS updates* on page 21
- *Migrate to another SMS version* on page 22

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. You can download and distribute TOS updates from the TippingPoint OS screen in the Devices workspace.

Download a TOS update

1. Select **Devices** in the SMS toolbar.
2. In the navigation pane, select TippingPoint OS.
3. Click **Download from TMC** under the TOS Inventory list.
4. In the Device Software Download dialog, select an update in the Available Device Software list, and then click **Download**.

   The TOS Inventory list displays package details once the TOS package is downloaded. After the download is complete, the next step is to distribute the update to the appropriate devices.

Distribute a TOS update

1. Select the TOS package in the TOC Inventory list.
2. Click **Distribute**.
3. In the TippingPoint OS Distribution wizard, select the appropriate devices in the Targets list, and then click **OK**.

Download, activate, and distribute 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 from the associated screens of the **Profiles** workspace.

Note: If you do not download Digital Vaccine to the SMS and your devices already have filter packages installed, the SMS will report events passed to it from the devices, but it will not be able to identify the filters associated with those events.

Download a Digital Vaccine from the TMC

1. In the Profiles workspace, click **Digital Vaccines** in the navigation pane.
2. On the DV Inventory tab, click **Download from TMC**.
3. In the New Digital Vaccine Download dialog, select a version to download.

   You can also select options to **Activate** and/or **Distribute** automatically following download.
4. Click **Download**.

Activate a Digital Vaccine

Select a Digital Vaccine in the DV Inventory list, and then click **Activate**.

The SMS supports only one active Digital Vaccine in the DV Inventory; however, you can distribute a Digital Vaccine whether or not it is the active DV.

Distribute a Digital Vaccine to one or more devices

1. Select the Digital Vaccine in the DV Inventory list.
2. Click **Distribute**.
3. In the Digital Vaccine Distribution dialog, select the target device(s), and then click **OK**.

   Once a Digital Vaccine is distributed, the device immediately begins blocking traffic that belongs to the Vulnerability—Default category. All other categories are disabled.

Install SMS 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 182.

Download an SMS update from the TMC

Follow these steps to install an SMS patch. To perform a full software update, see *Migrate to another SMS version* on page 22.

1. Select **Admin** in the SMS toolbar.
2. Click **Update** in the SMS Patches section.
3. In the SMS Patch Wizard, select **Download from TMC**, and then click **Next**.
4. Select the patch file from the list of available patches, and click **Download**.
5. Install the patch, and then click **Finish**.

   For information about installing an SMS patch, see *SMS patches* on page 418.

Migrate to another SMS version

To migrate from one version of SMS to a new version, you should first create a backup of your current SMS, then update the SMS software to the current release and install the new SMS client.

For more information, refer to the following topics:

- *Backup and restore* on page 456
- *Install SMS updates* on page 21
- *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 website at *https://tmc.tippingpoint.com*.

Manage your system

To begin managing your TippingPoint system from the SMS you must complete the following tasks:

- *Add a device to the SMS* on page 22
- *Download a Digital Vaccine from the TMC* on page 21
- *Activate a Digital Vaccine* on page 21
- *Distribute a Digital Vaccine to one or more devices* on page 21

Add a device to the SMS

1. On the Devices screen, click **New Device**.
2. In the New Device wizard, do the following:

- Specify an IP address for each device.
- Provide the Username and Password for authentication.
- Select the Device Type for the device(s).

Note: When you add multiple devices, all of them must 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. Once you manage a TPS device, you cannot switch the mode from the SMS.

3. You can select the following on the Options screen:
   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 immediately after the device(s) are added. You can also select **Clone an existing device** to copy settings from an existing device.
4. Click **OK**.

   When a device is successfully added to the SMS, the device appears on the Devices screen 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.

After adding devices to the SMS, you need to perform the following tasks:

- *Download a Digital Vaccine from the TMC* on page 21
- *Activate a Digital Vaccine* on page 21
- *Distribute a Digital Vaccine to one or more devices* on page 21

Tools

The Tools menu in the SMS toolbar provides 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 utilities available through the SMS include:

IP Lookup on page 24 — 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 25 — 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 on page 26 — 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 26 — Use the SMS Diagnostic Toolkit in connection with TippingPoint support staff to help diagnose and resolve issues.

IDResolver on page 29 — 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 521.
- **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 510.
- **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 515.

Use the IP Lookup utility

1. On any screen, click **Tools** in the top menu bar, and then select **IP Lookup** and the lookup service entry for the information you want to look up.

   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**.

   Results display in the lower, tabbed section of the window.

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** > **Whols**, 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.

Access the TMC

1. In any screen, select **Tools** > **TMC** from the top menu bar.
2. From the TMC, click the **Login** tab.
3. Log into the TMC using your username and password.
4. If you are not a register TMC user, click the **Register** link.

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 *Configure security preferences* on page 15.

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.

Access ThreatLinQ

Do one of the following:

- On any screen, click **Tools** in the top menu bar, and select **ThreatLinQ**.
- In the Events workspace, right-click an events entry, and select **ThreatLinQ**.
- In the Profiles workspace, 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:

Log Utils on page 27 - create a logs zip file and edit the logger levels.

Hotfixes on page 28 - view, install, and rollback hotfixes installed on the SMS.

Bookmarks on page 28 - generate a bookmark string for the SMS client or command line interface (CLI).

Users on LDAP on page 29 - look up information about those users and groups from the LDAP server, if configured.

Launch the SMS diagnostic toolkit

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

Log Utils

In the SMS, you can create a logs zip file and edit the log4j logger levels from the Log Utils screen.

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. On any screen, click **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. On any screen, click **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. Available levels include the following:

Level	Description
ALL	Includes all levels.
TRACE	Designates more details than the DEBUG level.
DEBUG	Designates informational events useful to debug the log file.
INFO	Designates informational messages.
WARN	Designates potentially harmful situations.
ERROR	Designates errors that might still allow the application to continue running.
FATAL	Designates severe errors.

Level	Description
OFF	Turns off logging.

4. Click **OK**.

Hotfixes

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. To make sure the SMS has enough disk space, you can delete previously installed hotfixes.

Install a hotfix

Describes how to install a software update.

1. On any screen, click **Tools** > **Diagnostics** > **Hotfixes**.
2. Do one of the following:
   - Click **Install** to install a single SMS software hotfix.
   - Click **Install Bulk** > **Add** to batch install multiple software hotfixes.

   The SMS uploads the file(s) to the list of installed hotfix entries.

Rolling back to a previous software hotfix

Describes how to roll back to a previous version.

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

Bookmarks

In the SMS, you can generate a bookmark string to be used for the SMS client or the command line interface from the Bookmarks screen.

Generate bookmark string

1. On any screen, click **Tools** > **Diagnostics** > **Bookmarks**.
2. Click **Generate Bookmark String**.

The SMS automatically generates the string and updates the **For UITtestBaseBookmark** and **"bookmark" arg** fields.

Users on LDAP

In the SMS, you can quickly look up user names and groups related to a user account that is authenticated against an LDAP server from the Users on LDAP screen.

To configure the LDAP server, go to **Admin** > **Authentication** > **Active Directory**.

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.

Configure and enable IDResolver

1. Select **Admin** in the SMS toolbar to open the Admin workspace.
2. Select **Server Properties** in the navigation pane.
3. On the Server Properties page, select the Integration tab.
4. Click **Edit** to open the Edit IDResolver Server dialog, and provide the following information:
   - **Address** and **Port**.
   - **User Name** and **Password**.
   - Select a value for **Password Encryption**.
   - Specify a numerical value for **Timeout**.
5. Click **OK** to close the Edit IDResolver Server dialog and return to the Integration tab.
6. Click **Enable** to enable IDResolver.

Query IDResolver

1. In the SMS client, 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.

Dashboard

The SMS dashboard provides at-a-glance insight into your network security status with charts and graphs that continuously update to reflect the health, status, and security events related to your system. This overview, composed of configurable, color-coded charts and tables, is the starting point for:

- Monitoring application visibility and utilization
- Troubleshooting events and issues on your network
- Monitoring security alerts or issues
- Capacity planning

Configure the dashboard to continuously display the information that is most important for monitoring your network. Display the dashboard on a monitor in your Network Operation Center (NOC) or Security Operation Center (SOC) and the SMS will alert 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.

The following sections contain information about:

Default dashboard configuration on page 31 — The SMS Dashboard will be configured with several gadgets out of the box. You can customize the existing gadgets or add additional gadgets to display the information that you need to monitor.

Customize the SMS dashboard on page 38 — Customize your dashboard to provide the information you need to monitor for issues and react quickly.

Dashboard gadgets on page 31 — 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.

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* .

Default dashboard configuration

The SMS dashboard will be configured with several gadgets out of the box. 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 38 for information on how to customize your dashboard and *Dashboard gadgets* on page 31 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 32 — Monitor system health and report on the basic health and status of managed devices
- *Task Status gadgets* on page 33 — Distribution Status and Software Update Status
- *Inspection Event gadgets* on page 33 — 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 33 — The Event Rate gadget shows the overall number of filter-triggered events that the SMS is processing over a specified period of time.
- *Security gadgets* on page 34 — 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.
- *Reputation gadgets* on page 35 — Reputation gadgets are based on the Security filter type, but are further refined by the Reputation filter category.
- *Application gadgets* on page 35 — 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.
- *User gadgets* on page 36 — User gadgets display 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 37 — 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.

Security gadget	Description
Attacks	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.
Top Attack Destinations	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.
Top Attack Geographic Destinations	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.
Top Attack Geographic Sources	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.
Top Attack Sources	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.

Security gadget	Description
Top Attacks	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.

Reputation gadgets

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

Application gadget	Description
Application Events	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.
Top Application Destinations	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.

Application gadget	Description
Top Application Geographic Destinations	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.
Top Application Geographic Sources	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.
Top Application Sources	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.
Top Applications	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.

User gadgets

The SMS dashboard has been updated with two new gadgets to display the Active Directory information that you need to monitor. User gadgets display information based on user and user group query criteria, including 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 65.

The following table provides a description of dashboard user gadgets.

User gadget	Description
Top App Users	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.
Top Attack Users	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.

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.

Firewall gadget	Description
Top Applications by Bandwidth	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.
Top Applications by Hit Count	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.
Top Blocked Applications	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.

Firewall gadget	Description
Top IPs by Bandwidth	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.
Top Rules by Bandwidth	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.
Top Rules by Hit Count	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.
Top Users by Bandwidth	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.

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 39 – Select the color and contrast of the visual elements of the dashboard
- *Change the dashboard layout* on page 39 – Change the column widths or move gadgets around
- *Add or remove a gadget* on page 39 – Choose which gadget you want to see on the dashboard
- *Configure a gadget* on page 40 – 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** (360º 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 31 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 61
    - **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 42 — Filter, view, and save inspection events for all or specific devices, segment groups, and event filter elements.

Firewall events on page 44 — Filter, view, and save firewall rule hit events detected by the Firewall for all or specific devices, interfaces, zones, and rule filter elements.

Threshold filter state on page 72 — View, edit, and reset triggered Traffic Threshold filters.

Monitor events on page 46 — 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 59 — You can save, run, and manage queries through the **Events** screen. Saved queries display in the **SavedQueries** sections under **Inspection Events** and **Firewall Events** in the navigation screen.

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 428.

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

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 61.

Inspection Events table

The following table describes the columns in the Inspection Events table.

Column	Description
Time	Date and time that the event was processed by the inspection.
Severity	Indicates the importance of the event.

Column	Description
Name	Name of the filter that generated the alert or block.
Category	Type of event filter.
Action	Type of action for the filter.
Hit Count	Number of times the filter was triggered.
Profile	Profile associated with the alert or block.
Device	Name of the device responding to the traffic.
Segment/Rule	Segment for IPS-generated events, and rules for firewall-generated inspection events.
Src. Addr.	Source IP address of the traffic that caused the event. Expand this column for location details, including geography map, region, city, and named resource.
Src. Port	Port of the source IP address.
Src. User	Login name of the source user.
Client Addr.	The IP address of the attacking client. Expand this column for location details, including geography map, region, city, and named resource.
Dst. Addr.	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.
Dst. Port	Port of the destination IP address.
Dst. User	Login name of the destination user.
Seg	Number of the segment.

Column	Description
VLAN	VLAN on which the event took place.
Trace	Indicates if the event has a packet trace (or saved portion of the packet used in the event).
URI Hostname	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.
Comment	Information added by the user.

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 58.

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

Column	Description
Time	Date and time that the event was processed.
Event Type	Type of Event.
Hit Count	Number of times the event was triggered.
Src. Addr.	Source IP address of the system that sent the event. Expand this column for location details, including geography map, region, city, and named resource.
Src. Port	Source port of the source IP address.
Src. NAT	Source NAT address of the system that sent the event. Expand this column for location details, including geography map, region, city, and named resource.

Column	Description
Src. NAT Port	Source port of the NAT address.
Interface In	Interface where the event entered.
Src. Zone	The source zone where the source originated.
Dst. Addr.	Destination IP address of the system targeted in the attach. Expand this column for location details, including geography map, region, city, and named resource.
Dst. Port	Destination port of the destination IP address.
Dst. NAT	Destination NAT address of the system targeted in the event. Expand this column for location details, including geography map, region, city, and named resource.
Dst. NAT Port	Destination port of the Destination NAT.
Interface Out	Outbound Interface.
Dst. Zone	Destination zone of the event.
User Name	The user name of the account involved.
Application	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.
Transport Protocol	Actual protocol as reported by the firewall.
Action	Type of action for the filter.
Total Byte	Total number of bytes.

Column	Description
Profile	Firewall profile associated with firewall rules.
Device	Name of the device responding to the traffic.
Firewall Rule	The specific firewall rule that was triggered.
Session ID	The session ID in which the event occurred.
Trace	Indicates if the events has a packet trace (or saved portion of the packet used in the event).
Comment	Information added by the user.

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.

Option	Description
Copy	Provides the following options for copying data: • Selected Rows — Copies the selected rows. Use the Shift key to select multiple rows or the Ctrl key to select specific rows. • Cell Value — Copies the cell content data, such as an event name or IP address.
Export to File	Exports selected rows or all rows to a delimited text file. • **Selected Rows** — Exports the selected rows. Use the Shift key to select multiple rows or the **Ctrl** key to select specific rows.

Option	Description
	• **All rows** — Copies all currently viewed rows.
Find	Allows you to find a term or times listed in the table.
Details	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.
Event Comment	Adds annotation to event listing.
Search on	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.
ThreatlinQ	Displays globally aggregated information about filters, source IP addresses, and source/destination ports.
Packet Trace	Provides the following Packet Trace options: • View • Save • Download to the SMS • Configure View Settings
IP Addr ID Config	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.
Reputation	For both Inspection and Firewall events you can create a reputation entry 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.
New Traffic Capture	(Inspection Events only) Create a new traffic capture for a segment on the device.

Option	Description
Reports	(Inspection Events only) Provides the following report options: • Specific Filter Report • Specific Source Report • Specific Destination Report • Specific User Report • Specific Peer Report (Src. Addr.) • Specific Peer Report (Dst. Addr.)
Profile	(Inspection Events only) Allows you to edit filters, create exceptions, or create a Traffic Management filter.
Firewall Rule	(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.
Show Inspection Events	(Firewall only) Filter the Inspection Events table based on firewall event data for the following: • Source Address • Destination Address • Firewall Rule • Session ID
IP Lookup	• Geo Locator • Named Resource • DNS • User ID • Who is • Reputation • End Point Attributes

Option	Description
	• Multiple Lookups
Create Response	Create a manual response based on Source Address, Source NAT, Destination Source, and Destination NAT.
Query IDResolver	Provides access to IP address information for A10 Networks.
Create Named Source	Create a named source based on Source Address, Source NAT, Destination Source, and Destination NAT.
Table Properties	Allows you to define the order, visibility, sorting, and aggregation properties of each column in your 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 orclick 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 515.

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 Eventstable, 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 58.
- **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 51.
- **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 56 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
- Vendor

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 \x*HH* 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 102.

The system saves the packet trace to a packet capture (PCAP) file. The default filename uses the convention *SMSTrace-VulnerabilityId - FilterName* where *VulnerabilityId* and *FilterName* are unique identifiers of the event filter for which packet trace was enabled.

For more information, see *Packet trace (S-Series, N-Platform/NX-Platform)* on page 358.

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 358.

The **PCAP Download** option can be enabled through the **System Preferences** wizard. See *Configure PCAP download preferences* on page 19.

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 514.

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. The SMS provides easy access to the TMC by right-clicking. You can also access the utility from the top menu bar by selecting the **Tools > TMC** menu item. For information about configuring ThreatLinQ, see *ThreatLinQ* on page 26.

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 61 and *Inspection Events table* on page 42.

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

Section	Description
Filter Details	Enables you to enter the name and/or number of the filter.

Section	Description
Filter Category	Enables you to select one or more filter categories: • Application Protection • Exploits, Identity theft, Reconnaissance, Security Policy, Spyware, Virus, Vulnerabilities • Infrastructure Protection • DDoS, Network Equipment Protection, Traffic Normalization, Traffic Thresholds • Performance Protection • Instant Messaging, Peer to Peer, Streaming Media
Profile	Enables you to select an existing profile.
Filter Severity	Enables you to select the severity of the event.
Filter Type	Enables you to filter the events by Security or Application type.
Reputation Type	Enables you to filter the events by Reputation or Geographic filter. By default, both filters are selected. 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.
Action Type	Enables you to select the action; Permit, Block, or Active Response.

Create an inspection query with filter criteria

1. On the Events screen, click **Inspection Events** in the navigation pane.

   The Query pane displays.

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 42.

    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 63 and *Inspection Events table* on page 42.

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

Section	Description
Classification	Type of event.

Section	Description
Protocol	System communication methods, such as ldap, snmtp, ssh, etc.
Platform	OS-based applications, services or supported device, such as Windows Client, networked router, UNIX Client application, etc.

Create a query with filter taxonomy criteria

1. On the Events screen, click **Inspection Events** in the navigation pane.

   The Query pane displays.

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 42.

   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 64 and *Inspection Events table* on page 42.

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

Create a query with network criteria

1. On the **Events** screen, click **Inspection Events** in the navigation pane. TheQuery pane displays.
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 42.

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 42.

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

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 42.

    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 67 and *Inspection Events table* on page 42.

Section	Description
Segment	Group of hosts protected through a licensed pair of ports on a device.

Section	Description
Device	Devices managed by the SMS.
Firewall Profile	Firewall profiles managed by the SMS.

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.
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 42.

   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 102.

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 may 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. See *Right-click options* on page 72.

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* on page 111.

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 42.

   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
- 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 42.

   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.

Threshold filter state

Traffic Threshold filters enable the SMS to detect statistical changes in network traffic patterns. The SMS determines normal traffic patterns based on the network statistics over time, and traffic threshold filters generate alerts when network traffic varies from the norm.

Through the **Threshold Filter State** screen, you can review, edit, and reset Traffic Threshold filters.

Right-click options

Right-click on an entry in the filter list to select **Edit**, **Reset**, and **Reset All** options.

You can perform the following tasks:

- *Edit a traffic threshold filter* on page 73
- *Reset a traffic threshold filter* on page 73
- *Reset all traffic threshold filters* on page 74

See *Reputation filters* on page 160.

Edit a traffic threshold filter

1. On the Events (Threshold Filter State) screen, select a filter.
2. Right-click the selected filter and select **Edit**.

   The Filters - Traffic Threshold - Edit dialog opens.
3. Enter the Traffic Threshold Filter Name. The profile for the filter displays below the name.
4. For Filter Parameters, modify one or more of the following:
   - Select the direction of the flow for the segment ports: **A to B** or **B to A**.
   - Select the Units per Second and the amount to be based on.
   - The unit values include packets, bytes, and connections. The period values include the last minute, hour, day, 7 days, 30 days, and 35 days.
   - For Monitoring, select an option: **Monitor only** or **Monitor with thresholds**.
   - The Monitor only option sets the system to generate a report without triggering traffic thresholds.
5. For Thresholds, you can modify up to 4 thresholds for each filter. For each of the following options, enter a value in percent and select an action set.
   - Enable Above Normal Major
   - Enable Above Normal Minor
   - Enable Below Normal Major
   - Enable Below Normal Minor
6. For the Type, select and modify one of the following:
   - **Protocol** — Select the type of protocol from the drop-down list, including **TCP**, **Other**, **ICMP**, and **UDP**.
   - **Application** — Select the type of protocol and enter the **Port**. Select one of the following to apply the type to: **requests**, **replies**, or **both**.
7. Click **OK**.

Reset a traffic threshold filter

1. On the Events (Threshold Filter State) screen, select a filter to reset.
2. Right-click the entry and select **Reset**.
3. The Traffic Threshold filter resets. To modify the filter to keep it from constantly triggering, edit the settings. See *Edit a traffic threshold filter* on page 73.

Reset all traffic threshold filters

1. On the Events (Threshold Filter State)screen, click **Reset All**.
2. All Traffic Threshold filters reset. To modify a filter to keep it from constantly triggering, edit the settings of a particular filter. See *Edit a traffic threshold filter* on page 73.

   To view the details about an event, you need to locate the event and display it. Each entry includes information on the device, segment, and issues of the triggered event. 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 58.

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 *Overview* on page 523.

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.

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 y 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, Traffic Threshold, 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 76.
- **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 90.
- **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 94.
- **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 93.
- **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 98.

- **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 100

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 445.

AD User reports

The SMS report templates have been updated with two new security reports:

- Specific User
- Top User

The SMS also includes two new 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 92.

Use this criteria panel...	To filter the report by:
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. • **Major** — Indicates major attacks that must be looked at soon. • **Minor** — Indicates minor attacks that should be looked at as time permits. • **Low** — Indicates traffic that is probably normal, but may have security implications.
Filter Taxonomy Criteria	Classification, protocol, and/or platform. Click the Lookup icon to quickly search the list.
Network Criteria	Addresses and Ports, VLAN, country, and/or client IP.
User Info Criteria	Login IDs of source/destination users and user groups, and the IP addresses of the source/destination domains and machines.
Device, Segment, Rule Criteria	Segment, device, and/or firewall profile and rules. • Click **Add** to add a device, segment, or firewall profile. • Click **Delete** to remove an existing device, segment, or firewall profile.
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:

Use this criteria panel...	To filter the report by:
	• Chart Type • Classification labels • Include All Details Table • Number of matching details • Report logo • Report style • Security Classification label • Inbound, Outbound, or both (Bandwidth reports)

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 92.

Use this criteria panel...	To filter the report by:
Application, Transaction and User Criteria	Application groups, individual applications in the digital vaccine, transactions of those applications, and/or specific users to be included or excluded.
Firewall Policy Criteria	Existing firewall profiles and rules. On this panel, you can also dictate severity and actions. • Click **Add** to add a profile or rule. • Click **Remove** to remove an existing profile or rule.
Device, Interface Criteria	Segment, device, and incoming and/or outgoing interfaces. • Click **Add** to add a device, device group, or interface. • Click **Delete** to remove an existing device, device group, or interface.
Network Criteria	Addresses and Ports, Security Zones, VLAN, and/or country.
Network Address Translation Criteria	Source NAT addresses, ports, and/or country and Destination NAT addresses, ports and/or country.
Schedule, Service Criteria	Included or excluded schedules and services.

Use this criteria panel...	To filter the report by:
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 • 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 92.

Use this criteria panel...	To filter the report by:
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. • **Major** — Indicates major attacks that must be looked at soon. • **Minor** — Indicates minor attacks that should be looked at as time permits. • **Low** — Indicates traffic that is probably normal, but may have security implications.
Filter Taxonomy Criteria	Classification, protocol, and/or platform. Click the Lookup icon to quickly search the list.
Network Criteria	Addresses and Ports, VLAN, country, and/or client IP.
Device, Segment, Rule Criteria	Segment, device, and/or firewall profile and rules. • Click **Add** to add a device, segment, or firewall profile. • Click **Delete** to remove an existing device, segment, or firewall profile.

Use this criteria panel...	To filter the report by:
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 • Number of matching details • Report logo • Report style • Security Classification label

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 92.

Use this criteria panel...	To filter the report by:
Device / Rate Limit Criteria	Device or Rate Limit action set.

Use this criteria panel...	To filter the report by:
	• Click **Add** to add a device. • Click **Remove** to select or clear Rate Limit action sets.
Device Rate Limit Report Options	Time (minute, hours, or days) and/or throughput.
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 • 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.

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 92.

Use this criteria panel...	To filter the report by:
Device Criteria	Device or specific segment of a device.
Device Traffic Report Options	Time (minute, hours, or days), data display, data aggregation, and/or traffic direction.
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 • Number of matching details • Report logo • Report style • Security Classification label

Traffic Threshold templates

The Traffic Threshold report provides options for reporting statistical changes in network traffic patterns. Thresholds trigger when traffic edges the set amounts. When traffic exceeds a threshold and returns to normal levels, the system generates an alert. These alerts inform you of the triggered filter; when the thresholds are exceeded and when they return to normal; and the exceeded amount. These amounts include an amount exceeded above and below normal levels.

The SMS includes one traffic threshold report template: Traffic Thresholds.

Traffic Threshold criteria panels

The following table lists the criteria panels that are available for the traffic threshold 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 92.

Use this criteria panel...	To filter the report by:
Filter Criteria	Details including filter name and number, category, profile, severity, 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. • **Major** — Indicates major attacks that must be looked at soon. • **Minor** — Indicates minor attacks that should be looked at as time permits. • **Low** — Indicates traffic that is probably normal, but may have security implications.
Segment Criteria	Segment groups of a device.
Traffic Threshold Report Options	Time (minute, hours, or days).
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 • Number of matching details • Report logo • Report style • Security Classification label

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 92.

Use this criteria panel...	To filter the report by:
Filter Criteria	Inspection Profile and Advanced DDoS filters are required to run this report.
Segment Criteria	Segment groups of a device.

Use this criteria panel...	To filter the report by:
Advanced DDoS Report Options	Time (minute, hours, or days) and/or one or more DDoS types.
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 • Number of matching details • Report logo • Report style • Security Classification label

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

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 92.

Use this criteria panel...	To filter the report by:
Filter Criteria	Details including filter name and number, profile, severity, 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. • **Major** — Indicates major attacks that must be looked at soon. • **Minor** — Indicates minor attacks that should be looked at as time permits. • **Low** — Indicates traffic that is probably normal, but may have security implications.
Filter Taxonomy Criteria	Classification, protocol, and/or platform. Click the Lookup icon to quickly search the list.
Network Criteria	Addresses and Ports, VLAN, country, and/or client IP.
Device, Segment, Rule Criteria	Segment, device, and/or firewall profile and rules. • Click **Add** to add a device, segment, or firewall profile. • Click **Delete** to remove an existing device, segment, or firewall profile.
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

Use this criteria panel...	To filter the report by:
	• Number of matching details • Report logo • Report style • Security Classification label

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.

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 92.

Use this criteria panel...	To filter the report by:
Protocols, Services Criteria	Protocols, such as GGP, ICMP, TCP, and UDP, and services to be included or excluded. 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.

Use this criteria panel...	To filter the report by:
Segment, Device Criteria	Available physical segments and devices. • Click **Add** to add a device, device group, or physical segment. • Click **Remove** to remove an existing device, device group, or physical segment.
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 93.

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 ora 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 94.
    - **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**.

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

popular document format, such as a PDF; or delete a report result. For more information about tracking report results, see *Report results* on page 96.

- **Manage report schedules.** Use the Schedules table to drill down into the schedules for a saved report. You can create a new report schedule; edit the result settings and permissions of a report result; export a report result to a local file, email, or external source; or delete a report schedule. Alternatively, you can access this information on the All Schedules table. For more information about viewing all report schedules, see *All schedules* on page 100.

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 90.

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 90.
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 rew 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 94.

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

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**.

   The Report Results table opens.

2. Select a report title, and then click **Open**.

   The report opens in a new window.

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 ora 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**.

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 or rules that provide a method for setting up security configuration options for TippingPoint solutions. The SMS ships with default security and firewall profiles 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.

The Profiles screen provides a comprehensive, centralized interface for managing, editing, and applying profiles and shared settings, including action sets, contacts, and services. This screen also allows you to download and distribute Digital Vaccine packages.

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

- Enterprise-wide — These settings affect all devices and segments on your network. Examples of these are in the Shared Settings, including action sets, shared exceptions, and notification contacts. Digital Vaccine and DVT packages also fall under this type of protection, as you can distribute these packages to all devices.
- Device-wide — These settings affect all of the segments on a particular device. Digital Vaccine and DVT 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; segmental settings do not affect an entire device. An example of these includes an inspection profile distributed to a segment group.

Note: Virtual segments are used with V2.5 and later devices. For V2.5 and above, physical segments can be used but cannot be created. See *Virtual segments* on page 279.

Filters are a part of security profiles and can be customized to address specific network security needs. Filters are policies with settings and rules for managing and blocking traffic on a network. Each filter includes an action set that contains instructions for managing data and a category setting. The Threat Management Center assesses each filter and assigns it to one of the categories. See *Filters* on page 587.

Profiles

The SMS supports the following types of network security profiles:

- *Inspection profiles* on page 121 — a collection of filters that is key to protection and prevention of malicious invasion on your network and data. IPS devices support IPS Profiles.
- *Firewall profiles* on page 170 — Firewall profiles are a collection of rules created to permit or block network traffic between devices separated by the firewall, such as employees' PCs and Internet websites.

Hosts in your network are protected by the *profiles* installed on each device. Profiles apply threat recognition data to traffic passing through specific areas of your network.

Profile support areas

The following items support profiles:

- *Digital Vaccines* on page 182 — 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 TippingPoint Threat Management Center (TMC) researches, creates, and distributes these filter packages from the Threat Management Center website at: *https://tmc.tippingpoint.com/TMC/*
- *Auxiliary DV* on page 191 — 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.
- *Digital Vaccine Toolkit* on page 194 — An optional, stand-alone, TippingPoint application that lets you write custom filters for use on IPS and SMS devices.
- *Reputation database* on page 203— Collection of IP addresses and DNS names on an SMS that represent potential risks to network security. This information may be user provided, ThreatDV provided, or both.

Planning and using profiles

As you create, import, export, 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 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.

When devising your network security using the TippingPoint system, you should plan to create profiles based on your security needs. You may need to create custom filter settings, exceptions, and limitations for profiles to protect external and internal services. You may also 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 in the SMS. You can then associate and distribute profiles to devices through segment groups.

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 428.

Navigation and menu options

To open the Profiles workspace, click **Profiles** on the SMS toolbar. From here, you can manage your system response to attack traffic, customize shared settings, configure VPN, and implement Digital Vaccine packages.

Note: You must distribute any modifications to the inspection and firewall devices for your changes to take effect. See *Distributing profiles* on page 128.

From the left navigation pane on the Profiles workspace, you can manage the following types of profiles and network protection packages:

- *Shared settings* on page 105 - Shared Settings include common configuration objects that are shared by all profiles on the SMS. They include:
  - *Action sets* on page 106 - Create groups to determine what the policy is when traffic triggers a filter or firewall rule
  - *Application groups* on page 111 - Create groups of applications using query criteria or by selecting applications individually so the groups can be used in other policy settings.
  - *Notification contacts* on page 112 - The collections of email, syslog, or snmp contacts that will be used for notification when a policy event occurs.
  - *Schedules* on page 115 - Create and manage schedules specifying when to include or exclude traffic evaluation.
  - *Security zones* on page 116 - Create groups of interfaced from one or more devices that can be used to define policy
  - *Services* on page 117 - Configure additional ports associated with specific applications, services and protocols to expand scanning of traffic.
  - *Service groups* on page 119 - Create groups of services to make management of services easier.
  - *SSL Servers* on page 120 - Manage SSL server configurations.
- *Inspection profiles* on page 121 - Encapsulate all inspection filters, global exceptions, and updates for distribution to the system. Profiles contain filters that apply threat recognition data to traffic passing through specific areas of your network. These filters include:
  - Default profile
  - User-created profiles
- *Firewall profiles* on page 170 - Firewall rules are created to permit or block network traffic between devices separated by the firewall such as employees' PCs and internet Web sites.
- *Digital Vaccines* on page 182 - Import and distribute a Digital Vaccine package to devices on the SMS system.
- *Digital Vaccine Toolkit* on page 194 - Import and distribute a DVT package to devices on the SMS system.

Global search

The global search option allows you to search for inspection profiles. See *Search options* on page 139 and *Digital Vaccines* on page 182.

Note: The standard search option listed in the tree for each profile supports filter search within a selected profile.

Shared settings

Shared Settings include common configuration objects that are shared by all profiles on the SMS. These settings include:

- *Action sets* on page 106 — Create groups of to determine what the policy is when traffic triggers a filter or firewall rule.
- *Application groups* on page 111— Create groups of applications using query criteria or by selecting applications individually so the groups can be used in other policy settings.
- *Notification contacts* on page 112 — The collections of email, syslog, or snmp contacts that will be used for notification when a policy event occurs.
- *Schedules* on page 115— Schedules enables you to create and manage schedules specifying when to include or exclude traffic evaluation.
- *Security zones* on page 116— Create groups of interfaced from one or more devices that can be used to define policy.
- *Services* on page 117 — Configure additional ports associated with specific applications, services and protocols to expand scanning of traffic.
- *Service groups* on page 119 — Create groups of services to make management of services easier.

Shared settings affect all categories of filters in the entire system. All settings entered and modified in Shared Settings affect all profiles. When you create or modify any of these settings, all devices and their segments receive the available settings.

Note: The system does not create a set of Shared Settings for each profile. All settings entered and modified in Shared Settings affect all profiles.

Right-click on entries in the any of the list settings except Notification Contacts to do the following:

- Copy —You have the option to copy just the cell contents or the entire row. When copied, the actual value of the cell is pasted (true/false) along with the column headings.
- Export to file — You can choose to export a single row or all of the rows to either a plain text file or a comma delimited file. Options are available for including headings or not including headings in the export.

- Find — Search for a setting.
- New — Create a new action set.
- Edit — Edit a selected action set.
- Delete — Delete a selected action set. You can only delete action sets you create.
- Table properties — Allows you to define the order, visibility, sorting and aggregation properties of each column in your table.

Action sets

Action sets determine what the happens when a packet triggers a filter. An action set can contain more than one action, and can contain more than one type of action. You can globally affect all action sets for pillars in the SMS. When you modify or add an action set, the settings change enterprise-wide for all filters using the action set.

The Action Sets table displays the following information.

Setting	Description
Name	Displays the name of the action set.
Flow Control	Defines the type of action to be performed, such as block, permit, or trust.
TCP Reset	Indicates if the action set has a TCP reset setting enabled (for either source, destination, or both).
Rate Limit	Indicates if the action set provides the Rate-Limit action enabled.
Console	Indicates that the option to send notifications to the SMS console is enabled.
Response	Indicates that an SMS Active Response action is enabled.
Email	Indicates if the action set has notification contacts enabled.
SNMP	Indicates if the action set has SNMP engine enabled.
Remote Syslog	Indicates if the action set has syslog logging enabled.

Setting	Description
Packet Trace	Indicates if the action set has packet trace logging enabled.

Note: When you distribute a profile, all shared settings are also distributed. To distribute action sets, distribute a profile.

Create or edit an action set

1. On the Profiles navigation pane, expand **Profiles**, and then expand **Shared Settings**.
2. Click **Action Sets**.
3. Click **New** to create a new action set.

   The Create Action Set wizard opens.
4. Enter a **Name** for the action set.
5. Select a **Flow Control**.
   - **Permit** — Permit traffic associated with this action set.
   - **Block** — Block traffic; select **TCP Reset** to reset the source, destination, or both IPs of an attack.
   - **Quarantine** — Enable quarantine and to provide settings and exceptions for managing quarantines. Selecting this option will also enable the **Quarantine Settings** and **Quarantine Exceptions** options.
   - **Rate Limit** — Limit the traffic rate and select a predefined bandwidth.
   - **Trust** — Trust traffic associated with this action set.

   See *Flow control* on page 108 for more details:
6. Click **Next** or select **Notifications** from the wizard navigation pane.
7. Select the appropriate Notifications options.

   See *Notifications* on page 109 for more details.
8. Click **Next** or select **Packet Trace** from the wizard navigation pane.
9. To enable the packet trace, select the **Packet Trace** check box and complete the following items:
   - In the Level field, select **Full** or **Partial**. If you select **Partial**, enter the number of bytes.
   - In the Priority field, select **High**, **Medium**, or **Low**.
10. If you selected Quarantine flow control, configure Quarantine Settings and Exceptions.

    See *Quarantine settings* on page 110 and *Quarantine exceptions* on page 110 for more details).
    Otherwise, skip this step.

11. After entering information on the final screen, click **Finish**.

Default action sets

The SMS provides default action sets that can be edited and customized to your specific needs. You can also create new action sets.

Type	Description
Block	Blocks a packet from being transferred to the network.
Block + Notify	Blocks a packet from being transferred and notifies the SMS management console in the form of an event listing.
Block + Notify + Trace	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.
Permit + Notify	Permits a packet and notifies the SMS management console in the form of an event listing.
Permit + Notify + Trace	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.
Trust	Allows the traffic stream to continue without comparing it with any other filter rules.

Manage action sets

Use action sets to create a new action set, edit an existing or default action set, or delete an action set.

Flow control

Flow control specifies the actions taken with a packet after it triggers a rule. The options include the following:

- Permit — Allows a packet to reach its intended destination.

- Block — Discards a packet. The TCP Reset option enables the device to reset TCP flows, which ends the session. With TCP Reset, you can set the option to reset the source IP, the destination IP, or both. See *Create or edit an action set* on page 107 for more information.
- Quarantine — Manages internal and external threats by quarantining network connections. This option provides the ability to automate sophisticated responses to security events. By enabling quarantine, you reduce the exposure of your network to internal and external threats. When an IP address/system is quarantined, use the Responder > Response History screen to review the list and manage the status of these systems. See *Working with the Responder (Response History)* on page 228.

Note: For devices using v. 3.1 TOS and later, you have the option to either block or permit the packets until the threshold settings are reached. For devices prior to v. 3.1, Quarantine blocks the first packet that triggers the action, regardless of the quarantine settings specified. all other packets after that are managed according to the quarantine settings for that action set.

- Rate Limit — Enables you to define a maximum bandwidth that can be used by traffic that matches filters assigned to that action set. Incoming traffic exceeding this bandwidth is dropped. If two or more filters use the same rate limiting action set, then all packets matching those filters share the bandwidth. For example, if filters 164 (ICMP Echo Request) and 161 (ICMP Redirect Undefined Code) use the same 10 Mbps "pipe" as opposed to 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% of the total bandwidth of the product.
- Trust — Allows a packet from a specific IP address to flow through.

Notifications

Notifications establishes the contacts to notify about the event. Contacts can be systems, individuals or groups. The notification options include the following:

- Management Console—Notifies the SMS upon a filter hit. This generates an event in the Events area of the SMS.
- SMS Response —Indicates the Active Response Policy to be associated with the filter hit.

Note: The Active Response Policy must have Enable Policy enabled in order to appear in this list. See *Responder* on page 227.

- Remote Syslog — Indicates whether remote syslog entries should be sent to the server(s) designated in Server Properties.
- Email— Filter hits generate an email message to each of the email contacts listed in the table. See *Create or edit an email notification contact* on page 113.
- SNMP— Filter hits generate an SNMP trap to each of the SNMP contacts listed in the table. SNMP notification contacts require SNMPv2.

Packet trace

Packet provides packet trace options for tracking. The packet trace options include the following:

- Packet Trace— Allows you to capture all or part of a suspicious packet for analysis. You can set the packet trace priority and packet trace verbosity for action sets.
- Level— Determines how much of a suspicious packet will be logged for analysis. If you choose full verbosity, the whole packet will be recorded. If you choose partial verbosity, you can choose how many bytes of the packet (from 64 to 1600 bytes) the packet trace log records.
- Priority— Sets the relative importance of the information captured. Low priority items will be discarded before medium priority items if there is a resource shortage.

Quarantine settings

Quarantine settings allows you to set quarantine hit count and time thresholds, manage all HTTP traffic from the quarantined addresses, and configure a response to non-HTTP traffic. The quarantine settings options include the following:

- Thresholds— Configures hit count (1-10,000), and period in minutes (1-60). Determines whether traffic is permitted or blocked before threshold is reached, and enables you to reset blocked TCP flows.
- Web Requests— Manages all HTTP traffic from the quarantined addresses. You can configure the SMS to block the requests entirely, redirect the client to another Web server that you specify, or display the quarantined Web page according to options you select. If you select the option "Display quarantine Web page" you can select to display:
  - Show the filter causing the quarantine action.
  - Show the description of the filter causing the quarantine action.
  - Show customized HTML, that you specify in the text field. You can include HTML code in this field with a maximum of 1500 characters.

Note: When entering HTML code for the message, do not use <frameset> and the <form> HTML tags.

- Other Traffic— Configures the response (Block or Permit) to other non-HTTP traffic from hosts listed in the Active Response History queue.

Quarantine exceptions

Quarantine exceptions creates a list of "limit to" IP addresses, excluded IP addresses or exceptions, and enables quarantine access. The quarantine exceptions options include the following:

- Restrictions— Allows you to create a list of "limit to" IP addresses, or Restrictions. This option limits the quarantine action to specified IP addresses.
- Exceptions— Allows you to create a list of excluded IP addresses, or Exceptions, which will not receive a response action. Despite the filter triggering, these IP addresses will not receive a response action,

continuing with any other commands in the action set. For example, the action set may include response commands to block the traffic and redirect Web requests to a particular server.

- Quarantine Access— When a client is detected as malicious and is quarantined, network administrators may need to allow access to specific Web sites to remedy their situation. This feature provides a list of hosts to enter that clients can still access regardless of being quarantined.

Application groups

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. On the Profiles navigation pane, expand **Profiles**, and then expand **Shared Settings**.
2. Select **Application Groups**. Click **New** to create a new Application Group or **Edit** to edit one. An Application Group wizard opens.

   Note: The SMS must be managing an NGFW device for the **Application Groups** option to appear.

3. Enter a **Name** for the application group.
4. Enter a **Description** of the 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.
6. 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 subapplication criteria, which are included in the digital vaccine and are unrelated to transactions, match traffic. The Transaction field of any generated logs remains empty.

7. Click **OK**.

Because criteria can contain multiple entries, 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 subapplication 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.

Notification contacts

Alerts are messages that are sent to a specific recipient (either human or machine) when traffic flowing triggers a filter that requires notification. *Alert aggregation for notifications* on page 114 determines how frequently alerts for the same filter will be sent. These alerts are sent to notification contacts set for action sets.

When you create or edit an action set, you have the option to inform specified *contacts* about matching traffic. Contacts include the *management console*, which encompasses both the SMS and LSM, Firewall, email addresses, SNMP servers, and the remote syslog. The management console is a default contact. Any other contacts must be added to your system. When you modify or add a notification contact, the settings change enterprise-wide (or to all devices and segments). Through the Notifications Contacts screen, you can also set the aggregation amounts for the Management Console and Remote Syslog.

To use email contacts, you must complete the Mail Server panel of the Configuration window for each IPS. For all contacts, you must specify an *aggregation period*. The aggregation period is the amount of time that the system accrues information about attack traffic before it sends a notification.

For example, a user may want to be notified about all UDP flood commands that have occurred within a five-minute period.

Note: The SMS limits the number of e-mail alerts sent in a minute. This feature supplements the currently used aggregation functionality in the SMS. The system by default allows the sending of ten (10) email alerts per minute. On the first email alert, a 1 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.

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 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.

Note: When you distribute a profile, all shared settings are also distributed. To distribute notification contacts, distribute a profile.

A remote syslog server is another channel that you can use to report filter triggers. Remote syslog sends filter alerts (which must be configured for every device using that contact) to a syslog server on your network. See *Create or edit an email notification contact* on page 113.

Caution: Only use 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.

Tip: For more information about syslog, consult the syslog server documentation that came with your operating system or syslog software.

The **Notification Contacts** page displays the following information:

- **Global Contacts**
  - Management Console (aggregation setting is in minutes)
  - Device Remote Syslog (aggregation setting is in minutes)
- **Email Contacts**
  - Name
  - Email Address
  - Aggregation
- **SNMP Contacts**
  - Name
  - SNMP Host
  - Port Aggregation

For information on associating a notification contact to an action set, see *Action sets* on page 106.

Create or edit an email notification contact

1. On the Profiles navigation pane, expand **Profiles**, and then expand **Shared Settings**.
2. Click **Notification Contacts**.

3. On the Email Contactspanel, do one of the following:
   - Click **New** to create a new contact.
   - Select an existing contact, and then click **Edit**. The Email Contact wizard opens.
4. In the **Name** field, provide or modify the name of the contact.
5. In the **Email Address** field, provide or modify the email address for the contact, for example, bob@mail.com. The limit is 36 characters for email addresses.
6. In the **Aggregation** field, specify or modify the number of minutes that the device will accrue alerts before it sends a notification.
7. Click **OK**.

Create or edit an SNMP notification contact

1. On the Profiles navigation pane, expand **Profiles**, and then expand **Shared Settings**.
2. Click **Notification Contacts**.

   Note: SNMP notification contacts require SNMPv2, and will not work when SNMPv2 is disabled.
3. On the **SNMP** section, do one of the following:
   - Click **New** to create a new SNMP notification contact.
   - Select an existing SNMP notification contact, and then click **Edit**. The SNMP Contacts wizard opens.
4. In the **Name** field, provide the name of the contact.
5. In the **SNMP Host** field, provide or modify the SNMP host for the contact.
6. In the **SNMP Port** field, specify the port number for the contact's SMNP host (typically, 162).
7. In the **Aggregation** field, specify the number of minutes that the device will accrue alerts before it sends a notification.
8. Click **OK**.

Alert aggregation for notifications

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 notification at intervals to prevent this flooding.

For example, if you set the aggregation period to five minutes, you will receive an email at the first trigger of a filter, and then subsequent alerts will be collected and then sent every five minutes.

See *Create or edit an email notification contact* on page 113.

Aggregation period

Alert notification is controlled by the aggregation period that you configure when you *Create or edit an email notification contact* on page 113. The aggregation period is the amount of time that the device will accrue alerts before it sends a notification. The first time a particular filter is triggered, a notification is sent to the alert contact target. At the same time, the aggregation timer starts ticking down the aggregation period.

During the aggregation period, further packet triggers are counted, 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 will continue to cycle as long as the filter in question is active.

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.

Set aggregation settings for global contacts

1. On the Profiles navigation pane, expand **Profiles**, and then expand **Shared Settings**.
2. Select **Notification Contacts**.
3. For the **Management Console Aggregation**, enter an amount of minutes from 0 to 10,800.
4. For the **Device Remote Syslog Aggregation**, enter an amount of minutes from 0 to 10,800.
5. Click **Save**.

Schedules

Schedules enables you to create and manage schedules specifying when to include or exclude traffic evaluation.

Each schedule consists of a name and one or more intervals. An interval is defined by days, start time, and end time. For example, one interval might be defined as Tuesday and Thursday, between 8:00 AM and 5:00 PM. Each schedule can include up to four intervals.

Access the Schedules screen from **Profiles** > **Shared Settings** > **Schedules**. The Schedules screen displays a list of the schedules that have been created on the SMS. 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 a schedule

1. On the Profiles navigation pane, expand **Profiles**, and then expand **Shared Settings**.
2. Click **Schedules**.

3. On the Schedules screen, click **New**.
4. In the Create Schedule dialog, provide a **Name** for the new schedule.
5. Click **New** at the bottom of the Schedule panel.
6. In the Schedule - Time Interval dialog, select the days and specify start and end times to define the interval.

   Note: Note that 12:00 AM is considered to be midnight and 12:00 PM is interpreted as noon. Also, the start time and end time always occur in the same day. That is, a valid time interval never has a start time before midnight and an end time after midnight.

7. Click **OK**.
8. Repeat the previous three steps to create each time interval.

   Note: A schedule can include up to four time intervals.

9. Click **OK** to close the Create Schedule dialog.

Edit a schedule

1. Select a schedule in the list, and then click **Edit** or double-click on a schedule or interval.
2. In the Edit Schedule dialog, edit the schedule name or start and end times as needed.

   If the schedule contains multiple intervals, select an interval, and then click **Edit** to open the Time Interval dialog.

3. Click **OK** to save your changes.

Delete a schedule

1. Select a schedule in the list, and click **Delete**.
2. In the Delete Confirmation dialog, click **OK**.

   Note: You cannot delete a schedule that is used by one or more firewall rules, whether or not the rule has been distributed.

Security zones

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 and edit security zones

1. On the Profiles navigation pane, expand **Profiles**, and then expand **Shared Settings**.
2. Click **Security Zones**.
3. On the Security Zones pane, do one of the following:
   - Click **New** to create a new security zone.
   - Select an existing security zone, and then click **Edit**. The Security Zone wizard opens.
4. In the **Name** field, provide a name for the security zone.
5. In the **Description** field, provide a description for the security zone.
6. Select **Application Visibility** if you want to monitor applications passing through the zone.

   Note: This will force additional inspection of the traffic as it passes through the device and could affect performance.
7. Click **Add** to add interfaces to the zone. Select the interface(s) in the Select Interfaces dialog, and then click **OK**.
8. To remove interfaces, select the interface in the Member Interfaces list, and then click **Remove**. Press Ctrl and click to select more than one interface.
9. Click **OK** to save the security zone settings.

Services

To enhance scanning and detection of malicious traffic, the SMS provides management of services. This feature enables you to 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 engine then accesses and scans traffic against the list of additional ports. Each service supports 16 additional ports to configure.

The **Shared Settings** > **Services** page displays the following information:

Column	Description
Name	Name of the service or protocol.
Description	Description or expanded name of the service or protocol.
TCP	Lists the TCP ports.

Column	Description
UDP	Lists the UDP ports.
IP Protocol	List the IP Protocol by number.
Service Type	How the service is being monitored - Firewall or Inspection.
User Modified	Whether or not the entry has been modified from the default settings.

Add a non-standard port

1. On the Profiles navigation pane, expand **Profiles**, and then expand **Shared Settings**.
2. Click **Services**, select a service name, and then click **Edit**.

   The Edit Service dialog box for that service displays.
3. Click **Add**.

   Each service supports 16 additional ports.
4. Enter a **Port** number.
5. Click **Save**.
6. Click **OK**.

Delete a non-standard port

1. On the Profiles navigation pane, expand **Profiles**, and then expand **Shared Settings**.
2. Click **Services**, select a service name, and then click **Edit**.

   The Filters - Service - Edit dialog box displays.
3. Select a port to delete, and then click **Delete**.
4. Click **OK**.

Add a new service

1. On the Profiles navigation pane, expand **Profiles**, and then expand **Shared Settings**.
2. Click **Services**, and then click **New**.

   The Create Service wizard opens.
3. In the **Name** field, enter a unique name.

4. In the **Description** field, enter a description for the service.
5. In the Create Service wizard navigation pane, select **TCP/UDP Ports**, and then click **Add** to add TCP/UDP ports.
6. Specify whether you want to add TCP ports, UDP ports, or both by selecting the appropriate radio button. Choosing both will duplicate the information for both TCP and UDP ports.

   Note: A maximum of 16 additional ports are allowed per protocol. For inspection device service **HTTP**, the limit is a maximum of 8 additional ports.

7. Enter the port number or the range of ports.
8. Click **OK**.
9. Select **IP Protocols** in the Create Service wizard navigation pane.
10. In the Specify IP Protocol dialog, specify the IP protocol number, and then click **OK**.
11. Select **ICMP Types and Codes** in the wizard navigation pane.
12. Define the ICMP entry by choosing the version, type, and code:
    - **Any** — Does not specify a specific type and code value. It will match any valid type and code.
    - **Predefined** — Choose from a list of known type and code combinations.
    - **Specified** — Pick any Type and Code values between 0 and 255. You have the option of choosing **Any** for Code.
13. Click **Ok**.
14. Click **Quick View** at the bottom left of the Create Service panel to review your choices.
15. Click **OK** to save the service.

Service groups

Service groups allow you to group services together, similar to application groups, in a single element to make it policy management easier.

Create and edit service groups

1. On the Profiles navigation pane, expand **Profiles**, and then expand **Shared Settings**.
2. Select **Service Groups**, and then click **New** to create a new service group.

   The Create New Service Group wizard opens.

3. Enter a **Name** for the service group.
4. Enter a **Description** of the group.
5. Add services to the group by either select 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**.

SSL Servers

An SSL Server specifies the SSL server configuration.

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

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`. We recommend naming 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 2200T to write log information about SSL inspection to the external log disk (external Cfast). 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 2200T 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 533.
- **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 2200T blocks an SSL session. This option overrides the TCP reset action set, if enabled, on a DV filter. We recommend that you 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**. You are now ready to assign the SSL Server to an SSL inspection policy.

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.

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 IPS profile.

Inspection profiles

The Inspection Profiles Main Interface screen provides a centralized location for managing Inspection profiles.

Inventory pane

The Inventory pane on the Inspection Profiles screen provides a list of profiles and top-level information about the profiles and profile hierarchy. To see all the profiles in a hierarchy, expand the top-level profile entry.

Column	Description
Name	Name of the profile.
Version	Version number for the profile.
Modified	Date and time the profile was last modified.
Distributed	Date and time the profile was last distributed successfully.
Changed	**Yes** indicates that the profile has changed since the last time it was distributed. **No** indicates that the current version on the SMS is the same version distributed to devices.
Deployment	Type of deployment for the profile (default, aggressive, core, edge, perimeter).

This area supports the following profile management tasks:

- **Import** — Imports a profile as a new profile or replaces an existing profile with the option to add any new setting or change existing settings.
- **Export** — Exports an existing profile to either a local file, the SMS http server, or an external SMB or NFS server.
- **Distribute** — Distributes a profile or profiles to IPS devices in your network.
- **New** — Creates a new profile.
- **Save As** — Saves an existing profile using a different name.
- **Compare** — Views the difference between profiles. Edits profiles, filter, and category setting across multiple profiles.
- **Details** — Views profile details. Edits profiles.
- **Delete** — Removes a profile.

Distribution progress pane

Perform the following distribution tasks from the Distribution Progress pane on the main Inspection Profile screen:

- **Details** — Displays the status details for a selected profile distribution entry in the table.
- **Stop Distribution** — Stops a profile distribution.
- **Clear Obsolete** — Clears entries from the table.

Column	Description
Device	The name of the device to receive the distributed profile.
Package	The name and version of the profile distributed.
Start Time	The date and time when the distribution process began for the device.
End Time	The date and time when the distribution process ended for the device.
Status	The status of the distribution, such as *Complete (Success)*.
Progress	Current progress of the distribution by percentage complete.

Note: If you receive errors or have issues distributing profiles due to exceeded limits of filters or exceptions, see *SMS error messages* on page 574.

See *Distribute inspection profiles* on page 127.

Management tasks

Basic inspection 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. You can also edit multiple profiles.

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. 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 later modify the name and description of the copy from the Details screen of the

profile. After you copy/create filters, modify settings, and update Shared Settings (including action sets, notification contacts, and services), you must distribute the changes to the devices managed by the SMS.

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.

Common Profile Management tasks include:

Task	Description
Import	Import a profile as a new profile or replaces an existing profile with the option to add any new setting or change existing settings.
Export	Export an existing profile to either a local file, the SMS http server, or an external SMB or NFS server.
Distribute	Distribute a profile or profiles to IPS devices in your network.
New	Create a new profile.
Save As	Save an existing profile using a different name.
Compare	View the difference between profiles. Edit profiles, filter, and category setting across multiple profiles.
Details	View profile details and edit profiles.
Delete	Remove a profile from the Inventory pane.

Import profiles

Using the Import wizard, you can import an existing profile from a local file, from a device segment, or from another SMS. 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.

Filter	New	Replace	Combine (add)	Combine (change)
Attack Filter	Adds new	Delete and add all new	Adds from Snapshot. Does NOT overwrite user-modified filters.	Adds from Snapshot. Overwrites user-modified filters.
Traffic Management	Adds new	Delete and add all new	Adds all at top of list (default).	Adds all at top of list (default).
DDoS	Adds new	Delete and add all new	Adds all (unordered).	Adds all (unordered).
Traffic Threshold	Adds new	Delete and add all new	Adds all (unordered).	Adds all (unordered).
Category Settings	Adds all new	Delete and add all new	Adds individual category if non-DV default. Does NOT overwrite user-modified filters.	Adds individual category if non-DV default. Overwrites user-modified filters.
Profile Settings	Adds all new	Delete and add all new	Adds non-duplicated address pairs.	Adds non-duplicated address pairs.

Import a profile

Note: When you import a profile, you have the option of creating a new profile or merging the profile with an existing profile.

Note: When you import a profile that has shared settings, for example, services running on non-standard ports, all existing profiles will receive the additional ports.

1. Review information in *Import profiles* on page 124.
2. On the Profiles navigation pane, expand **Profiles**, and then click **Inspection Profiles**.
3. Below the Inventory pane, click **Import**. The Profile Import wizard opens.
4. On the Profile Import wizard, do one of the following:
   - To import from a local file, select the **Import from local file** option, and then enter the Profile name of the file to import or browse to its location and then click **Next**.

- To import from a device segment, select the **Import from Device Segment** option, select the segment from the drop down box, and then click **Next**.
- To import from another SMS, select the **Import from another SMS** option, provide the **SMS Server**, **Username**, **Password**, and then determine which **Profile to Import**.

5. On the Import Action wizard:
   - To create a new profile, click **Create a new profile**, and then enter a new profile name. You have the option of using an embedded name if the imported profile has one. See *Inheritance* on page 132 for information on using inheritance to create profiles.
   - To combine or replace an existing profile with the imported profile, select **Use an existing profile**, and then select **Combine** or **Replace**. Select an existing profile from the drop-down list.
6. Click **Next**.
7. Review the summary information, and then click **Finish** to upload the profile. To make changes to your selection, click **Previous** and follow the appropriate steps.

Export profiles

Using the Export wizard, you can export an existing profile to a local file, the SMS http server, an external SMB or NFS server or directly to one or more SMS servers.

Export a profile

1. On the Profiles navigation pane, expand **Profiles**, and then click **Inspection Profiles**.
2. Right-click on a profile on the Inventory pane, and then click **Export**.

   The Export Profile wizard opens.
3. Select one of the following options:
   - Export to Local File: Click **Next**, browse to the local destination, enter the package name, and then click **OK**.
   - Export to local SMS Exports and Archives: Click **Next**, and then enter the package name. The exported file can be viewed and accessed from the Exports and Archive section of the SMS Web interface. See *Exports and archives* on page 514.
   - Export to External Source: Select an option from the drop-down box, complete the required information, and then click **Next**. 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 **Next**, click **Add** andprovide the SMS address and credentials, and then click **OK**. Use the **Add** and **Remove** options to refine the list of SMS servers for export

4. 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:
    - Create a new profile: Enter the **Profile Name** and specify any inheritance information.
    - 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.
    - Click **Next**.
5. Review the summary information, and then click **Finish** to upload the profile. To make changes to your selection, click **Previous** and follow the appropriate steps.

Distribute inspection 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 279.

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.

Segment groups

You should create your profiles for specific segments prior to creating a segment group.

Required distributions

Filter modifications that require a distribution include the following items:

- Create, modify, or delete shared and custom filter exceptions.
- Create, modify, or delete filters.
- Modify Traffic Management filters or the order of the Traffic management filter.

DV and DV Toolkit version verification

When you distribute profile, the SMS verifies that all managed firewall and inspection 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 DV or DV Toolkit 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

When performing a distribution of the profile, you can select a high or low priority. The priority aids in the performance of the IPS. High priority updates will run before low priority updates. Low priority updates are regulated to ensure the best performance of the system. You can designate a distribution as High Priority by selecting the High Priority check box at the bottom of the Inspection Profile Distribution dialog.

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 SMS. Selecting low priority updates can take hours to perform a full update but there is less risk of loss in traffic packets.

Distributing profiles

You can distribute an IPS Profile to one or more segments or segment Groups. IPS profiles update the IPS filter settings for a device according to the profile being distributed. An IPS profile may include modified filter behavior, and/or shared settings including action sets, notification contacts, and services.

For ease of monitoring, IPS Profile Distribution dialog groups the distribution tasks by status. The groups include Pending, Succeeded, Failed or Canceled.

The SMS provides the following profile distribution options:

- *Manual profile distribution* on page 128
- *Creating new profiles* on page 130

You distribute profiles from the Profiles main screen or the Details screen for a selected profile.

Manual profile distribution

The SMS provides a straightforward method that allows you to manually distribute a profile to a device segment or group.

Distribute an inspection profile manually to inspection segments and firewall devices

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 fo the following items from the **Organize By** drop-down box:
        - **Segment Group**
        - **Device**

- Select the appropriate group(s).

4. To distribute the profile to Firewall Devices:
   - In the Targets section, select **Firewall Devices** tab.
   - Select the appropriate device(s).
5. For a high priority distribution, select the **High Priority** check box. See *High/low priority distributions* on page 128.
6. Click **OK**.

   See *Segment groups* on page 282 and *IPS distribution queue configuration (S-Series, N-Platform/NX-Platform)* on page 354

   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 an TippingPoint technical support representative to assist in extending the time-out setting for your profile distribution needs.

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 your 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.

Distribute multiple profiles

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. To distribute a profile to Firewall Devices:
   a. Select the **Firewall Devices** tab.
   b. Select the appropriate device(s).
5. For a high priority distribution, select the **High Priority** check box. See *High/low priority distributions* on page 128.
6. 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.
7. 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 282 and *IPS distribution queue configuration (S-Series, N-Platform/NX-Platform)* on page 354.

   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.

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.

Creating 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 (DVs) version 3.2 and above 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.

There are currently six available Deployment Modes:

Deployment mode	Description
Default	Provides a balance between high quality security and appliance performance and are suitable for most deployments.
Aggressive	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.
Core	Offers improved performance for IPS devices that are deployed on the interior of a network, with the expectation that perimeter-facing devices have blocked most malicious internet traffic.
Edge	Ideal for Web farms and DMZs that typically expose services to the Internet.
Hyper-Aggressive	Provides an ideal way to enforce an aggressive policy with filters designed to detect anomalies, application deviations, coding practices, and protocols. This deployment mode offers the best security posture.
Perimeter	Offers optimal security for IPS devices deployed on the perimeter of a network; protects the network from general Internet traffic.

For each profile, you can select a Deployment Mode to use, and by default the IPS 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 or categories.

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 Digital Vaccine versions that support this option. For more information, see the Digital Vaccine (DV) 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:

- Application and Infrastructure Restrictions/Exceptions
- Performance Protection Restrictions
- Reputation Exceptions
- Category settings
- Filters from the DV, Auxiliary DV and Custom Packages
- Advanced DDoS filters
- Traffic Thresholds filters
- Reputation filters
- Traffic Management filters

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. Review the information in *Creating new profiles* on page 130.
2. On the Profiles navigation pane, expand **Profiles,** and then click **Inspection Profiles**.
3. Below the Inventory pane, click **New**.

   The Create New Profile dialog opens.
4. Enter the following information for the profile:
   a. **Name** — Unique name for the profile.
   b. **Deployment Mode** — Option to choose a type of deployment. See *Deployment mode* on page 131.
   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 devices will detect this and provide the original Client IP address in the Inspection event.
   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. See *Inheritance* on page 132.
   f. **Description** — Brief description for the profile.

5. Click **OK**.

   The profile is added to Inventory pane and the navigation pane.

Use the 'Save As' option to copy a profile

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**.

Deleting a profile

Important: Deleting a profile will also delete all data relating to that profile, including all profile snapshots. However, events that have been generated by the profile will remain accessible.

1. On the navigation pane, expand **Profiles**, and then click **Inspection Profiles**.
2. Select on or more profiles on the Inventory pane, and then click **Delete**.

Compare profiles

The Profile Compare option allows you to select up to three profiles and compare various settings and filters. The Profile Compare screen is divided into tabbed functional areas that provide specific information about the specified category setting and associated filters. Each tabbed screen has associated tasks that can be performed.

Compare profiles

1. On the Profiles navigation pane, expand **Profiles**, and then click **Inspection Profiles**.
2. On the Inventory pane, 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.**

3. The Profile Compare screen displays with tabs for the following areas of comparison:
   - Category settings
   - Filters
   - Traffic Management filters
   - Advanced DDoS filters
   - Traffic Threshold filters
   - Reputation filters
   - Profile settings
4. (Optional) 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.
5. To make changes, select:
   a. Tabbed area.
   b. Entry you want to edit.
   c. **Edit** (at the bottom of the window)
   d. When changes are complete, click **Close**.

View profile details

For every Inspection profile you create, the SMS tracks information about the profile when the profile was distributed to devices. You can access this information by selecting a profile from the **Inspection Profiles > Inventory pane** and select **Details**. Alternatively, you can double-click a profile in the navigation pane to access the individual tabs.

Details view

For each inspection profile, the **Details** view provides the most current profile information including details about the Profile, Profile Distribution Schedule and Profile Distribution Details.

The **Profile Details** area includes the following items:

Column	Description
Name	Name of the profile.

Column	Description
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, such as perimeter, core, datacenter, etc.).
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.

This area also provides convenient access to the following profile functions:

- **Edit Details** — Change name, description and deployment mode of the selected profile.
- **Snapshot** — Backup current profile settings.
- **Export** — Export the selected profile to either a local file, the SMS http server, or an external SMB or NFS server.
- **Compare** — View the difference between profiles. Edit profiles, filter, and category setting across multiple profiles.
- **Distribute** — Distribute the selected profile or profiles to IPS devices in your network.

Profile distribution schedule

The Profile Distribution Schedule area displays information about scheduled distributions. From this area, you can create a **New Schedule** for the profile.

Distribution details

The Distribution Details area displays information on the distribution of the selected profile to IPS devices.

The Profile Distribution Details area includes the following items:

Column	Description
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 tab

For each profile, 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 IPS devices, and any comment that has been added.

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.

The All Versions area includes the following items:

Column	Description
Active	Displays a checkmark for the active version of the profile.
Version	Version of the profile.
Created	Date and time of the profile was created.
Distributed	Date and time of the last profile distribution.

Column	Description
Comment	Added information related to the profile.

This area also provides convenient access to the following profile functions:

- Details — View name and associated detailed version history for the selected profile.
- Activate — Make the selected version of the profile active.
- Distribute — Distribute the selected version of the profile.
- Delete — Delete the selected version of the profile.

View profile details and version options

1. On the Profiles navigation pane, expand **Profiles**, and then click **Inspection Profiles**.
2. Select a profile on the Inventory pane, and then click **Details** to:
   - Edit profile details
   - Take a snapshot
   - Export the profile
   - Compare profiles
   - Distribute the profile
   - Create a new profile distribution schedule
   - View profile distribution details

   See *Versions tab* on page 136.
3. Select the **Versions** tab to:
   - View version details for the selected profile.
   - Activate a version of the selected profile Distribute a version of the selected profile.
   - Delete a version of the selected profile.

Edit profile details

1. Review the information in *Creating new profiles* on page 130.
2. On the Profiles navigation pane, expand **Profiles,** and then click **Inspection Profiles**.
3. Select a profile on the Inventory pane, and then click **Details**.
4. In the Details pane, click **Edit Details**.

5. In the Edit Profile Details dialog, make any necessary changes:
   - Name— Name of the selected profile.
   - Deployment Mode — Deployment settings for filters related to specific types of deployments. For more information, see *Deployment mode* on page 131.
   - Capture Client IP (X-Forwarded-For & True-Client-IP) — Option to capture the originating IP address of a client using X-Forwarded-For (XFF) or True-Client technology.
   - HTTP — Option to convert a relative URI value to an absolute value.
   - Description — Description of the selected profile.
6. Make any changes, and then click **Save**.

Create a snapshot of a profile version

1. On the Profiles navigation pane, expand **Profiles,**and then click **Inspection Profiles**.
2. Select a profile on the Inventory pane, and then click **Details**.
3. In the Details pane, 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.
4. Click the **Versions** tab.

   The new entry displays in the All Versions table.

View profile version details

1. Review the information in *View profile details* on page 134.
2. On the Profiles navigation pane, expand **Profiles**, and then click **Inspection Profiles**.
3. Select a profile on the Inventory pane, and then click **Details**.
4. Click the **Versions** tab, and then select a profile version.
5. Click **Details**. The selected profile version displays the change list of modifications.

Activate a profile version

1. Review the information in *View profile details* on page 134.
2. On the Profiles navigation pane, expand **Profiles**, and then click **Inspection Profiles.**
3. Select a profile on the Inventory pane, and then click **Details**.
4. Click the **Versions** tab, and then select a profile version.
5. Click **Activate**. The selected profile activates as the current profile replacing all filter changes with changes from the snapshot.

Search options

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

The Search features enable you to search by extended criteria, across all filter categories, including options for user settings, severity, protocol, platform, modified or added filters, and taxonomy. Through the Search screen, you can select filter results to edit the filter, add an exception, or distribute the filter. Displayed results include the state, name, control, action set, category, and severity of the filter. See *Digital Vaccines* on page 182.

The Find feature performs a quick search on a displayed page for filters that match the keyword.

Type	Description	Access
Global Search	Searches all listed profiles for filters that match search criteria.	• Left navigational menu
Search	Searches within a selected profile for filters that match search criteria.	• Left navigational menu • **Search** button located on a filter screen
Find	Searches on the displayed page and highlights the next filter that contains the keywords.	• **Find** button located on a filter screen • **CTRL + F** on the keyboard

Global search

To perform a filter search across all listed profile, select the **Global Search** the option in the navigation pane of the selected profile. **Global Search** enables you to search by extended criteria, across all filter categories in all listed profiles.

Search

To perform a filter search within a selected profile, click the **Search** button on a filter screen or select the **Search** the option in the navigation pane of the selected profile. Search enables you to search by extended criteria, across all filter categories within a listed profile.

Find

To perform a quick keyword search, click the **Find** button at the bottom of the screen or press **CTRL + F** on the keyboard to bring up the **Find** screen. Then enter a keyword in the **Find in View** dialog box. The next filter that contains the keywords is highlighted. The **Find** option only searches on the displayed page.

Default inspection profile

The SMS is shipped with a default profile that can be used out of the box to start protecting your network. When you first enter the SMS application, the **Profiles** screen includes one initial profile. This profile is called **Default** and includes the default set of filters on the SMS. You can create copies, modify, and update this profile.

Profile overview

The **Profile Overview** screen provides a convenient location to view detailed information regarding modifications of a specific IPS profile. From this screen you can take a snapshot and distribute the IPS profile. You can sort through the information by clicking the table headings. This screen provides in-depth information regarding category settings, filters, restrictions and exceptions, and referenced shared settings, such as action sets, notification contacts, and services.

To view the information, browse between the tabbed screens:

- **Category settings** — Displays the state of the categories as enabled or disabled and the selected action setting per category. The default setting is Recommended for filters.
- **Filters** — Displays the filters you have modified in the profile and additional filters, such as Traffic Management filters. The information includes that state, name, action set, category, and specific information depending on the filter type.
- **Profile settings** — Displays the restrictions and exceptions for Attack and Performance Protection filters.
- **Shared settings** — Displays the action sets, notification contacts, and services used by profile.

Profile settings

Attack Protection filters scan for, detect, and block malicious attacks that try to locate vulnerable areas in your network security. These filters are enabled, from the start-up of your TippingPoint system, to automatically shield against triggering packets. You can change the action settings for all attack protection filters, default or user-activated, at the category level or for individual filters. These filters use Recommended settings from the Digital Vaccine by default.

Attack Protection filters detect traffic that meets one of the following criteria:

- Known to be malicious
- Considered suspicious

- Known to have security implications

You can modify all profiles, or filters, through Profile Settings. These settings include exceptions and restrictions for filters within a specific profile. When you create a profile setting, you add the setting to all Attack and/or Performance Protection filters in the profile. If you create filters or modify an existing filter with custom settings, the profile setting does not override the custom setting.

Note: Different exception and restriction options are available for different pillars of filters.

Profile Settings affect specific profiles. The option displays in every profile on the system through the navigation pane. When you create or modify these settings, unlike global action sets and notification contacts, these settings only affect a specific profile.

Note: When you distribute a profile, all profile settings are also distributed. To distribute profile settings, distribute a profile.

Security filter

When you enter a profile setting for IP address restrictions, you restrict all attack filters of a profile to apply only to the listed IP addresses. You can enter IP address restrictions and exceptions through the Security Filters screen. These settings do the following:

- Restrictions — Restrict all attack filters to function for the listed IP addresses.
- Exceptions — Exempt all attack filters to not function for the listed IP addresses.

Create or edit a security filter profile restriction

1. On the Profiles navigation pane, expand **Profiles**, expand **Inspection Profiles**, expand **Default**, and then click **Security Filters**.
2. Select the **Restrictions** tab to do one of the following:
   - Click **Add** to create a new restriction.
   - Select an IP address pair name, and then click **Edit** to modify an existing restriction.
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. On the Profiles navigation pane, expand **Profiles**, expand **Inspection Profiles**, expand **Default**, and then click **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** if you want to lock the settings.
7. Click **OK**.

Delete a security restriction or exception

1. On the Profiles navigation pane, expand **Profiles**, expand **Inspection Profiles**, expand **Default,** and then click **Security Filters**.
2. On the **Restrictions** or **Exceptions** tab, do one of the following:
   - Select a restriction in the **Restrictions** table.
   - Select an exception in the **Exceptions** table.
3. Click **Delete**.
4. Click **Yes** to confirm.

Application filters

Application Protection is a set of filter categories that defend against exploits that target applications and operating systems of workstations and servers on a network. These 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. Application Protection filters defend your network by providing a device with threat assessment, detection, and management instructions.

Through the Profiles screen, 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, changing how or when contacts are notified, or even disabling the filter.

These filters block traffic depending on the configured actions for a filter. You can set these actions to the entire category of filters or override specific filters to perform a different set of actions. See *Action sets* on page 106.

Application Protection Filters are a category of filters that protect your network from malicious attacks that seek to find and exploit vulnerabilities in your network. These filters are enabled by default on your TippingPoint system and shield against invasive attacks.

Application Protection filters include the following categories:

- Exploits — Category of filters that protect against known exploits of software components.
- Reconnaissance — Category of filters that detect and block reconnaissance scans of your network.
- Security policy — Category of filters that require deployment knowledge and/or operational policy.
- Vulnerabilities — Category of filters that protect against attackers looking for vulnerabilities in a network.
- IM, peer-to-peer, and streaming media— Category of filters that protect potentially vulnerable software of the network such as operating systems.

The **Profiles** > **Inspection Profiles** > **Default** > **Application Filters** screen displays the following filter information:

Column	Definition
State	Indicates whether the filter is currently enabled, disabled, or invalid.
Name	Name of the filter. Double-click the filter entry to view and configure filter details.
Control	Level at which the action set is defined for the attack filter.
Action Set	Action set that is performed when the filter is triggered. See *Action sets* on page 106.
Category	Filter category.

Column	Definition
AFC	Indicates whether Adaptive Filter Configuration (AFC) is enabled. See *Application filter categories* on page 144.
Locked	Indicates the lock status of the filter.
Exception	Indicates whether there is an exception set.
Severity	Indicates the potential consequences of traffic that matches the filter. See *Digital Vaccines* on page 182.

You can right-click on entries in the filter list and do the following:

- Copy — Copy selected rows or cell value.
- Export to file — Save selected rows or all rows as a TXT or CSV file.
- Find — Search for a filter using a keyword.
- Edit — Edit a selected filter.
- Copy filter settings — Copy action, AFC, exception, or all settings to the clipboard.
- Paste filter settings — Paste copied action, AFC, exception, or all settings from the clipboard.
- Add exception — Create a new exception.
- View related events — Display any events relating to the filter.
- Change lock — Change locked status.
- Change inherited settings — Change inherited settings option.
- ThreatLinQ — Obtain ThreatLinQ filter information.
- Table properties — View and change the order, visibility. sorting, and aggregation properties of table columns.

Note: If you receive errors or have issues editing and saving filters and exceptions due to exceeded limits, see *SMS error messages* on page 574.

Application filter categories

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.

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.

Reconnaissance

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.

Note: By default, Reconnaissance filters are either disabled or set to Block/Notify. To enable these filters or modify their category settings, see *View and edit application filter details* on page 148.

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.

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.

Note: 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.

The Scans/Sweeps Filters appear at the bottom of the Reconnaissance listings in the List pane. To view these filters, use the scroll bar to scroll to the bottom of the listings.

Security policy

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. The Threat Management Center (TMC) develops these filters.

Note: Security policy filter recommended settings are set to disabled by default. Configuring security policy filters requires knowledge of the installation network configuration. To enable these filters or modify their category settings, see *Create or edit a security filter profile restriction* on page 141.

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

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

You can enable, disable, or create exceptions to these filters according to the requirements for your environment.

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.

You can right-click on entries in the filter list and do the following:

- Edit — Edit a selected filter.
- New exception — Create a custom filter exception.
- View action set — View the action set properties for the selected filter.
- View related events — Display the related events for the filter in the Events screen.
- Find — Search for a filter using a keyword.
- Search — Search for a filter with advanced criteria options.

Vulnerabilities

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.

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.

As security threats are recognized, the Threat Management Center (TMC) creates and releases filter updates to protect potentially vulnerable systems.

Peer-to-peer

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.

Instant messaging

Instant messaging is a real-time, text-based communication between two or more people using computers that are connected over a network such as the Internet.

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.

Adaptive Filter Configuration (AFC)

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. The device continues inspecting traffic, but traffic inspection can slow down processing. To prevent such a scenario from causing the device to enter HA state, the SMS uses adaptive filtering to disable the filters that are the likely cause of traffic congestion.

Application filters allow you to enable or disable adaptive filtering. If you do not want a filter to be subject to adaptive filtering, you can disable the adaptive filtering option. You can also edit the Adaptive Filter Configuration (AFC) Settings for Device Configuration to modify the device-wide adaptive filter configuration. The AFC is under the AFC section of the Device Configuration. For more information, see *AFC settings* on page 309.

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 (e.g., **All Devices** > **[device]** > **Events**).

View and edit application filter details

1. On the Profiles navigation pane, expand **Profiles**, expand **Inspection Profiles**, expand **Default**, and then click **Application Filters**.
2. Select the type of filter by double clicking to expand the section.
3. (Optional) Double-click the filter you want to view, or click **Edit** to open the Edit Filter wizard.
4. (Optional) View the filter settings and make any changes as required.
5. (Optional) To see the filter details including detailed description of the filter, select **Filter Details** from the wizard navigation pane.
6. If you made changes to the filter, click **Distribute** to distribute the filter to managed devices or click **OK** to save the changes for distribution later.

Edit the state or action set for application filter category settings

1. On the Profiles navigation pane, expand **Profiles**, expand **Inspection Profiles**, expand **Default**, and then click **Application Filters**.
2. Click **Edit** for the category you want to edit.
3. In the Edit Category Settings dialog you can:
   - Change the **State** (enabled or disabled).
   - Choose the **Action Set** from the Action Sets created in the **Shared Settings** > **Action Sets** section.
4. Click **OK**.

Custom filter exceptions

You can create custom filter exceptions for application protection filters. When you create exceptions for a specific filter, the IP addresses you enter will not have the filter applied.

Note: These exceptions apply only to the updated filter. The exception does not globally affect all filters.

Most attack filters apply to traffic from any source IP address to any destination IP address. Exceptions allow you to permit traffic from a source or to a destination that you specify when that traffic matches an attack filter.

Exceptions are intended to eliminate *false attacks* from your network behavior. A false attack is traffic that matches an attack filter but is not considered a problem for your network. For example, if you are using custom or legacy software that uses standard protocols in non-standard ways, you might receive false attack notifications. To avoid being alerted to benign traffic that you know originates from a particular software package, you can add an exception that allows that type of traffic between specific source and destination addresses.

Caution: Be sure to scan your network hosts before disabling or creating exceptions to specific attack 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.

Create or edit application filter restrictions

1. On the Profiles navigation pane, expand **Profiles**, expand **Inspection Profiles**, expand **Default**, and then click **Application Filters**.
2. Select the **Restrictions** tab.
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**.

Delete application restrictions

1. On the Profiles navigation pane, expand **Profiles**, expand **Inspection Profiles**, expand **Default**, and then click **Application Filters**.
2. Select the **Restrictions** tab.
3. In the Restrictions section, select a restriction in the Restrictions table, and then click **Delete**.
4. Click **Yes** to confirm.

Create or edit application filter exceptions

1. On the Profiles navigation pane, expand **Profiles**, expand **Inspection Profiles**, expand **Default**, and then click **Application Filters**.
2. Select the type of filter by double clicking to expand the section:
   - Exploits
   - Reconnaissance
   - Security Policy
   - Vulnerabilities

- IM
- P2P
- Streaming Media

3. Click **Add Exceptions.**
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**.

Note: If you receive errors or have issues editing and saving filter exceptions due to exceeded limits, see *SMS error messages* on page 574.

User defined filters

User defined filters are a set of filter categories that protect network bandwidth and network infrastructure elements, such as routers from attacks. These filters use a combination of traffic normalization, DDoS protection, and application, protocol, and statistical anomaly detection. User Defined filters include the following categories:

- *Advanced DDoS filters* on page 151 — Detect and block a wide range of Denial of Service attacks, including SYN, Connection Per Second (CPS), and Established Connection floods. TippingPoint E-Series and IPS-N devices offer various levels of Advanced DDoS filter support. Default Advanced DDoS filters are not included. You must create and then distribute these filters.
- *Traffic Threshold filters* on page 158— Detect and manage traffic on a network. These filters support Block and/or Notify options for action sets and check for the following types of network inconsistencies:
  - Incorrect checksums
  - Invalid TCP header flags
  - Invalid IP fragments

- Invalid TCP reassembly
- Unsolicited requests

- *Reputation filters* on page 160— Detect and block traffic associated with suspect IP addresses and domain. These filters enable you to perform actions based on the selection of entries in the Reputation Database.
- *Geographic filters* on page 160— Detect and manage traffic based on a computer's IP address/ hostname within a geographic region or country. These filters enable you perform actions based the countries that you allow or deny in a filter.
- *Traffic Management filters* on page 169— Detect issues in bandwidth usage. These filters enable you to perform bandwidth-shaping. You create these filters; the SMS does not include default filters.

Advanced DDoS filters

Advanced Distributed Denial of Service (DDoS) filters enable you to create filters for detecting denial of service attacks. Different platforms offer various levels of Advanced DDoS filter support.

The following tables show the DDoS filter configuration settings the SMS supports for specific models and indicates whether the option is found in the Profiles (P) or Devices (D) area in the SMS client.

Note: When using Advanced DDoS Protection filters, you must place the inspection device in a Symmetric Network. You must disable Asymmetric Mode for your device. The device must see both sides of the traffic.

SYN proxy

Model	Enable	Threshold
10[1]	P	P
100E	P	P
110[1]	P	P
200E	P	P
210E	P	P
330[1]	P	P

Model	Enable	Threshold
600E[2]	D	P
1200E[2]	D	P
2400E[2]	D	P
5000E[2]	D	P
660N[3]	P	P
1400N[3]	P	P
2500N[3]	P	P
5100N[3]	P	P
6100N[3]	P	P
2600NX[3]	P	P
5200NX[3]	P	P
6200NX[3]	P	P
7100NX[3]	P	P
7500NX[3]	P	P

1) For models 10/110/330, support is dependent on platform. On the IPS 2.5.x platform, Advanced DDoS options SYN Proxy, CPS Flood, and Connection Flood are available through the Profiles area of the SMS. On platform NCP 3.2.2 and later, only SYN Proxy options are available, in the Profiles area of the SMS.

[2] For E-Series devices 600E/1200E/2400E/5000E, create Advanced DDoS filters and set the SYN Proxy Threshold in the Profiles area of the SMS. Enable SYN Proxy, and configure CPS Flood and Connection Flood options through the Devices area of the SMS.

[3] For N and NX platform devices 660N/1400N/2500N/5100N/6100N/2600NX/5200NX/6200NX/7100NX/7500NX, enable SYN Proxy and specify the Threshold in the Profiles area of the SMS. No other Advanced DDoS options on the SMS are available for these devices.

CPS flood

Model	Enable	Threshold
10[1]	P	P
100E	P	P
110[1]	P	P
200E	P	P
210E	P	P
330[1]	P	P
600E[2]	D	D
1200E[2]	D	D
2400E[2]	D	D
5000E[2]	D	D
660N[3]	N/A	N/A
1400N[3]	N/A	N/A

Model	Enable	Threshold
2500N[3]	N/A	N/A
5100N[3]	N/A	N/A
6100N[3]	N/A	N/A
2600NX[3]	N/A	N/A
5200NX[3]	N/A	N/A
6200NX[3]	N/A	N/A
7100NX[3]	N/A	N/A
7500NX[3]	N/A	N/A

[1)] For models 10/110/330, support is dependent on platform. On the IPS 2.5.x platform, Advanced DDoS options SYN Proxy, CPS Flood, and Connection Flood are available through the Profiles area of the SMS. On platform NCP 3.2.2 and later, only SYN Proxy options are available, in the Profiles area of the SMS.

[2)] For E-Series devices 600E/1200E/2400E/5000E, create Advanced DDoS filters and set the SYN Proxy Threshold in the Profiles area of the SMS. Enable SYN Proxy, and configure CPS Flood and Connection Flood options through the Devices area of the SMS.

[3)] For N and NX platform devices 660N/1400N/2500N/5100N/6100N/2600NX/5200NX/6200NX/7100NX/7500NX, enable SYN Proxy and specify the Threshold in the Profiles area of the SMS. No other Advanced DDoS options on the SMS are available for these devices.

Connection flood

Model	Enable	Threshold
10[1]	P	P
100E	P	P

Model	Enable	Threshold
110[1]	P	P
200E	P	P
210E	P	P
330[1]	P	P
600E[2]	D	D
1200E[2]	D	D
2400E[2]	D	D
5000E[2]	D	D
660N[3]	N/A	N/A
1400N[3]	N/A	N/A
2500N[3]	N/A	N/A
5100N[3]	N/A	N/A
6100N[3]	N/A	N/A
2600NX[3]	N/A	N/A
5200NX[3]	N/A	N/A
6200NX[3]	N/A	N/A

Model	Enable	Threshold
7100NX[3]	N/A	N/A
7500NX[3]	N/A	N/A

—

[1] For models 10/110/330, support is dependent on platform. On the IPS 2.5.x platform, Advanced DDoS options SYN Proxy, CPS Flood, and Connection Flood are available through the Profiles area of the SMS. On platform NCP 3.2.2 and later, only SYN Proxy options are available, in the Profiles area of the SMS.

[2] For E-Series devices 600E/1200E/2400E/5000E, create Advanced DDoS filters and set the SYN Proxy Threshold in the Profiles area of the SMS. Enable SYN Proxy, and configure CPS Flood and Connection Flood options through the Devices area of the SMS.

[3] For N and NX platform devices 660N/1400N/2500N/5100N/6100N/2600NX/5200NX/6200NX/7100NX/7500NX, enable SYN Proxy and specify the Threshold in the Profiles area of the SMS. No other Advanced DDoS options on the SMS are available for these devices.

Advanced DDoS configuration

SYN proxy — Protects 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.

When managed by the SMS, if you have configured Advanced Distributed Denial of Service (DDoS) filters to protect against SYN floods, the IPS supports DDoS protection of the SSL server, but not on the ports where we are performing inspection of SSL traffic. For example, if you have a server at 1.1.1.1, and that server responds to HTTP traffic on port 80 and HTTPS traffic on port 443, and you have configured SSL Inspection of the traffic on 1.1.1.1:443, and you have configured DDoS protection of 1.1.1.1 - then you will get DDoS protection on 1.1.1.1:80, but not on 1.1.1.1:443.

CPS flood — Protects against Connection-Per-Second floods. Each CPS protection limits the average number of connections that a client may open to a particular server per second. The protection includes a threshold setting of the calculated average number of connections per second to allow from a particular client.

The network administrator can create a CPS filter for both port A > B and port B > A traffic. The flexible settings allow customizations for in-coming and outgoing traffic and attack detection based on network traffic needs. Because the approach is based on an average connection-per-second rate, this implementation

allows for normal fluctuations of traffic (such as a Web browser that opens 10 connections at once while downloading a complex page, then sits idle while the user reads). As a result, the CPS protection scans and detects against the amount of new connections averaged over a period of time.

Connection flood — Protect against Established Connection floods. The Connection flood protection limits the number of simultaneous open connections that occur between a client and server.

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 DDoS filter analyzes and blocks possible SYN request floods to the network. These attacks do not harm data, but the flood can deny users access and connections to networks and services.

Create or edit an Advanced DDoS filter

Note: Before you can create a new Advanced DDoS filter, you must have an action set that has a block action and does not perform a packet trace.

1. On the Profiles navigation pane, expand **Profiles**, expand **Inspection Profiles**, expand **Default**, expand **User Defined Filters,** and then click **Advanced DDoS**.
2. Click **New**, or select a filter, and then click **Edit**.

   The Advanced DDoS Filter wizard opens and displays the **Filter Parameters** by default.
3. On the Create Advanced DDoS Filter Parameters screen, provide or edit the following information:
   - **Filter Info** — Edit or provide a name to identify this filter.
   - **Action** — Select the action set to perform if an attack against the specified host is detected.
   - **Network Settings** — Choose the direction to which the filter should be applied; specify the address of the destination to protect or click the arrow to select a named resource to protect.
   - **Exceptions** — Add exceptions to specify traffic that is exempt from inspection by this filter.

   Note: You can select the **Locked** check box near the top of the Filter Parameters screen to lock the filter and prevent unintentional changes. Note that if a filter has inherited settings and the base filter is locked, the filter with inherited settings CANNOT be edited.
4. Select the appropriate option from the left navigational menu:
   - 100E/110/200E/210E/330 Settings
   - 600E/1200E/2400E/5000E Settings
   - TOS 3.1+ Settings
5. Configure the available DDoS filter options. Note that the setting you select in the Advanced DDoS Filter wizard navigational menu determines the filter options displayed on the screen.

- **SYN Proxy** — In the **Notification Threshold** field, specify the number of SYN requests allowed per second (1 to 10,000).
- **CPS Flood** — In the **Threshold** field, specify the number of maximum average connections allowed per second (1.0 to 4096.9).
- **Connection Flood** — In the **Threshold** field, specify the number of open connections to allow (1 to 65,536).

Note: Refer to *Table* on page 151 to determine the **Advanced DDoS Filter** options available for each specific device.

6. Click **OK**.

   For information on configuring advanced DDoS filters for 600E devices and higher, see *Editing device configurations* on page 299.

   If you receive errors or have issues editing and saving filters due to exceeded limits, see *SMS error messages* on page 574. See *Edit Advanced DDoS filters* on page 375 for editing information.

   Note: The TippingPoint-5000E supports a total of 15 filters. You cannot create more than 15 filters of this type for this device.

Traffic Threshold filters

Traffic Threshold filters allow you to perform bandwidth-shaping or traffic monitoring. These filters enable the TippingPoint device to detect statistical changes in network traffic patterns. Using these filters, you can set your system to accept a set amount of traffic, profiling and shaping the bandwidth of your network.

Traffic Threshold filters alert you and the system when network traffic varies from the norm. The SMS determines normal traffic patterns based on the network statistics over time. You can set 4 types of thresholds for each filter:

- Minor increase — Traffic is slightly over the set threshold.
- Major increase — Traffic is greatly over the set threshold.
- Minor decrease — Traffic is slightly below the set threshold.
- Major decrease — Traffic is greatly under the set threshold.

Thresholds are expressed as a "% of normal" traffic. For example, a threshold of 120% would fire if traffic exceeded the "normal" amount by 20%. A threshold of 80% would fire if the level of traffic dropped by 20% from "normal" amount of traffic.

Thresholds trigger when traffic goes over or under the set amounts. When traffic exceeds a threshold and returns to normal levels, the system generates an alert. These alerts inform you of the triggered filter, when the thresholds are exceeded and return to normal, and the exceeded amount. These amounts include an amount exceeded above and below normal levels. If you set the action to Block, you can manage it from the Devices workspace under **device name** > **Events** > **Blocked Streams** tab.

At times, a Traffic Threshold filter can trigger multiple times. The filter could be triggering falsely due to threshold settings not matching the new traffic behavior of your system, or other such issues. A triggered Traffic Threshold filter will not perform functions until you manually reset it. Resetting a triggered filter is not the same as enabling or disabling a filter.

Note: If your device supports creating security zones, there are some restrictions regarding which types of segments will accept Traffic Threshold filters. These filters require physical ports and not virtual ports. These filters can only be distributed to segments that have a single port in the from-zone and a single port in the to-zone. Segments containing security zones with VLAN IDs cannot be used with Traffic Threshold filters and these filters cannot be distributed to the ANY-ANY-segment.

Traffic Threshold filter events can be found in the alert and block logs, based on the action set of the filter. You can use the Events screen to review which Traffic Threshold filters have triggered. Through Events, you can view, edit, and reset triggered Traffic Threshold filters. See *Create or edit a Traffic Threshold filter* on page 159.

Create or edit a Traffic Threshold filter

1. On the Profiles navigation pane, select **Profiles**, expand **Inspection Profiles**, expand **Default**, expand **User Defined Filters**, and then click **Traffic Thresholds**.
2. On the Traffic Threshold Filters screen, do one of the following:
   - To create a traffic threshold filter, click **New**.
   - To edit a traffic threshold filter, select the filter, and then click **Edit**.
3. To lock the filter, select the **Locked** check box.
4. In the Filter Info area, provide or modify the filter name.
5. In the Thresholds area, do one of the following:
   - To configure the system to generate a report without using traffic thresholds, choose **Monitor Only**.
   - To set thresholds and specify actions, choose **Monitor with Thresholds**, and specify thresholds and actions for **Above Normal** and **Below Normal** conditions.
   - Select **Enable** to enable a threshold, and provide a numeric value for the percentage of normal for that particular threshold. Thresholds are compared to normalized numbers based on time.
   - For each threshold that you enable, select the **Action** you want the system to perform when the specified threshold limit is reached.
6. In the Network Settings area, do the following:
   - Choose the direction of the flow for the segment ports: **A to B** or **B to A**.
   - Select the unit of measurement and duration on which to base thresholds. For example, you can use the drop-down lists to base thresholds on **connections/sec** over the last **minute**.
   - Choose **Protocol** or **Application**.

- If you choose **Protocol**, use the drop-down list to select the specific protocol.
- If you choose **Application**, use the drop-down list to select the protocol, and provide a **Port** number. Choose whether to apply Network Settings to **Requests Only**, **Replies Only**, or **Both Requests and Replies**.

7. To re-distribute the modified filter, click **Distribute**.
8. Click **OK** to save your changes and close the Traffic Threshold Filters screen.

   If you receive errors or have issues editing and saving filters due to exceeded limits, see *SMS error messages* on page 574.

Reputation filters

A Reputation filter associates an action set with one or more of entries in the Reputation Database. Possible actions include: block, permit, notify, and trace. 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 203.

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.

Geographic filters

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 521.

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 countries. Once you select a country, the SMS removes *Any* country from the Geographic filter; however, if you exclude all countries in the selected filter, the SMS includes *Any* country again.

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.

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. The table includes the following information about each filter:

The Filters screen displays the following Reputation and Geographic filter information:

Column	Definition
Expand/Collapse	Pertains to a Reputation or Geographic filter. By default, all filters are initially expanded.

Column	Definition
	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.
Order	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.
Name	Displays the name of the Reputation or Geographic filter. You can double-click a filter entry to edit it.
State	Displays whether a filter is active. A check mark indicates that the filter is activate and can be distributed to a device.
Locked	Indicates the lock status of a filter. A check mark indicates that the filter is locked and cannot be edited.
Action	Associated action set that is performed when the filter is triggered. See *Action sets* on page 106. The SMS displays an icon to indicate the type of action for the selected filter.
IPv4/IPv6	Indicates the version of the Internet protocol.
DNS	Indicates whether the filter has a Domain Name System.
Untagged/Tagged	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.

Column	Definition
Criteria	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.

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 filer 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.

Right-click options

Right-click on any filter in the Reputation Filters table to do the following:

- **Copy** —You have the option to copy just the cell contents or the entire row. When copied, the actual value of the cell is pasted (true/false) along with the column headings.
- **Export to File** — You can choose to export a single row or all of the rows to either a plain text file or a comma delimited file. Options are available for including headings or not including headings in the export.
- **Find** — Search for a Reputation setting.
- **Edit** — Edit the selected Reputation or Geographic filter.
- **Delete** — Delete the selected Reputation or Geographic filter.

- **New Reputation** — Create a new Reputation filter.
- **New Geographic** — Create a new Geographic filter.
- **View Related Events** — Quickly jump to the Reputation Events for the selected filter. See *Inspection events* on page 42.
- **Table Properties** — Define the order, visibility, sorting and aggregation properties of each column in your table.

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.

Edit Reputation settings

1. On the Profiles navigation pane, expand **Profiles**, expand **Inspection Profiles**, expand **Default**, expand **User Defined Filters**, and then click **Reputation/Geo**.

   The Reputation Filters and Settings workspace appears.

2. On the Reputation Settings pane, click **Edit Settings**.

   The Edit Reputation Settings dialog opens.

3. (Optional) Select the **Locked** check box if you want to prevent the ability to edit the Reputation settings.
4. On the Filter Matching Address pane, select an option to specify addresses to use for filter comparisons:
   - Both source and destination addresses
   - Source address only
   - Destination address only
5. On the Lookup Packet Handling pane, select an option to specify how incoming packets are handled during a lookup:
   - Permit packets
   - Block packets
6. Click **OK**.

Create a Reputation filter

1. On the Profiles navigation pane, expand **Profiles**, expand **Inspection Profiles**, expand **Default**, expand **User Defined Filters**, and then click **Reputation/Geo**.

   The Reputation Filters and Settings workspace appears.

2. Under the Reputation Filters table, click **New Reputation**.

   The Create Reputation Filter wizard opens.

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, or DNS Domains) 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.
7. Click **OK**.

   The Reputation filter is added to the Reputation Filters table.

Edit a Reputation filter

1. On the Profiles navigation pane, expand **Profiles**, expand **Inspection Profiles**, expand **Default**, expand **User Defined Filters**, and then click **Reputation/Geo**.

   The Reputation Filters and Settings workspace appears.

2. Select a Reputation filter from table, and then click **Edit**. Alternatively, double-click a filter in table to open it.

   The Edit Reputation Filter wizard opens.

3. Update any fields as required.
4. Click **OK**.

Create a Geographic filter

1. On the Profiles navigation pane, expand **Profiles**, expand **Inspection Profiles**, expand **Default**, expand **User Defined Filters**, and then click **Reputation/Geo**.

   The Reputation Filters and Settings workspace appears.

2. Under the Reputation Filters table, click **New Geographic**.

   The Create Geographic Filter dialog opens.

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 County list, and then select **AddCountry**.

   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 county 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**, expand **User Defined Filters**, 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**.

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**, expand **User Defined Filters**, 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.

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**, expand **User Defined Filters**, 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.

Create or edit Reputation filter exceptions

1. Go to **Profiles** > **Inspection Profiles** > **Default** > **User Defined Filters** > **Reputation/Geo**
2. Click the **Exceptions** tab.
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. (Optional) Select **Locked** if you want to lock the settings.
6. Type a name for the exception in the **Name** field.
7. 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.
8. 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.
9. Click **OK**.

   Note: If you receive errors or have issues editing and saving filter exceptions due to exceeded limits, see .

Create or edit domain name exceptions

1. Go to **Profiles** > **Inspection Profiles** > **Default** > **User Defined Filters** > **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**.

Traffic Management filters

Traffic Management 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 Management 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. We do not recommend using a Permit action, as this action could introduce invulnerabilities 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.

Note: 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.

Edit a Traffic Management filter

1. On the Profiles navigation pane, expand **Profiles**, expand **Inspection Profiles**, expand **Default**, expand **User Defined Filters**, and then click **Traffic Management**.
2. Select a filter, and then click **Edit**.

3. To lock the filter, select the **Locked** check box.
4. Enter a name for the filter in the **Name** field.
5. In the Action area, choose one of the following options:
   - Select **Enabled** to enable filter specific settings, or clear the check box to disable the custom settings.
   - Select an action:
     - Block
     - Allow (Incoming traffic will be inspected using profile settings)
     - Trust (Incoming traffic will be trusted and not inspected)
     - Rate Limit

   Note: If you choose the Recommended action set, the filter is set to predefined recommended setting for the specific filter. If you choose a Permit action for a traffic management filter, packets matching the rule are logged and passed without further inspection. This process differs from normal packet processing and can introduce vulnerabilities. If you select a non-blocking action set or create an exception to a management filter, you receive a notification from the system.
6. In the General Settings area, enter any necessary comments.
7. Configure the network settings:
   - Direction
   - Protocol
   - ICMP settings
   - Source and destination addresses and ports
8. To re-distribute the modified filter, click **Distribute**.
9. Click **OK** to save your changes and close the Edit Filter wizard.

   If you receive errors or have issues editing and saving filters due to exceeded limits, see *SMS error messages* on page 574.

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.

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.

Common Profile Management tasks include:

Task	Description
Import	Imports the policy from a device and saves it as a new profile.
New	Creates a new profile.
Distribute	Distributes a profile or profiles to IPS devices in your network.
Delete	Removes a profile.

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 132.
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 132.
6. Click **OK**.
7. Configure Captive Portal, Firewall, and NAT rules as necessary:

- See *Firewall rules* on page 173 for setting basic firewall rules.
- See *Captive portal rules* on page 177 for information on setting captive portal rules.
- See *NAT rules* on page 178 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 174.

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 174.
   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 174.
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 174.

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 174.
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 174.

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 a firewall profile as well as any associated inspection profiles to one or more 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 *High/low priority distributions* on page 128.
5. Click **OK**.

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.

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.

Digital Vaccines

The Threat Management Center (TMC) constantly researches and distributes filter and software updates to protect systems against new malicious threats to networks. One way that the TMC provides continued support and protection to your TippingPoint system is through Digital Vaccine (DV) packages. These packages include filter updates you can distribute to appliances and customize in profiles.

You can download and distribute DV updates manually or automatically from the **Profiles** > **Digital Vaccines** screen. The screen allows you to download packages and distribute them to appliances according to your own schedules. You can also configure the system to automatically check for, download, and distribute filter updates to the devices managed by the SMS.

Note: If you do not want to activate a Digital Vaccine when downloading it, clear that option when prompted to download a new DV.

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.

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

The DV Inventory area displays the following details:

Column	Description
Version	Version of the Digital Vaccine package.
Active	Active status of the Digital Vaccine package. You can download many packages that can be activated based on your system needs.
vTPS DV	A check mark indicates that the Digital Vaccine package is only available for virtual TPS (vTPS) devices.
Released	Date and time the Digital Vaccine package was released.
Downloaded	Date and time the Digital Vaccine package was downloaded from the TMC.
Size	File size of the Digital Vaccine package.
Devices	Number of devices that have received the distributed Digital Vaccine package. If the number is zero (0), the package has not been distributed.

The Distribution Progress area displays the following details:

Column	Description
Device	Version of the Digital Vaccine package.

Column	Description
Package	Version of the Digital Vaccine package.
Start Time	Date and time the DV distribution started.
End Time	Date and time the DV distribution ended.
Status	Status of the completed distribution.
Extended Status	Availability of extended status. A check mark indicates that additional information is available that is relevant to the distribution. Double-click on the entry to view distribution details including any Extended Status information.
Progress	Indication of the current progress of a DV during the distribution process.

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.

A Digital Vaccine that begins with	Applies to
2.5	Devices running TOS v2.5.2 to TOS v3.1x.
3.2	Devices running TOS v3.2.0 or later, such as IPS and TPS devices.
4.0	vTPS devices only.

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. For distribution information, see *Distributing profiles* on page 128.

   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/*.

   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 186.

   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 189
- *Stop distribution of a DV, virtual DV, or Auxiliary DV* on page 190

- *Create a new scheduled distribution* on page 190
- *Edit a scheduled distribution* on page 190

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 186
- *Import a DV, virtual DV, or Auxiliary DV package* on page 187
- *Download a DV, virtual DV, or Auxiliary DV package* on page 187

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.
4. On the Download File page, click **Download**.

   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 **AutoAuxiliary 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.

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**.

Activate 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, 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.

Search filters in a DV package

Note: 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 options* on page 139.

1. On the Profiles navigation pane, expand Inspection Profiles in the navigation tree and select **Global Search**.
2. In the Search Criteria screen, expand the Source Criteria section to reveal the Package Source options and select the type of package from one of the following options.
   - Digital Vaccine
   - DV Toolkit
   - User (Threshold, Adv DDos, Reputation)
   - Auxiliary DV (select the type: ANY or MalwareAux)
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.

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.

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.
3. On the Distribution Progress section, click **Stop Distribution**.

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 DV

An Auxiliary Digital Vaccine (DV) is a specialized filter package 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. In version 4.1, SMS supports a new type of Auxiliary DV, ThreatDV, that is supported on devices running TOS 3.7 or later.

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 new 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 186.
- 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.

Column	Description
Category	User-created label
Version	The version of the Auxiliary DV
Active Status	The active status of the Auxiliary DV. You can import multiple Auxiliary DVs that can be activated based on your system needs.
Released	Date and time the Auxiliary DV was released by TippingPoint
Downloaded	Date and time the Auxiliary DV was downloaded from the TMC
Size	File size of the Auxiliary DV
Description	Brief description of the Auxiliary DV
Devices	Number of devices that have received the distributed Auxiliary DV. If the number is zero (0), the ADV has not been distributed.

Column	Description
Device	Number of devices receiving the distributed Auxiliary DV. Expand to see the name of each target device.
Package	Version of the Auxiliary Digital Vaccine package being distributed
Start Time	Date and time the distribution began
End Time	Date and time the distribution ended

Column	Description
Status	Status of the distribution
Progress	Progress of the distribution expressed in a percentage value

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 inspection profiles* on page 127.

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 186.

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

Digital Vaccine Toolkit (formerly known as Custom Shield Writer) 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 distributed.

Go to **Profiles** > **DV Toolkit Packages** to access the DV Toolkit Packages screen.

Note: The latest version of the Digital Vaccine Toolkit application may not function the same way as previous versions of this tool. For the most recent documentation updates, check the Threat Management Center (TMC) website at *https://tmc.tippingpoint.com/TMC/*.

Associate DV Toolkit packages with devices and profiles in the SMS

Associating the filters in DV Toolkit packages with devices and profiles in the SMS involves these steps.

1. *Create a DV Toolkit package* on page 195.
2. *Import a DV Toolkit package* on page 197.
3. *Activate a DV Toolkit package* on page 198.
4. *Create an inspection profile* on page 132 (or edit an existing profile). Using this profile, you can *review filters from the active DV Toolkit packages and enable filter settings* on page 198.

5. *Distribute a DV Toolkit package to the device* on page 200.
6. *Distribute a profile to the device* on page 127.

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/*.

Use multitenancy to limit access to DV Toolkit packages

You can use role-based access control for DV Toolkit packages. With multitenant DV Toolkit packages, multiple users can have separate, active DV Toolkit packages running on the same SMS.

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.

To limit access to DV Toolkit packages, go to **Admin** > **Authentication and Authorization** and then:

- Create (or edit) a role and set capabilities for DV Toolkit Management (**Create Role** > **Capabilites** > **Profiles** > **DV Toolkit management**). See *Managing user roles* on page 443
- 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 445
- 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.

Column	Description
Package	Name of the DV Toolkit package.

Column	Description
Version	Version of the DV Toolkit package.
Active	Active status of the DV Toolkit package (indicated by a check mark). You can have multiple, active DV Toolkit packages on the SMS.
Imported Date	Date and time the DV Toolkit package imported.
File Size	File size of the DV Toolkit package.
Devices	Number of devices that have received the distributed DV Toolkit package. If the number is zero (0), the package has not been distributed.

Distribution Progress

Perform the following distribution tasks from the Distribution Progress pane on the DV Toolkit Packages screen:

- **Details** — Displays the status details for a selected device distribution entry in the table.
- **Stop Distribution** — Stops a device distribution.
- **Clear Obsolete** — Clears entries from the table except for the last distribution for each managed device.

Column	Description
Device	The name of the device to receive the distributed DV Toolkit package. You can collapse and expand the details in the distribution by clicking the "-" or "+".
Package	Displays the status of the DV Toolkit package distribution to the device. ("Merged DVT package" displays when you distribute the package to the device. "Uninstall DVT package" displays when you install a package from the device).
Start Time	The date and time when the DV Toolkit package distribution process began for the device.

Column	Description
End Time	The date and time when the DV Toolkit package distribution process ended for the device.
Status	The status of the DV Toolkit package distribution.
Ext. Status	The extended status of the DV Toolkit package distribution (indicated by a check mark).
Progress	Current progress of the DV Toolkit package distribution by percentage complete.

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, go to **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. Click **Profiles** > **DV Toolkit Packages**.
2. Click **Import**.
3. Click **Browse** to browse to and select a DV Toolkit package file.
4. (Optional) 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 197
- From the DV Toolkit Inventory table
- From the DV Toolkit Details screen

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:
   - Click **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**.

   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.

Search for DV Toolkit packages from an Inspection Profile

When searching for DV Toolkit packages, 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.
- The SMS assigns each filter a new filter ID based on the ID assigned by the Digital Vaccine Toolkit application. Each filter starts with a C and is followed by numbers.

- 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 *Use multitenancy to limit access to DV Toolkit packages* on page 195.

1. Go to **Profiles** > **Inspection Profiles** and select an existing Inspection Profile. Alternatively, you can create a new profile. See *Create a new profile*.
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 options*.
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 and trigger an action in the Inspection Profile, do any of the following:

Select a filter	Edit filter settings - Actions
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

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.

Note: After you distribute the DV Toolkit package to the device, the Local Security Manager (LSM) of the device will display the name of the merged package, which is generated by the SMS. This name is different from the individual DV Toolkit package names that display in the SMS.

1. Do any of the following:
   - Click **Profiles** > **DV Toolkit Packages** and select an active package from the DV Toolkit Inventory table.
   - Click **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. See *High/low priority distributions* on page 128.
4. Click **OK**.

   The package distributes to the selected device. As it runs, an entry displays with updating status in the Distribution Progress table (on the DV Toolkit Packages screen) and the Device DV Toolkit Inventory table (on the DV Toolkit Details screen).

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:

- Click **Profiles** > **DV Toolkit Packages**, select a package from the DV Toolkit Inventory table, and then click **Details**.
- Click **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*.
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*.
4. *Delete a DV Toolkit package from the SMS*.

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 t 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 202.
- 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:
   - Click **Profiles** > **DV Toolkit Packages** and select an active package from the DV Toolkit Inventory table.
   - Click **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 201
  - 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. Click **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. See *High/low priority distributions* on page 128.
5. Click **OK**.

The package distributes to the selected device. As it runs, an entry displays with updating status in the Distribution Progress table (on the DV Toolkit Packages screen) and the Device DV Toolkit Inventory table (on the DV Toolkit Details screen).

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 201
- 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. Click **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 and DNS names on an SMS that represent potential risks to network security. Entries may be user provided, ThreatDV provided, or both.

Entries in the Reputation Database can be tagged or untagged. A tagged entry consists of an IP or DNS address 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 or DNS address and function as a Black List.

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 160.

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 for domain name and may have one or more associated tag categories

with specified values. A Reputation Database entry must contain an IP Address or domain name, 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:

Column	Description
Device	Number and name of one or more target devices.
Package	Type of synchronization, such as Full or Delta.
Distributed	Date and time of last successful synchronization.
Status	Status of the synchronization, such as Complete (Success).
Progress	Current progress of the synchronization.

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:

Column	Description
Type	Type of task.
Status	Status of task, such as Complete or In Progress.
Time Queued	Date and time when the task was placed in the queue.
Time Started/ Completed	Date and time when the task started/completed.

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 Profilesnavigation pane, click **Reputation Database.**
2. On the **Edit** menu, click **Full Sync**.

Stop a synchronization of the Reputation database

1. On the Profilesnavigation 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 or by ThreatDV. Tag categories created by the reputation service are read-only and may not be modified. 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.

This area provides the following information about Reputation Database tag categories:

Column	Description
Name	A unique name for the tag category.
Type	Type of data that the tag category contains: • Text — Arbitrary text strings • List — List of items • Date — Dates and times • Yes/No — Yes or no value • Numeric Range — Range of whole numbers
User Defined	An indication if a tag category was created by the user and not a subscription service.
Description	A brief description (up to 255 characters) indicating how the tag category is to be used.

Descriptive name	Type	Settings	Notes
Comment	Text	Up to 255 characters.	
Country	List	A list of values, such as: • China • France • Mexico	Defined values should be a subset of the descriptive name.
Last Seen	Date	Date and time input format, such as: MMM d, yyyy	For Input Format options, see help embedded in the Create/Edit Tag Category dialog.
Approved	Yes/No	Pre-defined values of: • Yes • No	Similar to the List category, this category has two pre-defined values, Yes or No.
Score	Numeric Range	Minimum and Maximum value, such as: 1 - 100	The description of this might indicate that the defined value represents a percentage of confidence.

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 Generalarea, 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 are 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 460.

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

ThreatDV is a subscription-based service that identifies and delivers suspect IP and DNS 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 Reputation DV screen provides a summary of the Reputation DV Status and Reputation DV entries in the Reputation Database.

Reputation DV status

- 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.

Reputation DV entries

- IPv4 — Number of entries with IPv4 addresses.
- IPv6 — Number of entries with IPv6 addresses.
- DNS — Number of entries with domain names.
- Total — Total of entries.

View license details for a ThreatDV reputation filter

1. On the Profiles navigation pane, expand **Reputation Database**, and then click **Reputation DV**.
2. On the Reputation DV Status area, click **View License Details**.

   The License Status Details dialog lists general license information for the SMS and managed devices.
3. To view a detailed list of licensed capabilities for a specific device, select the device from the table and click **Details**.

   The Licensed Capabilities dialog lists the license information for the device.
4. To view details for a specific licensed capability, select the capability from the table and click **Details**.

   The Licensed Capability Details dialog displays information for the license. To view information about another license listed in the Licensed Capabilities dialog, click the left or right arrows in the License Capability Details dialog.
5. Click **Close** to return to the previous dialog.
6. Repeat previous step until all license-related dialogs close and you return to the main Reputation DV screen.

Enable or disable automatic DV download for a Reputation DV

1. On the Profiles navigation pane, expand **Reputation Database**, and then click **Reputation DV**.

2. On the Reputation DV Status area:
   - Click **Enable** to receive automatic ThreatDV updates to your reputation filters when a new DV becomes available.
   - Click **Disable** if you do not want to receive automatic updates.

Import a ThreatDV package

Note: ThreatDV is a subscription-based service.

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** > **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 Reputation DV

Important: Reset DV deletes ALL Reputation DV entries in the Reputation Database and CANNOT be undone. Reputation DV tag categories are NOT deleted.

1. On the Profiles navigation pane, expand **Reputation Database**, and then click **Reputation DV**.
2. Click **Reset DV**.
3. Verify that you want to delete ALL Reputation DV entries in the Reputation Database, and then click **OK**.

User-provided entries

The SMS supports user-provided entries to the Reputation Database. Reputation entries represent IP addresses or DNS domains that are known to be malicious. Address entries in the Reputation Database can be tagged or untagged. Untagged entries contain only an address and function as a Black List.

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 160.

Import entries into the Reputation database

You can create a file that contains the information you want to add to the Reputation Database. 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. See *Reputation import rules* on page 593.

Import user-provided entries to the Reputation database from a file

1. Before you create your CSV import file, refer to *Reputation import rules* on page 593.
2. On the Profiles navigation pane, expand **Reputation Database**, and then click **User Provided 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**, or **DNS names**, 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 entries in the Reputation database. When you add entries, you have the option to add addresses only or add addresses with tag categories and values. Addresses with tags provide more options for tracking and blocking suspicious traffic. See *Reputation filters* on page 160.

Add a user-provided entry (addresses only) to the Reputation Database

1. On the Profiles navigation pane, expand **Reputation Database**, and then click **User Provided 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
4. Click **OK**.

Add an address, tag category, or tag value to the Reputation database

1. On the Profiles navigation pane, expand **Reputation Database**, and then click **User Provided 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
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 comma-separated value (CSV) file. 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 Provided 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
5. Click **Finish**.

Reputation database search

The Search 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.

Criteria	Description
IP Address	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.
DNS Domain	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.

Criteria	Description
Include Untagged Entries	Includes addresses that do not have tags associated with them.
Include Tagged Entries	Includes addresses that have tags associated with them.
Include Rep DV Entries	Includes Reputation Digital Vaccine entries, an optional subscription-based service. These entries are displayed in a separate column on the search results table.
Include User Entries	Includes User-Provided entries. These entries are displayed in a separate column on the search results table.
Include Geographic	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.

See *Tag Categories tab* on page 206.

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 213.
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 address 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
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 203.
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 214.
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 214.
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 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 214.
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 214.
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**.

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 *High/low priority distributions* on page 128 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

Vulnerability Assessment Policy Tuning is a new function of the SMS, located in **Profiles** > **Vulnerability Scans**. The Vulnerability Scans screen provides a centralized location for managing vulnerability scan files.

This section includes the following topics:

- *Overview* on page 218
- *Vulnerability scans* on page 218

- *CVE Search* on page 222
- *Vulnerability Criteria* on page 224

Overview

The Vulnerability Assessment Policy Tuning integration gives the SMS administrator the ability to fine tune their policy against vulnerabilities found by their scanner. The SMS will correlate these vulnerabilities with the DV filters using the CVE ID and help guide the SMS administrator as they tune their policy.

To view **Vulnerability Scans**, click **Profiles** on the SMS toolbar. From the left navigation pane, you can see **Vulnerability Scans** near the bottom. Nested under **Vulnerability Scans** is **CVE Search**.

Vulnerability scans

The **Profiles** > **Vulnerability Scans** page displays the following information:

Column	Description
File Name	The vulnerability scan file that has been imported to the SMS
Vendor	The company associated with the file
Import Time	The time and date that the file was imported
Scan Start Time	The time and date that the scan began
Scan End Time	The time and date that the scan ended
Version	The version number of the scanner file format
Entries	The number of records reported by the scanner
Comments	A place for the administrator to write notes or leave reminders

This area supports the following tasks:

- **Import** - Imports a vulnerability scan file.
- **Show CVEs** - Shows the CVEs for that particular vulnerability scan file.
- **Profile Tuning** - A wizard that allows the user to compare the data from the vulnerability scans to their current policy in order to make adjustments to the filters by changing their action sets as needed.
- **Comments** - A place for the administrator to write notes or leave reminders for a particular vulnerability scan file.
- **Delete** - Deletes one or more selected vulnerability scan files.

CSV file capacity requirements

When importing a CSV file, note the following capacity restrictions:

- Each row in a CSV file must be less than 10240 bytes.
- The maximum number of host IP address and vulnerability combinations that you can import into the SMS is 10 million. When the SMS reaches the maximum limit, it will display an error message. You must delete one or more vulnerability scans before you can import a new scan.

To import a CSV file

Note: Imported CSV files use the native converter. The native converter option requires file records to be in the SMS Native Format.

Custom converters are available for Qualys and Nexpose. If you require a converter for another vendor, you should consult your TippingPoint sales engineer.

1. Navigate to **Profiles** > **Vulnerability Scans**.
2. Click **Import**.
3. Click **Browse**, and select the vulnerability scan file that you want to import.
4. Make sure that **Native** next to **Converter** is selected, and then click OK.

   A prompt appears to indicate if the import was completed and with how many errors.

To import a file using a custom converter

Custom converters are available for Qualys and Nexpose. If you require a converter for another vendor, you should consult your TippingPoint sales engineer.

The custom converter for importing a file allows you to load a vulnerability scan file that is not compatible with the SMS. Custom converters change proprietary vulnerability scanner formats to the native format used by the SMS.

1. Navigate to **Profiles** > **Vulnerability Scans**.
2. Click **Import**.

3. Click **Browse**, and select the vulnerability scan file that you want to import.
4. Select the option **Custom** under **Converter**.
5. Next to **Custom**, select the necessary converter from the drop-down list.

   The **Converter Properties** will display basic information about the selected custom converter.

6. Click **OK**.

   A prompt will appear with information about the vulnerability scan import. This prompt will inform you of any errors that might have occurred during the import, and also gives you the option to download the conversion information file or download the conversion error file.

Show CVEs

Highlight a vulnerability scan file, and click **Show CVEs** to view the CVE information for that file.

Profile Tuning

Click **Profile Tuning** to open the Profile Tuning Wizard.

Functions of the Profile Tuning Wizard

The primary function of this wizard is to allow the user to compare the data from the imported vulnerability scans to a selected profile's settings. This will allow the user to make adjustments to the filters by changing their action sets as needed.

To begin this wizard, select a file, and then click on **Profile Tuning**. This button is located in both **Profiles** > **Vulnerability Scans** and **Profiles** > **Vulnerability Scans** > **CVE Search**.

Note: In **Vulnerability Scans**, only one file at a time can be selected to run the Profile Tuning Wizard. In **CVE Search**, more than one file can be selected at once to run the wizard.

The following is a walk-through of the Profile Tuning Wizard.

Dialog Page 1

This page displays the available profiles to compare with the CVEs. Select the profile you want to tune.

Dialog Page 2

This page shows the filters identified in the CVEs that are currently permitting traffic.

This page displays the following information:

Column	Description
Name	The name of the filter

Column	Description
Action Set	The action set that is currently selected for that filter
Category	The filter category
Source	The CVEs associated with that filter
Severity	The severity of that filter
Pending Action Set	The action set to be applied to that filter

The name of the filter is listed, and next to the name is the action set that is currently being used for that filter. The wizard recommends that these filters be changed from their current action set to the **Block + Notify** action set.

To change all of the filter action sets to **Block + Notify**, select the files you wish to change, and then click **Apply to Selected**. The action sets for each filter can also be manually changed by choosing a pending action set from each drop down menu.

Note: To see the filters with an **Ignored** action set, select the check box near the bottom of the window. The action set for these can be changed to **Show (Unignore)** from the drop down list.

Dialog Page 3

This page shows the vulnerabilities that do not have an associated filter in the Digital Vaccine. There is no required action for this page.

Dialog Page 4

This is the confirmation and summary page of the Functions Vulnerability Wizard.

This page lists all of the pending action set changes that have been made on the previous pages. These changes can be reviewed, and comments can be left for the changes made at the bottom at the page.

Note: If a comment is added, it will erase any existing comments for the filters that are changed.

When you click **Finish**, the changes are saved. However, the changes are not actually distributed to the system unless the **Launch distribution wizard when finished** check box is selected.

Comments

To place a comment on a particular vulnerability scan file, select the file, and then click **Comments**.

Delete

To delete a vulnerability scan file, select the file, and then click **Delete**.

CVE Search

The **Profiles** > **Vulnerability Scans** > **CVE Search** contains several panes and tables of information.

Scan Criteria pane

The Scan Criteria pane displays search criteria options for the CVE vulnerability scan files.

- **Scans**- Lists the vulnerability scans that have been imported. To view the CVEs for a vulnerability scan, select a file. More than one file can be selected at once.
- **Scan Vendor**- Search the CVEs by vendor.
- **Scan Time**- Search the CVEs based on the time they were scanned.
- **Import Time**- Search the CVEs based on the time they were imported.

Note: By clicking **Reset**, the search criteria in this pane will be cleared.

CVE Criteria pane

The CVE Criteria pane displays search criteria for individual CVEs.

- **CVE Details**- Search the CVEs based on the CVE ID.
- **Assets**- Search the CVEs based on the asset number (IP address).
- **Discovered Time**- Search the CVEs based on the time they were discovered.
- **Flagged Status**- Select the **Flagged** check box to view the flagged profiles, and select the **Not Flagged** check box to view the profiles that are not flagged.

Note: By clicking **Reset**, the search criteria in this pane will be cleared.

CVE Search Results

After the search criteria has been entered in the Scan Criteria pane and the CVE Criteria pane, click **Search** to view the results.

Note: After any change made in the Scan or CVE Criteria pane, click **Search** to view the updated results.

The CVE Search Results table displays the following information:

Column	Description
CVE	The CVE ID number
Filters	The filters associated with that CVE **Note:** If there is more than one filter, click the **+** symbol next to the CVE column to view all of the filters.
Not Protected Profiles	Profiles that are not protected from that particular CVE
Protected Profiles	Profiles that are protected from that particular CVE
Assets	IP addresses for that particular CVE
Flagged	Indicates if the CVE has been flagged
Comments	A place for the administrator to write notes or leave reminders

This area also supports the following tasks:

- **Search**- Updates the CVE search results table, based on the selections made in the Scan Criteria pane and the CVE Criteria pane.
- **Reset All**- Resets the search criteria for both the Scan Criteria pane and the CVE Criteria pane.
- **Details**- Shows the details for individual CVEs in a vulnerability scan file.
- **Policy Tuning**- Displays a wizard that allows the user to compare the data from the imported vulnerability scans to their current profile settings. For more information, see *Functions of the Profile Tuning Wizard* on page 220.

Details

For every CVE within a vulnerability scan file, the SMS tracks information about that CVE. You can access this information by selecting a CVE from the CVE Search Results table and then clicking **Details**. Alternatively, you can double-click a CVE in the search results to view the details.

When you view the details, a dialog box will appear with several tabs that show the CVE details.

Details Dialog

This dialog displays different information about the CVE that was selected.

Details tab- The basic details of the selected vulnerability.

- **URL**- A link to the CVE database.
- **Flagged Status**- A check box that indicates whether or not this CVE is flagged.
- **Comments**- A box for the user to add comments to the CVE.

Ignored Profiles tab- A list of profiles and their ignored status. An ignored profile will not show on the list of covered or not-covered profiles in the CVE.

- **Name**- The name of the profile for this CVE.
- **Ignored**- Shows the ignored status of this profile.

Filters tab- A list of filters identified by the active Digital Vaccine as being effective in protecting the network from this CVE.

Assets tab- The assets are the network IP addresses of the host vulnerable to this CVE as identified by the vulnerability scan. The asset group for the particular IP address is also displayed.

Vulnerability Criteria

The Vulnerability Assessment Policy Tuning update to the SMS also includes a new **Search** criteria pane. This pane allows you to search each individual profile for vulnerability scan files and CVEs.

This search pane is located in **Profiles** > **Inspection Profiles** > **Profile Name** > **Search**.

Vulnerability Criteria search pane

The following is a list of search criteria options for this pane:

- **CVE ID**- Search the profile for a particular CVE based on the ID.
- **Bugtraq ID**- Search the profile for a particular Bugtraq based on the ID.
- **Contains CVE in scan database**- Select the check box to see if this profile contains any CVEs in the scan database.
- **Contains CVE from specific scan file**- Select the check box for each scan file to see if any of the CVEs in that file affect the profile.
- **Scan Vendor**- Search the profile by the scan vendor.
- **Asset Addr(s)**- Search the profile by a particular CVE asset number (IP address).
- **Flagged**- Displays flagged CVEs for the profile.

- **Not Flagged**- Displays CVEs for the profile that have not been flagged.

Vulnerability Criteria Search Results

After the search criteria has been entered, click **Search** to view the results.

Note: After any change made to the search pane, click **Search** to view the updated results.

The Vulnerability Criteria Search Results table displays a new column of information, **CVE IDs**.

The **CVE IDs** column lists the CVE associated with each filter.

More detailed information about each CVE can been seen and edited in the Edit Filter dialog.

You can view this information by selecting a filter from the Search Results table and then clicking **Edit**. Alternatively, you can double-click a filter in the search results to view the edit filter dialog.

For more information, see *Edit Filter Dialog* on page 225.

Edit Filter Dialog

This dialog displays actions to edit the filter settings and displays information about each CVE for the filter.

Filter Settings tab- The basic filter setting options.

- **Filter Info**- The basic information about that filter.
- **Action**- Displays two options:
  - **Use Category Settings**- Use the recommended settings for that filter category.
  - **Use Filter Specific Settings**- Select the state and the action set for that individual filter.
- **Locked**- Select to lock this filter.
- **General Settings**- Select whether or not to **Use Adaptive Configuration Settings** and write comments for that filter.
- **Exceptions**- Add exceptions to that filter or view exceptions that have already been applied to that filter.

Filter Details tab- Displays detailed information about the filter.

CVE tabs- A tab for each CVE associated with the filter is displayed.

Note: Some of the CVE descriptions are more detailed, depending on whether or not the CVE was found in the Vulnerability Scan Database.

- **URL**- A link to the CVE database
- **Vulnerability Scan Database**- Displays basic information, including the flagged state, the last and first found date and time, and any comments. Click **Edit CVE** to view more details or make changes to the CVE. For more information, see *Details Dialog* on page 224.

- **Assets**- Displays the asset IP address and the asset group.

When you are finished making changes in the **Edit Filter Dialog**, click **Distribute** to be taken to the distribute dialog pane or click **OK** to apply the changes to the search results table.

System preferences

A new option has also been added to the system preferences, located in **Edit** > **Preferences** > **Security**. The option to select or deselect **Enable sharing CVE coverage gaps to help TippingPoint improve DV coverege** is now available.

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 428.

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 258.
- Define actions. See *Responder actions* on page 232.
- 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 242.
- 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 107.
- 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

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.

Column	Description
ID	Unique identifier for the host.
Time	Date timestamp of the response.
Policy Name	Name of the Responder policy that triggered the response. If the device triggers the response, the SMS does not display the policy name.
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. • 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.

Column	Description
	• 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 230.
IP	IP address of the host. This column is aggregated with the following information; click the plus (+) symbol to expand the column. • Geo (Map) — Geographical map; click the link to display the map. • Region — Identified region where the host is located. • City — Identified city where the host is located. • Named Rsr — Named resource.
MAC	MAC address of the host.

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.

Column	Description
Time	Time the response occurred.
Type	Type of event that triggered the action.
Status	Current status.
Action	Action enforced in the response.
Source	Source that triggered the response.
Description	Details that describe the event.

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 241.

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 107.

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 re-authenticate. 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 460.

1. Review the *Create or edit a response action* on page 235.
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 242.

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 235.
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 235.
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 theIP 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 235.
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 203.

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 235.
2. Select **SNMPTrap** from the Action Type drop-down list.
3. Click **Trap Destination** (or click **Next**), and then do the following:

   Note: An SNMP trap receiving agent must be running on the destination port configured for this action when you implement the action.

   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:

   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 235.
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 242.

Web response action

Use this action to elicit a Web server response.

1. Review the *Create or edit a response action* on page 235.
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. Fore more information, see *Policies* on page 242. 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:
   a. Web Requests — Select one of the following actions: Block, Redirect to a Web server (an address is required), or Display quarantine Web page.
   b. Other Traffic — Select one of the following actions: Block or Permit.
4. To allow quarantined hosts to access specific sites, click **Quarantine Exceptions**, and then do one of the following:
   a. Click **New** to create a new listing.
   b. Select an existing listing, and then click **Edit**.

   The Quarantined Access dialog opens.
5. On the Quarantined Access Dialog, do the following:
   a. 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.
   b. Destination — Type the IP Address in the field.
   c. 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.

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**.
2. On the Response Actions screen, click **Export**.

   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**.
2. On the Response Actions screen, select a type of action on the Response Action Types table.

3. Click **Delete**.

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. Fore more information, see *Working with the Responder (Response History)* on page 228.

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 242
- *Policy remediation communication (timeout)* on page 243
- *Inclusions and exclusions* on page 161
- *IP correlation and thresholding* on page 243
- *Actions* on page 244
- *IPS destinations* on page 244

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 232.

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 244 and *New response policies* on page 246.

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 242.
   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 243. 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 232.
   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 dependancies 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 246, 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 244.

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 107.

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 242.

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 243. 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 235.
   - **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 107.

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.
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 250.

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 Modelarea, 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 432. 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 252
- *IP Correlation web services* on page 255
- *Testing IP Correlation* on page 256

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 253 (describes how to *Add/edit network mapping* on page 253)
- *Network mapping – bulk load via service mode* on page 253
- *IP Correlation configuration – RFC1213* on page 253
- *IP Correlation configuration – 3Com Network Director or 3Com Enterprise Management Suite* on page 254

- *IP Correlation configuration – external Web API* on page 254

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 253 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 252.

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 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. Use the following parameters:

Parameter	Example
Protocol	HTTP

Parameter	Example
IP	10.100.230.111
CGI Script	cgi-bin/myNetLookup

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://10.100.230.111/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* on page 255
- *Control web service precedence* on page 255

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 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 254), 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**.

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 228.
2. Edit the Manual Response policy. See *Edit the default response policy* on page 244.
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 246.

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*, or from the Documentation section of the SMS client Web page.

Devices

You can use the Devices workspace to configure, monitor, and manage your devices. You can also download TOS updates and distribute them to managed devices from this workspace.

This topic examines device management by the SMS. The following major topics are discussed:

- *SMS managed devices* on page 377 discusses the various security devices managed by SMS.
- *The Devices workspace* on page 258 discusses the screens, menu options, and fields of the Devices workspace on the SMS graphical user interface.
- *Editing device configurations* on page 299 discusses specific tasks to configure and manage your device using SMS.

The Devices workspace

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 428.

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 286 for details.

To open the Devices workspace, click **Devices** on the SMS toolbar.

The top-level options in the navigation pane for the Devices workspace include:

- *Devices (All Devices)* on page 259 — The Devices (All Devices) screen displays an overall summary of all the devices being managed by the SMS. This screen enables you to add a new device to the SMS, create a device cluster, and import/export device configurations.

- *TippingPoint Operating System* on page 277 — The Devices (TippingPoint OS) screen displays details for the TippingPoint operating system (TOS) software in the TOS Inventory list. The TOS Inventory panel enables you to manage TOS packages: import a package from your local machine, download a package from the TMC, distribute a TOS update to one or more managed devices, view details for each Inventory List entry, and delete packages from the TOS Inventory.
- *Virtual segments* on page 279 — The Devices (Virtual Segments) screen enables you to view, create, edit, and manage virtual segments.
- *Segment groups* on page 282 — The Devices (Segment Groups) screen enables you to manage groups of device segments for more control on distributing TOS, SMS, and profile updates. Use this screen to create, view, edit, and delete segment groups.

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:

Column	Description
Name	The name of the device.
IP	The IP address used to make a connection to the device.
Model	The device model. **Note:** For TPS devices, (IPS) displays if you specify the device to function as an IPS, and (NGFW) displays if you specify the device to function as an NGFW.
System Health	The health status indicator that provides information about the hardware components of the managed device.
Performance	The performance status indicator that provides top-level information about the managed device.
Port Health	The port health monitoring indicator that tracks key port statistics for the managed device.
TOS	The software package version installed on the device.
Digital Vaccine	Active Digital Vaccine (DV) version number.

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

See *IPS network configuration and tasks (S-Series, N-Platform/NX-Platform)* on page 333.

To access the Network Summary listings, use the Devices navigation pane to navigate to the Network summary option for All Devices - Member Summary.

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.

See: *IPS events configuration (S-Series, N-Platform/NX-Platform)* on page 341 and *Import IPS profile* on page 337

To edit interface properties, select the Interfaces tab, select an interface, and then click **Edit**.

Additional network configuration information is available through the Network Configuration feature for a specific device, see *IPS network configuration and tasks (S-Series, N-Platform/NX-Platform)* on page 333 and *Core controller network configuration* on page 388.

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 289 and *View events for a specific device* on page 289.

For information on system details for an individual device, see *Device Details* on page 272.

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:

Option	Description
Device	Device name.
Protocol	Protocol of the blocked or rate limited stream.
Src/Dest Address	Source IP address, destination IP address.
Port	Port address.
Slot	IO slot from 1 to 4 (for NX devices).
Segment	IP address of the segment.
Source Interface	Specific source network interface (for NGFW only).

Option	Description
Destination Interface	Specific destination network interface (for NGFW only).
Profile	Name of the profile for the filter triggered.
Reason	Reason for the blocked stream.

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 N/NX-Platform IPS 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:

Entry Title	Description
Device	Device name.
Protocol	Protocol of the blocked or rate limited stream.
Src/Dest Address	Source or Destination IP address.
Port	Port address.
Src/Dest Address	Source or Destination IP address.

Entry Title	Description
Port	Port address.
Slot	IO slot from 1 to 4 (for NX devices).
Segment	IP address of the segment.
Source Interface	Specific source interface.
Destination Interface	Specific destination interface.
Profile	Name of the profile for the filter triggered.
Reason	Reason for the trusted stream.

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:

Option	Description
Device	Device name.
Host Address	Quarantined IP address.

Option	Description
Slot	I/O slot.
Segment	Segment the IP address is quarantined on.
Source Interface	Specific source network interface (for NGFW only).
Destination Interface	Specific destination network interface (for NGFW only).
Profile	Name of the profile for the filter triggered.
Filter	Name of the filter that triggered quarantine.

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:

Option	Description
Device Name	Device name.
Filter Type	Indicates whether the filter is a Security filter or Application filter.
Filter Name	Name of the filter that triggered.
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.

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

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.

Factor	Major Parameters	Critical Parameters
Memory	> = 90%	> = 95%
Temperature (IPS)	> = 73° C	> = 75° C
Temperature (N/NX-Platform IPS)	> = 46° C	> = 51° C
Temperature (NGFW)	> = 62° C	> = 68° C
File System space	> = 90%	> = 95%

Note: Top-level indicators can be configured. To reset health threshold preferences for memory usage, temperature, and hard disk usage, see *Set health thresholds* on page 345. You cannot reset health threshold preferences for an NGFW appliance.

Additional system health monitoring information is available through the Events feature for a specific device, see *IPS events configuration (S-Series, N-Platform/NX-Platform)* on page 341.

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.

Heading	Description
Device	Name of the device.
Incoming	Number of Incoming packets.
Outgoing	Number of outgoing packets.
Blocked	Number of Blocked packets.
Permitted	Number of permitted packets.
Invalid	Number of invalid packets. This amount is part of the Blocked total.
Congestion	Indicator of incoming traffic congestion.

CPU

The CPU section displays the state and performance value expressed as a percentage. You can click **Refresh** to display current values.

Additional performance monitoring information is available through the Events feature for a specific device, see *IPS events configuration (S-Series, N-Platform/NX-Platform)* on page 341.

Device users

The SMS allows SuperUsers to create and edit multiple device users across many devices. In addition to assigning usernames and passwords, SuperUsers can specify whether device users authenticate locally or whether they use a remote server, such as RADIUS or TACACS+, to authenticate. How a device user authenticates indicates the user's role and reflects the authentication preferences in the device configuration. To change the password, the **New Password** and **Confirm Password** fields must be changed. To change the role, select the radio button associated with the appropriate role.

To access this feature, navigate to **Devices** > **All Devices** > **Member Summary** > **Device Users**.

The Device User Accounts screen displays a table that lists the user accounts available on managed devices and enables you to create and edit user accounts.

If the **Show All Devices** check box is selected, actions can be performed on all devices. If the check box is not selected, only the user accounts on devices in the current group are displayed. See *Creating or deleting a device group* on page 285.

The Device User Accounts screen displays the information listed in the following table.

Table heading	Description
State	Enabled or disabled state of the user account associated with the device.
Name	Unique identifier for the user account on the device.
Role	Access level assigned to the user.
Group	Group assigned to the user.
Password Expiration	Number of days until the password expires.
Auth Type	Indicates whether the user authenticates locally or remotely (through RADIUS or TACACS+).
Family	Displays the family name of the managed device, such as IPS, TPS, or NGFW.
Device	Unique name associated with the device.

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 an IPS 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 in saved in packet capture (PCAP) file format and support either an internal or external viewer.

Note: You cannot capture network traffic on the TPS device.

Concurrent traffic capture

The SMS allows multiple captures to run concurrently. Traffic capture files are created by the device on request of the user through SMS or LSM. The traffic capture files are moved from the device if they were created from the SMS or if the user wants to work with the file.

Note: You cannot capture network traffic on the TPS device.

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 current traffic capture.
  - **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.

The **Existing Captures** table details the following:

Column	Description	Type
Name	Name of the new traffic capture file.	Current, Existing
Date	Date of the traffic capture.	Current, Existing

Column	Description	Type
Slot	IO slot from 1 to 4 (for NX devices).	Current, Existing
Segment	Segment on which traffic is captured.	Current, Existing
File Size	Size of file from 1 to 10,000,000 bytes.	Current, Existing
Packets	Number of packets from 1 to 10,000 packets.	Current
Device	Name of the device.	Current, Existing
On Device	File status on the IPS device. A check mark indicates the traffic capture file is present on the IPS device.	Existing

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 TCPDump) are used in traffic captures to refine the types of packets that are captured. The following table outlines the use of traffic capture expressions:

Parameter	Description
ip	IPv4 traffic. By default, only IPv4 traffic is captured.
ipv6	IPv6 traffic.
proto	Designates the protocol of captured traffic. Can be an explicit number or **tcp**, **udp**, or **icmp**.
src	Specifies the source of the traffic. This parameter can be applied to both host and port.
dst	Specifies the destination of the traffic. This parameter can be applied to both host and port.

Parameter	Description
host	Designates a host IP address. IPv4 and IPv6 addresses are supported, as is CIDR format.
port	Designates the port; you must also specify a port number.
Examples:	
`host 172.31.255.254`	Captures all traffic to and from 172.31.255.254.
`src 172.31.255.254`	Captures all traffic from 172.31.255.254.
`dst 172.31.255.254`	Captures all traffic to 172.31.255.254.
`src 172.31.255.254 & dst 10.10.10.10`	Captures all traffic from 172.31.255.254 to 10.10.10.10.
`ip proto tcp`	Captures only TCP traffic.
`ip proto tcp & src port 63`	Captures only TCP traffic on port 63.

Note: You can use the ampersand (&) operator to concatenate parameters. Do not use the "or" operator.

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:

Column	Description
Component	Name of the device component, such as model, license, software, and segments.
Type	Type of component, such as chassis or copper port.
Segment	Device segment.
System Health	Health status of the device. See *Status indicators* on page 273. **Note:** For NX-Platform models, system health displays details about the two fans and the dual power supplies.
Details	Status details or description.

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 261.

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 574.

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.

Graphic	Component
	Copper ports

Graphic	Component
	Fiber ports

Status indicators appear in the following colors.

Color	Status	Meaning
white with gray stripes	Ignore	Ignore the status of this element.
red	Critical	Respond immediately.
yellow	Major	Respond quickly.
cyan	Minor	Respond as time permits.
gray	Informational	You might be interested in this event.
white	Unknown	Status is unknown for this item.
green	Normal	No issues exist for this item.

Color	Status	Meaning
status color with gray stripes	Acknowledged	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.

Additional device monitoring is available through the Events feature for a specific device. See *Event monitoring* on page 342.

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.

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 you device under extreme load conditions and protect against the potential adverse affects 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 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.

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 N-Platform or NX-Platform devices have the option to include LSM create 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.

TippingPoint Operating System

When TippingPoint identifies new attacks or improves methods of detecting existing attacks, the Threat Management Center (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. Digital Vaccine filter packages contain newly developed attack, peer-to-peer, and anomaly filters along with improvements to existing filters. See *Profiles* on page 102.

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.

Note: Depending on the device and the package, certain information may display. For example, 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.

The following table defines the TOS Inventory details.

Column	Description
Version	Version number of the TOS.
Product	Models that the selected TOS package supports.
Released	Date and time of the released version of the TOS.
Downloaded	Date and time of the download to the SMS.
Devices	Device models supported by the release.

The following table defines the distribution progress details.

Column	Description
Device	Name of the device updating to the TOS.
Package	Version number of the TOS.
Start/End time	Start/end date and time of the distribution.
Status	Status of the distribution.
Ext. Status	Additional status information related to this specific distribution.
Progress	Current progress of the distribution.

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 293
- *Import TOS software from a file* on page 293
- *Managing TOS distribution* on page 293
- *Distribute the TOS* on page 294

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 281
- *Traffic flow analyzer* on page 281

You can perform the following tasks:

- *Create a virtual segment* on page 294
- *Delete a virtual segment* on page 295
- *Segment groups* on page 282

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.
- **Name** — User-defined name of the virtual segment.
- **VLAN** — VLAN associated with the virtual segment.
- **Src/Dest Addr** — Source/Destination address of the virtual segment.
- **Segments Assigned** — User-assigned physical segments associated with the virtual segment.
- **Segment Group** — User-created segment group associated with the virtual segment.
- **Profile Name** — Name of profile associated with the virtual segment.

Note: The ANY-ANY segment is not in the virtual segment list. It can exist or be deleted. The priority order for traffic matching on an N-Platform or NX-Platform IPS device is virtual segment, physical segment, and then the ANY-ANY segment.

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:

Column	Description
Group Name	Name of the segment group.
Members	Total number of segment members.
Profile	Name of the associated profile of filters.

Common device tasks

Use the following topics to perform tasks common to all SMS-managed devices:

- *Adding, editing, or deleting a device* on page 283
- *Creating or deleting a device group* on page 285
- *Unmanaging or remanaging a device* on page 286
- *Importing or exporting device configuration* on page 287
- *Viewing and searching events* on page 288
- *Managing versions, updates, and snapshots* on page 290
- *Importing and downloading the TOS* on page 292

- *Managing TOS distribution* on page 293
- *Managing segment groups* on page 296

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.

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.

By default, the SMS can manage up to twenty-five devices. If you need to manage more, you must purchase a license upgrade from TippingPoint. See *SMS node count license* on page 419.

Note: 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.

Add a device

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. Once 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 (N-Platform or NX-Platform devices running TOS v3.7.0 or later) and TACACS+ (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 ( ) indicates that the information applies to an IPS device. A fire icon

( ) 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.

Note: During a multiple-devices edit, FIPS Settings are not available and will not display on the Device Configuration screen.

Note: The RADIUS and TACACS+ options and the RADIUS Servers and TACACS+ Servers sections are displayed in Remote Authentication Preferences only if at least one of the managed devices supports RADIUS and TACACS+ authentication. During a multiple-devices edit, setting a RADIUS or TACACS+ server as the Remote Authentication or changing one of these servers only updates 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). Devices that do not support these authentications do not get updated.

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 286.

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. When you unmanage a device, it no longer counts against your SMS license allotment. See *SMS node count license* on page 419.

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 overlayed 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 Settings** 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:

Status	Meaning
Blocked Streams	• Protocols: All, TCP, UDP, ICMP, ICMPv6 • Src/Dest Address: Source/Destination IP Address • Port
Rate Limited Streams	• Protocols: All, TCP, UDP, ICMP, ICMPv6 • Src/Dest Address: Source/Destination IP Address • Port
Trusted Streams	• Protocols: All, TCP, UDP, ICMP, ICMPv6 • Src/Dest Address: Source/Destination IP Address • Port
Quarantined Hosts	• Host Address

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 574.

Note: Not all Traffic Normalization filters result in blocked streams. See *Traffic Threshold filters* on page 158.

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 289 or *View events for a specific device* on page 289.
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.

Rollback to a previous version

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.

   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.

   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 423.

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

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, and N-Platform or NX-Platform IPS 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 293

- *Import TOS software from a file* on page 293

After importing and downloading the file(s), you need to distribute and manage the files. See the following:

- *Managing TOS distribution* on page 293
- *Distribute the TOS* on page 294

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 File** menu item.

   The distribution process displays on the Distribution Progress panel.

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 NX 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 297 and *Edit segment group membership* on page 298.
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.

   Note: For NX 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 428.

Note: For version 2.5.1 and above, the SMS displays an X before the TippingPoint Operating System (TOS) when viewing device information. See *Device Details* on page 272.

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 296
- *Create a segment group* on page 297
- *Edit segment group membership* on page 298

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 NX 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 297
   - *Edit segment group membership* on page 298
   - *Edit the name and descriptions for a segment group member* on page 298
   - *Create a segment group* on page 297
   - *Editing the management port settings for the S-Series devices* on page 305

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.

Note: For NX 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.

   Note: For NX devices the Segment Group table lists the slot number associated with the segment group.

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**.

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 428.

Caution: If an error occurs, the copper cable translator might not support auto-negotiation. See *IPS events configuration (S-Series, N-Platform/NX-Platform)* on page 341 or *IPS port out-of-service* on page 574.

The Device Configuration wizard enables you to configure or edit device-specific settings, depending on your device. See *Device Details* on page 272.

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 277 and *Digital Vaccines* on page 182.
- 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.

Field	Description	Valid Input
Hostname	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.	A valid host name on your network segment, a maximum of 32 characters.
Location	A description of the location of your device.	
Contact	A contact name for your device. **Note:** This feature is only available on TPS devices.	A maximum of 32 characters describing the device contact.

Field	Description	Valid Input
Model	The number of your device model, such as 2200T-IPS.	—
Serial Number	The serial number of your device.	—
Mgmt IP Address	The IP address that you use to make a network connection to your device.	A valid IP address on the network segment the device is attached to in dotted decimal IP address (255.255.255.255) notation.
Network Mask	The network mask in effect on the subnet that your device is attached to.	A valid network mask for the network segment on which your device resides in dotted decimal IP address (255.255.255.255) notation.
Default Gateway	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.	A network device that contains routing tables that list your device and external network entities as well.
Edit Management Port Settings	Informational dialog that provides Port Details and allows you to enable/disable auto negotiation. **Note:** This feature is only available on select IPS devices.	Enable/disable auto negotiation
View Management Port Settings	Click **View Mgmt Port Settings** to view management port settings and current state details.	
TOS	TippingPoint Operating System (TOS).	

Field	Description	Valid Input
	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.	
DV	Digital Vaccine (DV) version numbers.	Settings related to this item have moved to *Digital Vaccines* on page 182.
Auxillary 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 300.

Configure the management network for the N-Platform or NX-Platform IPS

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 300.

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.

The Device Configuration (Services) screen includes the following information:

Option	Description
SSH	Secure connection for using the CLI. Requires a user with SuperUser capabilities.
Telnet	Unsecure connection for using the CLI. Requires a user with SuperUser capabilities. **Note:** Telnet is not supported on TPS devices.
HTTPS	Secure network communication for Web pages. Enabling HTTPS enables Web services for the SMS. See *TippingPoint SMS External Interface Guide*.
HTTP	Unsecure network communication connection for Web pages. Enabling HTTP enables Web services for the SMS. See*TippingPoint SMS External Interface Guide*. **Note:** See *TSE Settings* on page 323 for HTTP mode on TPS devices.
Encrypted Alert Channel Settings	Compiles and sends alerts. Encrypted for security. You can disable this service to use SNMP. • **Enable Normal Mode** —Sends alerts as they are received • **Enable Batch Mode** — Compiles alerts according to a configured **Wait Time Interval** (minutes ranging from 1 to 60). Enter an amount of minutes if selecting this option. • **Disabled (Use SNMP)** — Alerts are sent using SNMP, disabling this service. **Note:** You must enable Encrypted Alert Channel if your profile's Capture Additional Event Information setting includes HTTP. SNMP does not support HTTP context. **Note:** Encrypted Alert Channel settings are not supported on TPS devices or NGFW appliances.

Option	Description
Data Retrieval Service	Enables the SMS to retrieve and display traffic stats by port per device. **Note:** Data Retrieval Services only apply to IPS devices.
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:

Column	Description
SSH	Secure connection for using the CLI. Requires SuperUser access.
HTTPS	Secure network communication for Web pages. Enabling HTTPS enables Web services for the SMS. See the *TippingPoint SMS External Interface Guide*.
Inband Mgmt.	Specifies that appliance management is done locally through the network itself.

Column	Description
DNS Lookup	Supplies the address or addresses that should be consulted for host name to IP address resolution.
NTP Lookup	Designated primary SNTP Server.
RADIUS Lookup	Server for administrative login authentication and network user authentication.
LDAP Lookup	Server for administrative login authentication and network user authentication.
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 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.
Email Notifications	Server for email alerts.

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)

On the HA (High Availability) screen of the Device Configuration wizard, you can configure settings for Intrinsic Network High Availability (INHA) and Transparent Network High Availability (TRHA).

Intrinsic Network High Availability is the ability of multiple SMS and LSM applications and their devices to see and direct the flow of network traffic between devices and their ports. When traffic flows through the ports of a device, one port might have an issue occur causing an interruption in traffic. The port then transfers the traffic flow to the other available port or device accordingly.

Through the INHA, the system routes network traffic by signaling one device, its port, and its LSM of the IP address, connection table, and flow information. The target port, device, and LSM then builds the information from scratch, to handle network traffic for optimum usage. It transfers the TCP flow when failovers occur.

Transparent Network High Availability performs the same service; however, it differs by constantly updating devices of the TCP flow information. For these networks and devices, the fail-over port/device does not have to rebuild the information flow tables based on the information sent from the failing port/

device. It receives information from an XSL to update its connection table settings. Once updated, this type of network HA quickly transfers fail-over traffic without having to rebuild the settings.

On the Device Configuration (HA (High Availability)) screen, you can configure the following:

- **Intrinsic HA** — Determines how the device manages traffic on each segment in the event of a system failure. When the system fails, the device goes into Layer-2 Fallback mode and either permits or blocks all traffic on each segment, depending on the Layer-2 Fallback action setting for the segment. When the device is in Layer-2 Fallback mode, any traffic allowed through the device will not be inspected; it simply passes through the device.
- **Transparent HA** — Enables you to install two device in a redundant network configuration. Transparent HA keeps the devices in sync with each other so that if one experiences a system failure, the network flow can be routed to the other with no interruption in intrusion prevention services. For TPS devices, you must use the HA ports.
- **Zero Power HA** — Zero Power High Availability (ZPHA) that ensures constant, non-interrupted flow of network traffic. If the power is interrupted, the ZPHA bypasses the IPS device, thus providing continuous network traffic. ZPHA is available for the IPS as an external modular device or as optional bypass I/O modules on NX-Platform devices.

The Device Configuration (HA (High Availability)) screen includes the following information:

Column	Description
Normal	Normal mode for the TRHA
Layer2 Fall Back	Source IP address of the blocked stream
TRHA enablement	Source port of the blocked stream
Partner IP Address	Destination IP address of the blocked stream
Dest Port	Destination port of the blocked stream

Configure network HA

For information on how to configure HA for the Core Controller, see *Management information* on page 385.

1. In the Device Configuration wizard, select **HA (High Availability)** from the navigation pane. The Device Configuration (HA (High Availability)) page displays.
2. For the **Intrinsic HA**, select one of the following, and then click **Apply**:
   - **Normal** — Overrides all INHA settings
   - **Layer-2 Fallback** — Enables INHA configurations per segment
3. In the **Transparent HA** section, click the **Enable** check box.
4. Enter the **Partner IP Address**.
5. For Zero Power HA, select **Normal** (default) or **Bypass IPS** for pass through traffic, and then click **Apply**.
6. 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 574.

Enable/disable the NX-Platform Bypass Mode on an installed Bypass module

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 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.

   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.

   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 Configurationwizard.
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.

   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.

   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 E-Series/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 342
- *Reset events/logs* on page 342

Remote syslog

A remote syslog server is another channel that you can use to report filter triggers. 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 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.

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 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 102.

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,
00000002-0002-0002-0002-000000000164,"0164:
ICMP: EchoRequest (Ping)","0164: ICMP: Echo
Request(Ping)",icmp,216.136.107.233:0,216.136.107.91:
0,20050113T125205+0360,199,"
",1,3:1
```

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.

Field	Description
1	Log-type; ALT = alert, BLK = block, P2P = misuse and abuse
2	Version of this message format
3	ISO 8601 Date-Time-TZ when this alert was generated
4	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)
5	Sequence ID
6	(reserved)
7	Action performed (Block or Permit)

Field	Description
8	Severity (Low, Minor, Major, or Critical)
9	Policy UUID
10	Policy Name
11	Signature Name
12	Protocol name (icmp, udp, tcp, or unknown)
13	Source address and port, colon delimited
14	Destination address and port, colon delimited
15	ISO 8601 Date-Time-TZ when the aggregation period started
16	Number of events since start of aggregation period
17	Traffic Threshold message parameters
18	Packet capture available on device (available = 1; none = 0)
19	Slot and segment of event

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 574.

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:

- **Manual – Internal Device Time** — The device uses its internal CMOS clock.
- **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.

The Device Configuration (Time Settings) screen includes the following information:

Column	Description
Manual/Internal Device Time	The internal time for the device. You can set this time manually.
NTP Server	An NTP server is configured that optionally authenticates all time messages before they can be accepted as a time source.
Remote SNTP Server	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. **Note:** This feature is not supported on TPS devices or NGFW appliances.
Time Localization/ Time Zone	Indicates the time zone for the device, including an option for daylight savings time.

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 for the N-Platform or 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 655535 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 sever 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**, click 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:

Abbreviatio	Offset from UTC (hours)	Daylight savings time	Time zone name
ACST	+9.5	OFF	AU Central Standard Time
AEST	+10	OFF	AU Eastern Standard/Summer Time
AKST	-9	OFF	Alaska Standard Time
AST	-4	OFF	Atlantic Standard Time
AWST	+8	OFF	AU Western Standard Time
CET	+1	OFF	Central Europe Time
CST	-6	OFF	Central Standard Time
EET	+2	OFF	Eastern Europe Time
EST	-5	OFF	Eastern Standard Time
GMT	0	OFF	Greenwich Mean Time
HST	-10	OFF	Hawaiian Standard Time
JST	+9	OFF	Japan Standard Time

Abbreviation	Offset from UTC (hours)	Daylight savings time	Time zone name
KST	+9	OFF	Korea Standard Time
MSK	+3	OFF	Moscow Time
MST	-7	OFF	Mountain Standard Time
NZST	+12	ON	New Zealand Standard Time
PST	-8	OFF	Pacific Standard Time
WET	0	OFF	Western Europe Time
GMT-12	-12	OFF	Time zone GMT-12
GMT-11	-11	OFF	Time zone GMT-11
GMT-10	-10	OFF	Time zone GMT-10
GMT-9	-9	OFF	Time zone GMT-9
GMT-8	-8	OFF	Time zone GMT-8
GMT-7	-7	OFF	Time zone GMT-7
GMT-6	-6	OFF	Time zone GMT-6
GMT-5	-5	OFF	Time zone GMT-5
GMT-4	-4	OFF	Time zone GMT-4
GMT-3	-3	OFF	Time zone GMT-3

Abbreviation	Offset from UTC (hours)	Daylight savings time	Time zone name
GMT-2	-2	OFF	Time zone GMT-2
GMT-1	-1	OFF	Time zone GMT-1
GMT+1	+1	OFF	Time zone GMT+1
GMT+2	+2	OFF	Time zone GMT+2
GMT+3	+3	OFF	Time zone GMT+3
GMT+4	+4	OFF	Time zone GMT+4
GMT+5	+5	OFF	Time zone GMT+5
GMT+6	+6	OFF	Time zone GMT+6
GMT+7	+7	OFF	Time zone GMT+7
GMT+8	+8	OFF	Time zone GMT+8
GMT+9	+9	OFF	Time zone GMT+9
GMT+10	+10	OFF	Time zone GMT+10
GMT+11	+11	OFF	Time zone GMT+11
GMT+12	+12	OFF	Time zone GMT+12

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 261.

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** — No security checking, basic, or maximum security checking.
- **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 Period** — Lockout time from 1 to 1440 minutes.

The following password expiration options apply to accounts that are configured for local authentication only:

- **Password Expiration** — Disabled, 10 to 90 days, 6 months or 1 year.
- **Password Expiration Action** — Force user to change password; notify user of expiration; deny login, SuperUser must reset password; or disable the account.

Note: You cannot disable the password expiration for a Threat Protection System (TPS) device; therefore, **Disabled** is not available as an option.

Local Authentication Only

Local — 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 324

Remote Authentication

Note: This pages 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. If the device does not support RADIUS authentication, the RADIUS options are disabled. TACACS+ authentication is supported only on 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

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.

Setting	Description
IP Address	IP address of the RADIUS server.

Setting	Description
Port	Port on the RADIUS server that listens for authentication requests; the default is port 1812.
Authentication Protocol	Authentication method used on the RADIUS server: • PAP • MD5 • PEAP/EAP-MSCHAPv2 To use the PEAP/EAP-MSCHAPv2 protocol, you must first import an X509 certificate for the RADIUS 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. For more information about certificate management, see .
Secret/Confirm Secret	String used to encrypt and sign packets between RADIUS clients and the RADIUS server, set in the RADIUS client configuration file.
Timeout	Timeout, in seconds, for communication with the RADIUS server. Default is 3.
Attempts	Number of times communication with the RADIUS server is attempted. The default is 1 (no retries after first unsuccessful attempt to contact RADIUS server).

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

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.

Setting	Description
IP Address / Hostname	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).
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.

Setting	Description
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®

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 an IPS 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. If there are no NX-Platform IPS 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 for NX-Platform devices

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 affects 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 affect.

- **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.

Note: You must reboot the device to completely enable or disable this service.

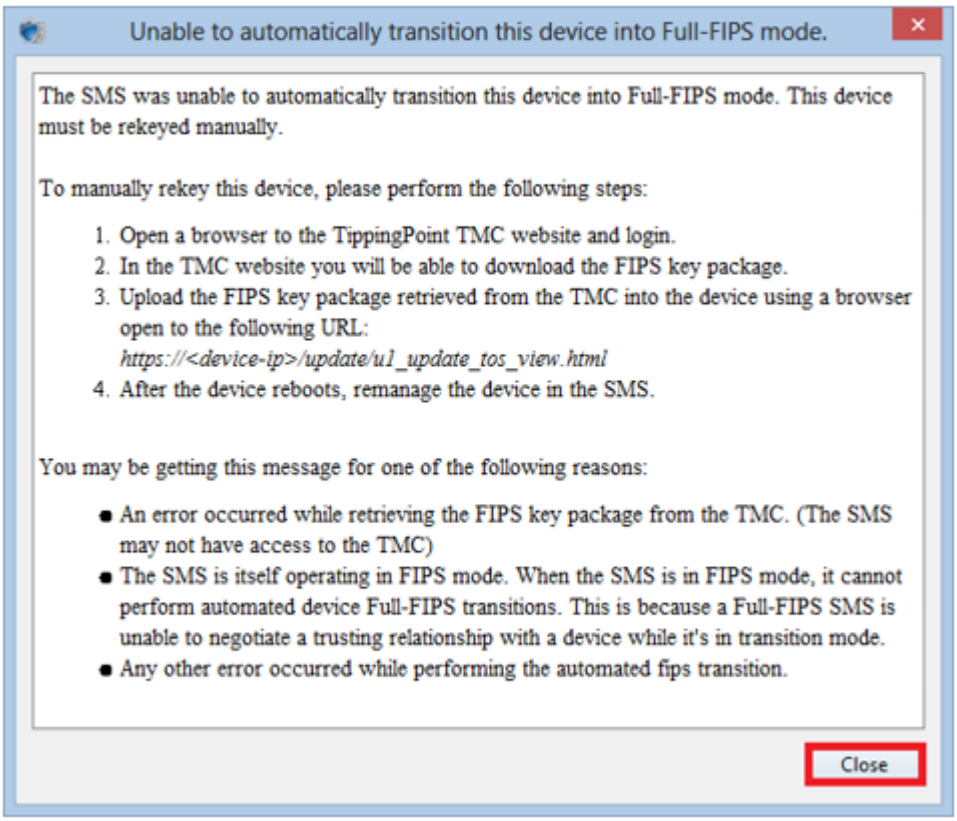
Setting	Description
None	No FIPS compliance actions or restrictions are activated on the device.

Setting	Description
Crypto	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.
Full	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 331.

Enable FIPS on IPS device using SMS

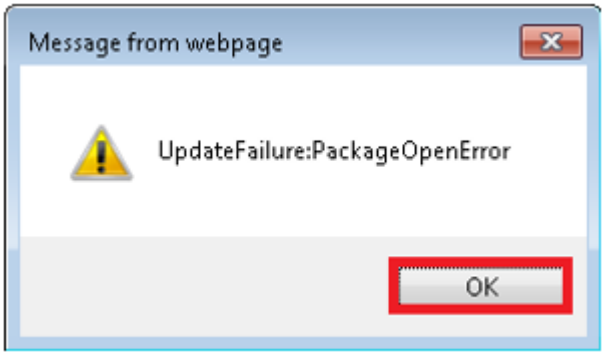
Important: Before you can enable FIPS on a managed IPS device, you must make sure that FIPS mode is disabled on the SMS. If the SMS does have FIPS mode enabled, enable FIPS on the IPS device using the IPS CLI. Refer to the product document for your IPS device.

1. Manage the device from the SMS.
2. Right-click on the device from the All Devices page and select **Edit > Device Configuration**.
3. On the Device Configuration page, select **FIPS Settings**.
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:



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 ay 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.

SSL Inspection

For managed 2200T devices, the SMS SSL inspection.

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. 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 2200T to inspect SSL sessions.
- **Persist Private Keys** — Select this check box to store private keys for SSL server certificates on the 2200T device.

IPS network configuration and tasks (S-Series, N-Platform/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 (S-Series and N-Platform)* on page 334
- *Ports tab* on page 338

You can perform the following tasks:

- *Import IPS profile* on page 337
- *IPS events configuration (S-Series, N-Platform/NX-Platform)* on page 341
- *Delete a virtual segment* on page 295
- *Import IPS profile* on page 337

Segments tab (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 279 and *Segment groups* on page 282.

- **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 (NX-Platform)

The Modules & Segments tab displays the following information about the NX-Platform IPS:

- Modules
  - **Slot** — IO slot from 1 to 4
  - **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 337
- Unassign physical segments from a virtual segment
- *Delete a virtual segment* on page 295

See *IPS network configuration and tasks (S-Series, N-Platform/NX-Platform)* on page 333

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 *IPS network configuration and tasks (S-Series, N-Platform/NX-Platform)* on page 333

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 segment details

1. On the Devices screen, expand the **All Devices** in the navigation pane.
2. Select a TPS 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 Layer2 Fall Back action:
   - **Block All**
   - **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 inspection profiles* on page 127.

Edit a virtual segment

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.

   Note: The ANY-ANY segment is not in the virtual segment list. It can exist or be deleted. The priority order for traffic matching on an N-Platform or NX-Platform IPS device is virtual segment, physical segment, and then the ANY-ANY segment.

Ports tab

The Ports tab displays the following information:

- **Type** — Type of port, such as Management Port or Data Port.
- **Slot** — IO slot from 1 to 4 (for NX-Platform devices only).
- **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 (for 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 (N-Platform and NX-Platform devices)

N-Platform and NX-Platform Devices can translate VLAN IDs per segment. The translation occurs after the inspection so incoming VLANs are used for virtual segments.

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 number from 1 to 4 (NX-Platform only).
- **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 for N-Platform or NX-Platform IPS devices

1. On the Devices screen, expand the **All Devices** in the navigation pane.
2. Select an N-Platform or NX-Platform IPS device and expand the options.
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 devices the Port Selection area, 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**.

IPS events configuration (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 342
- *System health* on page 343
- *Performance* on page 345
- *Port health* on page 347
- *Traffic* on page 347
- *System log* on page 348
- *Audit log* on page 350

For additional information on monitoring your IPS device, see *Events summary* on page 261.

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 262
- *Quarantined hosts* on page 264
- *Adaptive Filter* on page 265

The Events screen for N-Platform or NX-Platform 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 262
- *Trusted streams* on page 263

- *Quarantined hosts* on page 264
- *Adaptive Filter* on page 265

Event monitoring

In the Devices (Events) area, you can perform the following tasks to help you monitor events:

- *View realtime graph data* on page 342
- *View log* on page 342
- *Reset events/logs* on page 342

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 350.
   - **System Log** — Displays the system log. See *System log* on page 348

   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:
   a. 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**.

Column	Description
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 NX models • Voltage The following items also display for NX models • CPU XLR • Fans • Power Supply #1, Power Supply #2 • Voltage The following items also display for IPS 5000E: • Disk/boot • Disk/log • Disk/usr

Column	Description
	• Disk/opt The following item also displays for IPS 50: • Disk/usb0
State	One of the following status indicators: • Red square icon — critical • Yellow square icon —major • Green square icon — normal
Current Value	The percentage amount of the component used.
Details	The amount used of the total available megabytes (MB).

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 574.

See *System health summary* on page 266.

Health stats

The **Health Stats** section displays the following information about the managed system health:

Health threshold settings

These 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.

For default health threshold settings, see *Table* on page 266 and *Set health thresholds* on page 345.

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 342.

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**.

   The Devices - Health Thresholds dialog box displays.
5. For **Storage**, enter a **Major** and **Critical** amount. The amount should be between 60% to 100%.
6. For **Memory**, enter a **Major** and **Critical** amount. The amount should be between 60% to 100%.
7. For **Temperature**, enter a **Major** and **Critical** amount. The amount should be between 40 to 80 Celsius.
8. Click **OK**.

Performance

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 266.

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 tab* on page 345
- *Tier Statistics tab* on page 346

Performance Data tab

Monitored Performance data is displayed in textual and graphical formats. The Packet Stats Text section displays the following information:

Entry Title	Description
Device	Name of the device.
Total Packets	The total number of packets for the device.

Entry Title	Description
Blocked	The number of blocked packets.
Permitted	The number of permitted packets.
Rate-Limited (N-Platform/ NX-Platform)	Number of rate-limited packets.
Trusted (N-Platform/NX-Platform)	Number of trusted packets.
Dropped	The number of dropped packets.

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 (E-Series/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 342.

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.

Port health

Port health monitoring for IPS devices tracks key port statistics for managed devices and provides information in textual and graphical formats. For the NX-Platform, the SMS displays the slot number in addition to the other IPS 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 337.

Traffic

The **Traffic** section tracks and compiles information on all traffic managed by the device.

Traffic graphs

- **Frame Size** — Traffic profile by framesize, 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 342 and *Device Traffic templates* on page 83.

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 266.

The following table details the system log details:

Heading	Description
ID	The ID of the alert in the log.
Message	The description of the alert.
Entry Time	The time of the alert added to the log.
Severity Level	The severity level of the alert in the log.
Component	The component affected by the alert or event, such as report, policy, and OAM.

You can do the following:

- *View log* on page 342 — Details how to view a log
- *Reset events/logs* on page 342 — 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:

Event	Origin	Component	Definition
Add Device	SMS	device name	*Component* has been discovered and configured.
Alert Status	SMS	device name	The alerts status of *component* has changed to *status*.
Block Status	SMS	device name	The block status of *component* has changed to *status*.
Cold Start	device	device name	*Component* has been rebooted.
Config Sync	SMS	device name	SMS management data has been synchronized with *component*.
Connection Down	SMS	device name	*Component* has stopped communicating with the SMS.
Connection Up	SMS	device name	*Component* is now communicating with the SMS.
Device Availability	device	device name	*Component* entered Fall Back state at *time* or *Component* was available for service (not in the Fall Back state) at *time*
Delete Device	SMS	device IP	*Component* has been deleted from the SMS.
Delete Host	SMS	device component	*Component* has had a host removed from the SMS.
Fall Back Status	SMS	device-name	*Component* is in Fall Back state or *Component* is available for service (not in the Fall Back state)
Hardware Health	device	device component type	*Component* is *status*.
Hardware Status	SMS	device component	The health status of *component* has changed to *status*.

Event	Origin	Component	Definition
Manage Device	SMS	device name	The SMS is now managing *component*.
Managed From Device	device	device name	*Component* is now managed by the SMS.
New Host	SMS	device component	*Component* has a new host found by the SMS
Resource Health	device	resource name	*Resource-name* has changed from *pre-status* to *post-status*.
Resource Status	SMS	device component	The resource status of *component* has changed to *status*.
Unmanage Device	SMS	device name	The SMS is no longer managing *component*.
Unmanaged From Device	device	device name	*Component* is no longer managed by the SMS.
Warm Start	device	device name	*Component* has been restarted.

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.

The following table details the audit log details:

Heading	Description
ID	The ID of the alert in the log.
Time	The time of the alert added to the log.
Access Level	The access level of user causing the alert. Can include SMS for the system, SuperUser, and so on.
Interface	The interface used that generated the alert or event: WEB or SYS.
IP Address	The IP address of the system that generated the alert or event.
Component	The component affected by the alert or event, such as report, policy, and OAM.
Result	The result of the event, such as PASS for successful.
User	The user account causing the alert.
Message	The description of the alert.

You can do the following:

- *View log* on page 342
- *Reset events/logs* on page 342

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.

IPS traffic capture configuration (S-Series, N-Platform/NX-Platform)

Traffic capture is available for IPS and N-Platform devices that use TOS V. 3.2.1 or later and for NX devices. This feature allows permitted users to view and manage traffic capture files residing either on the SMS or on an IPS 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 in 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 current traffic capture
  - **Refresh Statistic**s— 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

The Current Captures table details the following:

Column	Description
Name	Name of the new traffic capture file
Date	Date of the traffic capture
Slot	IO slot from 1 to 4 (for NX devices)
Segment	The segment on which traffic is captured
File Size	Size of file from 1 to 10,000,000 bytes
Packets	Number of packets from 1 to 10,000 packets

The Existing Captures table details the following:

Column	Description
Name	Name of the new traffic capture file

Column	Description
Date	Date of the traffic capture
Slot	IO slot from 1 to 4 (for NX devices)
Segment	Segment on which traffic is captured
File Size	Size of file from 1 to 10,000,000 bytes
On Device	File status on the IPS device; a check mark indicates the traffic capture file is present on the IPS device

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. Navigate to the **Devices** > **All Devices** area, select an N-Platform or NX-Platform 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: NX-Platform 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).
- **Expression** — Expression based on standard TCP Dump parameters that refines the types of packets that are captured.

5. Click **OK**.

Export a traffic capture file

1. Navigate to the **Devices** > **All Devices** area, select an N-Platform or NX-Platform 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 an N-Platform or NX-Platform 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**.

IPS distribution queue configuration (S-Series, N-Platform/NX-Platform)

SMS supports queuing of any package distributions to an IPS 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 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 355
- *Change or delete a distribution queue entry* on page 355

For additional information about package distributions, see:

- *TippingPoint Operating System* on page 277
- *Distribute inspection profiles* on page 127
- *Digital Vaccines* on page 182

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. 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.

   The Distribution Queue table lists all the packages in the queue.
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 (N-Platform or NX-Platform)

Through the Events screen for N-Platform or NX-Platform IPS 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 2500N, 5100N, 6100N, and NX-Platform devices. The maximum number of bypass rules is eight.

To access the Inspection Bypass feature for a device, use the left navigational menu to navigate to the N-Platform or NX-Platform IPS device and select the **Inspection Bypass** listing.

The Inspection Bypass Rules table details the following items:

Entry title	Description
ID	Reference ID of the rule in the listing.
Enabled	Enable/disabled status.
Name	Name of the bypass rule. The name is an SMS-only feature. and does not appear on the IPS device.
Ethernet Type	Type of Packets that are exempt from traffic based on the Rules criteria: • IP — Type of IP packets e that are exempt. • Not IP — All non-IP packets that are exempt from inspection. • Protocol — Packets from a specified protocol that are exempt.
IP Protocol	Transport layer protocol of packets to exempt from inspection.
Statistics	Statistics associated with a bypass rule.
Src IP	Source IP address of packets to exempt from inspection.
Src Port	Source port of packets to exempt from inspection. This field is valid only if TCP or UDP is specified in the **IP Protocol** field.
Dst IP	Destination IP address of packets to exempt from inspection.
Dst Port	Destination port of packets to exempt from inspection. This field is valid only if TCP or UDP is specified in the **IP Protocol** field.

Configuring Inspection Bypass Rules includes the following areas:

- **Name** — Descriptive name and enabled state option.
- **Protocol** — Ethernet frames that match these settings and the settings specified for VLAN, MPLS & Tunneling are delivered directly to the other side of the IPS segment. They are not routed for inspection.
- **VLAN, MPLS & Tunneling** — Configure the Virtual LAN (VLAN) tag, Multi Protocol Label Switching (MPLS) label and Tunneling settings. 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/edit an inspection rule

Before you begin, review the information in *Device Details* on page 272.

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 an N-Platform or NX-Platform device that supports inspection bypass.
2. From the navigational pane expand the options for the device and then select **Inspection Bypass**.
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 **Protocol** from the wizard navigation pane.
   - Select the Ethernet Type.
   - For IP Protocol, specify the Source/Destination ports and addresses.
7. Click **Next** or select **VLAN and MPLS & Tunneling** 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 MPLS** 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**).
8. 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 devices, the segments are listed by slot numbers.
9. Click **Finish**.

Packet trace (S-Series, N-Platform/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 358
- *Download all packet trace files for a device to the SMS* on page 358

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 358.

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.

SecBlade IPS configuration

Unlike traditional IPS appliances which have a hard coded mapping between the physical ports and the IPS segment pairs, the TP SecBlade allows you to configure how the physical ports are assigned to segment pairs. There are a variety of potential types of segment layouts. For a layout that is similar to the ports on TippingPoint IPS devices, configure one or more virtual segments using the four external data ports.

The following table lists the default port mapping on the TP SecBlade 1200N:

Port	Mapping
Port 1	Unused
Port 2	Dedicated management port
Combo Ports 3 and 4	Inspection Segment 1
Port 5	Inspection Segment 2

Note: The default configuration of the backplane port is to work as a single port segment, but this is not a fixed configuration. All five ports can operate as members of either standard two-port segments or single-port segments.

From the SMS, you can custom configure the following areas:

- *Management port (SecBlade IPS)* on page 359
- *Physical ports and physical segments (SecBlade IPS)* on page 360

You can perform the following tasks:

- *Review or edit management port settings for the TP SecBlade* on page 360
- *Review/edit segment mapping for physical ports on the SecBlade* on page 360
- *Edit data port details for an IPS (includes TP SecBlade)* on page 361
- *Create/edit VLAN translation for N-Platform or NX-Platform IPS devices* on page 340

Management port (SecBlade IPS)

The management port is a separate network connection used to communicate with your TippingPoint IPS device. By default, Port 2 on the TP SecBlade is configured as the management port. The user can set the management port to any dedicated external port, or any VLAN on an external port or on the backplane port. In either case, management traffic can be untagged or use a VLAN tag. The management port can be connected to another switch port that is a member of a particular VLAN, whether the port is on the front panel or on the backplane. If you want to use a port for both management and data traffic, you must segregate management traffic from data traffic by assigning different VLANs.

During the initial device setup, you configure the network setting for the Management Port using the serial console. After the IPS is installed, you can use the **Edit Management Port** option in the SMS to review or modify the settings.

Review or edit management port settings for the TP SecBlade

1. From the **Devices** area do one of the following tasks:
   - In the left navigational tree, select **All Devices**. After the devices display in the right pane, right-click on the graphical representation of the N-Platform or NX-Platform device you want to configure, and then select **Edit** > **Device Configuration**.
   - In the left navigational tree, expand **All Devices** , and then select **Member Summary**. Select an entry in the **All Devices (Management Information)** table on the **Management Information** tab, and then click **Edit**.
   - In the left navigational tree, expand **All Devices,** expand a specific device entry, select **Device Configuration**, and then click **Edit** on the details summary screen.
2. In the Device Configuration wizard, select **Management Information** from the left navigational menu.
3. To review or make changes to the Management Port configuration, click **Edit Mgmt Port Settings**.

   The Port Details-Edit Management Port dialog displays
4. To change the port configuration, select a port number from the drop-down box next to Hardware and enter VLAN ID, if applicable.
5. Make any desired changes to the Auto Negotiation settings.
6. When your changes are complete, click **OK**.

Physical ports and physical segments (SecBlade IPS)

The IPS allows you to configure the four external ports for speed, duplex, auto negotiation and enable/disable status. The internal 10G port can only be set to enable/disable. Layer 2 Fallback can be configured to block or permit. Link Down Synchronization is fully supported.

Physical ports 3 and 4 include both a copper port and a module. These combo ports appear as a single port in the interfaces and not as distinct copper and ports. The copper port and module are mutually exclusive.

The combo ports automatically select whichever interface has a link present. It is not possible to manually override whether the copper port is active.

Note: In addition to the physical segments on the device, you can also configure virtual segments, a software representation of ports composed of two virtual ports (incoming and outgoing) that allows you to classify and filter traffic on the network by port, VLAN ID and CIDR.

Review/edit segment mapping for physical ports on the SecBlade

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.**

4. Select the **Segments** tab, and then click **Segment Mapping**.
5. In the Edit Segment Mapping dialog, review the entries and make any needed changes to Segments 1 through 5. You can select one of the following options:
   - Both ports set to **None** — segment unused.
   - Both ports set to different physical ports — forms a normal two-port segment.
   - Both ports are set to the same physical port — forms a single port segment and needs VLAN translation entries configured in order to pass traffic. See *Create/edit VLAN translation for N-Platform or NX-Platform IPS devices* on page 340.
6. Click **OK**.

Edit segment details for an IPS (includes TP SecBlade)

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 **Segments** tab.
4. In the **Physical Segments** table, select an entry and click **Edit**.
5. Modify the **Segment Name**.
6. For **Intrinsic Network HA**, select a Layer2 Fall Back mode:
   - **Block All**
   - **Permit All**
7. For **Link-Down Sync**, select a mode 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 goes 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.
8. For **Segment Group**, select the appropriate group entry from the drop down box.

Edit data port details for an IPS (includes TP SecBlade)

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.**
4. Select the **Ports** tab.
5. Select a data port from the Ports table, and then click **Edit**.

6. The Port Details - Edit dialog displays. Make any desired changes, and then click **OK**.

   - For **Hardware**, modify the **On** check box if the hardware is physically on or off.
   - 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, you should leave Auto-Negotiation disabled. See the information at the end of these instructions.

   If you are not using Auto Negotiation, modify the following settings:

   - **Line Speed**.
   - **Duplex** setting: **Full** or **Half**.

Backplane Port 5 on the TippingPoint SecBlade

On the TippingPoint SecBlade 1200N, Port 5 is the 10GbE port connected on the switch backplane. This port can be configured to send and receive traffic and to act as a single segment. However, you must configure VLAN translation for the port such that incoming traffic arrives on one VLAN and exits on a different VLAN.

To review or configure the settings for the backplane port 5, follow the general instructions listed for *Review/edit segment mapping for physical ports on the SecBlade* on page 360 and select TP SecBlade port number 5. to add VLAN Translation, see *Create/edit VLAN translation for N-Platform or NX-Platform IPS devices* on page 340.

VLAN translation on a single port

VLAN translation also enables you to use a single port on the TippingPoint SecBlade 1200N act as a segment that receives and sends network traffic. Typically users will use this configuration for Port 5, the 10GbE backplane port.

Traffic looped back on the 10G port without VLAN translation will create a network loop, breaking the network. To allow the backplane port segment to work, the IPS must translate the VLAN IDs on the packets as they pass through the segment. The port must be configured such that the incoming traffic arrives on one VLAN and outgoing traffic is sent on another. You must configure a VLAN translation entry to move the traffic between the VLANs as it passes through the device.

To create or edit a VLAN translation, see *Create/edit VLAN translation for N-Platform or NX-Platform IPS devices* on page 340.

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*.

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*.

Note: When you replace a devices, 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 363
- *IPS device replacement considerations* on page 364

Device replacement limitations

The device replace feature has the following limitation:

- 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.

Old Device	New Device	Device Replace Behavior
Non-N-Platform Device	Non-NX-Platform Device	No Change

Old Device	New Device	Device Replace Behavior
Non-NX-Platform Device	NX-Platform Device	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.
NX-Platform Device	NX-Platform Device	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.

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 364
- *DDoS* on page 364
- *Different models* on page 365

See *Device replace table*.

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.

For complete information on a specific IPS model, see the Release Notes and product documentation, available from the TMC, *https://tmc.tippingpoint.com*.

Replace a device

1. Review all of the topics in this section and the *Device replace table*.
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.

   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 364.
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 364.

   When the replacement process is complete, a dialog appears and directs you to redistribute the appropriate versions of the IPS profiles.

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
- GRE
- Loopback Interface
- Point-to-Point (PPPoE, PPTP, and L2TP)
- VLAN

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*.

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 and .

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.

ExpiryTime— 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 events

The Events screen provides a top view of event information for all managed NGFW appliances. See *Events summary* on page 261.

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 *IPS distribution queue configuration (S-Series, N-Platform/NX-Platform)* on page 354.

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.

Parameter	Description
Cluster Name	Name that is shared with both members of the cluster. Choose a name that makes sense for your organization.
Config Sync By	Method used to synchronize configuration information. **SMS** — 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.

Parameter	Description
	Manual — 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.
State Synchronization	Select the subsystems to include in state synchronization (Firewall, Routing, and IPS), and specify the log level for each subsystem.

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:

Parameter	Description
Encrypt Cluster Traffic	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. **Note:** If the HA port network traffic is physically secure, you do not need to encrypt the traffic. Leaving traffic unencrypted improves performance.
Use management Port for HA Link Failure	Enable the devices to use the management port to connect in the event that the HA port fails.
Auto Negotiation	Specifies if auto negotiation is enabled or disabled on the HA port. Auto-negotiation is enabled by default.
Link Speed	Speed of throughput on the port. Link Speed is uneditable if Auto Negotiation is enabled. Default Link Speed = 1 Gbps
Duplex	Specifies duplex mode on the port (half or full). Duplex mode is uneditable if Auto Negotiation is enabled. Default = Full Duplex
MTU	Maximum transmission unit. Largest data packet size (in bytes, 576–9,216) that is allowed. Default MTU = 9216 bytes
Multicast IP	IP address for multicast address transmission. Default IP address = 239.0.0.10 **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.
UDP Port	UDP port number for multicast address transmission.

Parameter	Description
	Default port = 5404
TTL	TTL setting (in milliseconds, 1–255) for multicast address transmission. Default TTL = 1 ms
Timeout	Timeout (in milliseconds, 100—10,000) for multicast address transmission. Default Timeout = 1000 ms
Retransmission	Number of attempts (1–10) to retransmit multicast address transmission. Default Retransmission attempts = 4

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.

Advanced DDoS tasks

This section includes the following topics:

- *Advanced DDoS supported models* on page 375
- *Advanced DDoS filter configuration* on page 375
- *DDoS preferences* on page 376

Advanced DDoS supported models

The SMS supports DDoS for the following devices:

- 600E/1200E/2400E/5000E
- 660N/1200N/1400N/2500N/5100N (TOS 3.1.x through 3.6 and newer)
- 10/110/330 (TOS 3.1.4, 3.2.2 through 3.6)
- 5200NX/7100NX (TOS 3.5 and newer)
- 2600NX/7500NX (TOS 3.6 and newer)

You must configure the following DDoS filter options in the Device workspace of the SMS:

- 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 workspace of the SMS.

Note: The Devices - Adv. DDoS Configuration screen is only shown for models 600E, 1200E, 2400E, and 5000E. For all other supported devices, the Advanced DDoS configuration options are set in the Profiles workspace.

You can access this screen directly through the Devices screen, or when creating and editing TippingPoint filters through the Profiles screen. See *Advanced DDoS filters* on page 151.

Advanced DDoS filter configuration

To view supported advanced DDoS filter configuration settings for devices, see *Table* on page 151.

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 375. 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 376.
- 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 375. 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 375. To create software-based exceptions, see *Advanced DDoS filters* on page 151.
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 375.

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 377 — 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. With an IPS deployment, the TPS solution is optimized for high resiliency, high availability, and network segment protection from both external and internal attacks.Offer the option of deploying as a Next Generation Firewall (NGFW) appliance or as an Intrusion Prevention System (IPS) device.

V Series Threat Protection System on page 378 — Software appliance designed to provide the same level of functionality available in the TippingPoint Threat Protection System (TPS), but virtually rather than physically.

IPS devices on page 379 — 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 381 — Monitor and control incoming and outgoing traffic.

Core Controller on page 382 — Controls traffic across its three 10GbE network segment pairs and across multiple TippingPoint devices.

SSL appliance on page 407 — Decrypts SSL traffic between clients and site servers and sends the decrypted traffic to an TippingPoint IPS device for analysis.

TippingPoint vController on page 406 — 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 device must be version 4.0 or later. To manage the TPS device, the SMS must be version 4.3 or later.

The TPS family includes:

440T device on page 378

2200T device on page 378

440T device

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 device

The 2200T device delivers the highest level of defense against network intrusion and provides application control.

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 2Gbps 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.

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.

The TOS 4.0.1 version of the vTPS supports the majority of features that were introduced with the 4.0.0 release of the 440T TPS device.

For additional information on the vTPS device, refer to the TMC.

IPS 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 379

N-Platform IPS devices on page 379

NX-Platform IPS devices on page 380

SecBlade IPS devices on page 381

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 IPS 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 IPS devices

The TippingPoint NX-Platform IPS devices are build 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 Input/Output (I/O) modules have hot-swap functionality and are available for the TippingPoint NX-Platform devices:

- 6-Segment Gig-T NX (Gig-T) with 12 Fixed RJ-45 copper ports and a port speed of 1 Gbps
- 6-Segment GbE NX () with 12 ports and a port speed of 1 Gbps
- 4-Segment 10 GbE + NX (+) with 8 Fiber ports and a port speed of 10 Gbps
- 1-Segment 40 GbE QSPF+ NX (Q+) with 2 Fiber ports and a port speed of 40 Gbps

Note: A 40 Gigabit I/O module is hot-swappable with an existing 40 Gigabit I/O module. However, 40Gigabit modules are not hot-swappable with a different module type. For example, a 10Gigabit or 1Gigabit 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/disable the NX-Platform Bypass Mode on an installed Bypass module* on page 312.

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

SecBlade IPS devices

The TippingPoint SecBlade 1200N IPS, an industry-leading Intrusion Prevention Systems (IPS) product developed by TippingPoint, is compatible with the H3C S7500E series switches. You can add multiple TP SecBlade 1200N modules to an H3C S7500E switch for service expansion. The TP SecBlade can be installed in H3C S7500E series switches and inspects up to 1.3 Gbps of traffic.

Configurable ports

The TippingPoint SecBlade features the following configurable ports:

- Two 1Gbps copper-only ports on the front panel of the module
- Two 1Gbps combo copper/ ports on the front panel
- One 10Gbps port connected internal to the switch backplane

Note: If you configure a port as a single-port segment with a single two-way segment, you must configure VLAN translation for the port such that incoming traffic arrives on one VLAN and exits on a different VLAN.

For additional information, see the TippingPoint SecBlade 1200N IPS documentation, available from the Threat Management Center (TMC) website at *https://tmc.tippingpoint.com*.

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 283.

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 283.

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.

Core Controller configuration

Use the following topics to set up a Core Controller device.

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, see 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 283.

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.

Configuring Core Controller mappings

You can use the Core Controller Mapping wizard to configure iLink and device segments manually, or you can choose the auto-detection option. However, auto-detection causes multiple interruptions to traffic flowing through the iLink segment. If you do not want to disrupt traffic on these segments, use the Core Controller Mapping wizard to configure mapping.

The iLinks should be in the same state they were put into during OBE. If the iLink/Segment assignments were not made during OBE, you can make those assignments in the SMS. However, that option can cause fallback due to the link aggregation thresholds. You can add devices through the typical process, or you can add them through the Core Controller setup OBE.

Note: You can manage devices through the SMS before you configure the Core Controller, or you can add devices to the SMS during Core Controller configuration by clicking **NewDevice**.

Use the Core Controller Mapping wizard to configure mappings

1. Identify Connected Devices.

   This step allows the SMS to identify the IPS devices that are connected to the Core Controller so that they can be managed.

   a. From the list of **Available Managed Devices** in the left pane, select the devices that are attached to your Core Controller.

   b. Select the IPS devices that are connected to your Core Controller, and then click the right arrow button to move the selected devices to the right pane.

2. Identify IPS segments connected to Core Controller iLinks.

   This step identifies which IPS segments are physically connected to the Core Controller iLink port pairs.

   a. Select a Core Controller iLink from the list in the left pane.

   b. Click the right arrow button to move the selected iLink to the right pane. Each time you click the arrow, an iLink is added to IPS segments.

3. Associate iLinks with Core Controller10GbE segments. This step maps Core Controller iLinks to the 10GbE segments on the Core Controller.

   a. From the **Link Aggregation** area, select an unassigned Core Controller iLink from the list in the left pane.

   b. Click the right-arrow to move the selected iLink to a 10G Core Controller segment or drag and drop an unassigned iLink to the desired Core Controller segment.

   c. You can set the Link Aggregation Thresholds, if desired.

   Note: The Link Aggregation Threshold value for a core controller 10G segment specifies the percentage of iLinks that must remain operational for that 10G segment. If the percentage of operational iLinks for any 10G segment falls below the threshold specified for that segment, the entire Core Controller enters Layer-2 Fallback mode. The default value is 75%.

4. Configure **Segment Groups**. This step allows you to group all the IPS segments that are connected and mapped to a single Core Controller 10G segment to one segment group. Setting up segment groups helps to simplify configuration and reporting.

   a. For each 10G segment and its associated IPS segments, select an existing segment group from the Segment Group drop-down box. To create a new segment group, click **New**.

   b. After completing the information, click **Finish** to save your entries.

   c. To change any of the mappings you set up in the Core Controller Mapping wizard, click **Edit Mapping**.

d. To change any of the Core Controller device settings, click **Edit Device Configuration**. To display current values, click **Refresh**. See *Device Details* on page 272.

Configuring the Core Controller

After the SMS is managing the Core Controller, you can configure network parameters on the device. See *Authentication and authorization* on page 428.

The Device Configuration wizard enables you to configure or edit several groups of network settings, depending on the device. See *Device Details* on page 272.

Note: When you click OK, the SMS restarts the segment, updates hardware settings for the device, and restarts 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 574.

Edit Device Configuration

1. In the Devices workspace, expand **All Devices**, and select the node for the Core Controller.
2. On the Device Configuration screen in the content pane, click **Device Configuration**.
3. Use the Device Configuration wizard to configure settings or to edit the configuration; click a node in the navigation panel to edit the associated settings.
4. Click **OK** to close the Device Configuration wizard and save your changes.

Management information

The Management Information page enables you to configure the **Hostname**, **Location**, and **Default Gateway** for the device.

To edit the management port settings, click **Edit Mgmt Port Settings**.

Note: Incorrect settings for the default gateway or management port prevent management communication with the device.

This page also provides options to reboot the device, shutdown the device, or reset filters to their recommended state.

If you set up an SSH client, you can click SSH Terminal to access the client. See *Change the SSH client setting* on page 18.

Services

The Services page allows you to do the following:

- Enable or disable services such as SSH and Telnet

Note: For the SMS to communicate with the Core Controller, SSH must be enabled.

- Enable or disable the retrieval of port traffic statistics, which are used in traffic reports

- Enable FIPS

To enable FIPS, select **FIPS 140-2 Mode**, and then click **OK**. You must then reboot for the system to operate in FIPS mode.

HA (High Availability)

High Availability directs the flow of network traffic between devices and ports when a device fails over. The HA page enables you to configure options for Intrinsic HA and Zero Power HA.

Intrinsic HA determines how the device handles network traffic in case of an internal failure, in which case the device automatically falls back to Layer 2 (transparent switch).

Each Core Controller 10G segment can have 1 to 24 iLinks assigned and a percent threshold configured. When the number of in-service iLinks falls below the threshold, the Core Controller goes into Layer 2 Fallback mode. When the iLink count moves above the threshold, the Core Controller automatically exits Layer 2 FallBack and returns to the Normal state.

When the Core Controller goes into Layer 2 Fallback mode, packets received on a 10GbE port are sent directly to the transmitter port on the same 10GbE segment. Packets are not sent to the iLinks, and flow management methods are not applied. During Layer 2 Fallback, the available actions are **Permit All** or **Block All**.

The *Intrinsic HA Settings* specify the action to be performed when the SMS is in Layer 2 fallback mode:

- Block All —No traffic is passed across the segment.
- Permit All — Packets are passed directly from one side of the segment to the other without inspection.

The *Intrinsic HA State* provides two choices for segment fallback action:

- Normal — Core Controller routes traffic to iLinks and IPS devices for inspection.
- Bypass IPS— Core Controller 10G segment blocks all traffic or permits all traffic depending on the Layer-2 Fallback Action setting.

The Core Controller might be put into Level 2 Fallback mode under the following circumstances:

- User-forced Level 2 Fallback mode
- Congestion exceeds the configured threshold
- No iLinks are configured or available for the 10GbE segment
- Active iLinks on the segment are below the assigned threshold value
- Software fault
- Hardware time-out

To enable transparent high availability, select **Enabled** on the Transparent HA panel, and select a partner device form the drop-down list.

iLink Flow Protection Settings protect Core Controller iLinks when oversubscription occurs. When oversubscription on an iLink is detected, the Core Controller routes all traffic for that iLink to the 10Gb segment. When this oversubscription has subsided, you can choose to automatically stop the rerouting and resume sending to that iLink. Select from the following options:

- **Enable** — Pushes all traffic for any iLink that is oversubscribed to the 10 Gb segment.
- **Enable Auto Recovery** — Automatically stops the push of all traffic for any iLink when the oversubscription has subsided.

Note: Deselect **Restore Normal after iLink Threshold Recovery** to turn off Layer 2 fallback after an iLink threshold recovery.

Zero Power HA (ZPHA) ensures constant, non-interrupted flow of network traffic, even when power is interrupted. If the power is interrupted, the ZPHA module bypasses the IPS device, thus providing continuous network traffic. Choose form the following options on the Zero Power HA panel:

- **Normal** — Core Controller routes traffic to iLink segments for inspection
- **Bypass IPS** — Core Controller 10G segments are physically connected so that network traffic completely bypasses the iLinks and IPS devices. All traffic is permitted.

Tip: You can also access L2FB Auto Recovery options from the 10G segment - iLink map in the Core Controller Configuration wizard.

NMS

The NMS page enables you to configure NMS traps to allow monitoring of the device by a restricted NMS.

Remote syslog

The Remote syslog page enables you to designate a remote syslog server on your network. You can have one or more remote servers.

Note: Designating a remote syslog server does not automatically send notifications to that server. You MUST select the Remote Syslog contact for action sets.

Servers

The Servers page enables you to configure Domain Name Service (DNS) settings. DNS supplies the address or addresses that should be consulted for host name to IP address resolution.

Time settings

Time settings enable you to configure settings that determine how the system tracks time. The TippingPoint 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.

Choose one of the following options:

- **Internal Device Time** — The device uses its internal CMOS clock.
- **Remote SNTP Server** — The device uses an Internet Simple Network Time Protocol (SNTP) server. Provide an address to designate as Primary SNTP Server.

Note: We recommend that you use the SMS as your primary SNTP server. The SMS IP address is displayed at the bottom of the timekeeping panel.

Core controller network configuration

Through the SMS, you can view information about Core Controller 10G segments, 10G ports, and iLinks. You can view and configure the networking and traffic processing of those segments. The Network Configuration screen has the following tab options:

- **Segments** — Provides information for the three segments and allows you to edit associated segment map, view Core Controller segments, and edit port settings for the segments.
- **iLinks** — Provides information for Core Controller iLinks and allows you to edit associated iLink map, view iLink ports, and edit port settings for the iLinks.

This section contains the following topics:

- *Segments* on page 388
- *Link down synchronization* on page 389
- *iLinks* on page 390

Segments

The Segments tab provides the following information about the CoreController10G segments and 10G ports:

- Core Controller 10G Segments
  - Name — Segment name
  - 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
- Core Controller 10 G Ports
  - Port — Port designation
  - Port Enabled — Enabled/disabled status
  - Configured — Speed and duplex configuration

- State — Health status of port
- Qualifiers — Health status information
- Media — Type of media for port

Link down synchronization

The Core Controller continually monitors the link state on the 10GbE segments. When a link state change occurs, the Core Controller enforces the Link Down Synchronization (LDS) mode for the segment. To edit the link-down synchronization for a segment, see *Change link down synchronization* on page 389.

The following LDS modes are available:

- **Hub**: Partner port remains active. This is the default LDS mode.
- **Breaker**: Partner port is also taken down, and both ports must be manually restarted.
- **Wire**: Partner port is also taken down and restarts when the link is re-established.

To change the name or link down synchronization a specific segment, select an entry and click **Edit Segment**. See *Change link down synchronization* on page 389

To change the iLink and segment mapping click **Edit Mapping**.

To edit port settings, select a port entry and click **Edit Port**.

Change link down synchronization

1. On the Devices screen, expand the **All Devices** in the navigation pane.
2. Select a Core Controller and expand the options.
3. Select **Network Configuration** and then select the Segments tab.
4. Select a segment entry from the Core Controller 10G Segments list.
5. Click **Edit Segment**. The configure Core Controller Segment Details wizard displays
6. From the left navigation pane, select **Link Down**.
7. Select the type of synchronization from the drop-down box:
   - **Hub** — When one port of a segment goes down, no action is taken on the other port in the segment.
   - **Breaker** — When one port of a segment goes down, the system disables the other port in the segment. Both ports must be restarted manually.
   - **Wire** — When one port of a segment goes down, the system disables the other port in the segment. When the port that originally went down comes back up, the system automatically restarts the other port.

8. If you select **Break** or **Wire** synchronization, specify the **Wait Time** which is how many seconds the system waits before disabling the other port in the segment.
9. Click **OK**.

iLinks

The iLinks tab provides the following information about the CoreController iLinks and iLink ports:

- Core Controller 10G Segments
  - iLink — iLink name or designation
  - Enabled — Enabled/disabled status
  - State — Health status
  - Qualifiers — Health status information
  - Device — Associated IPS device
  - Device Segment – Associated IPS device segment
  - Port A, Port B — Associated port for the iLink
  - Segment Group — Membership in a segment group
  - Profile
- Core Controller 10 G Ports
  - Port — Port designation
  - Enabled — Enabled/disabled status
  - Autonegotiate
  - Configured — Speed and duplex configuration
  - Negotiated
  - State — Health status of port
  - Qualifiers — Health status information
  - Media — Type of media for port

To change the iLink and segment mapping click **Edit Mapping**. To edit iLink settings, select an iLink entry, and then click **Edit Port**. To edit port settings, select a port entry, and then click **Edit Port**.

Core Controller system health

Through the system health screen for an individual device, you can monitor general system information such as device temperature, memory and HA state.

Note: When first adding a device to the SMS, the charts might not have a full 24-hours of data.

From the left navigation pane, you view the following system-specific information:

- *Core Controller performance* on page 391
- *Core Controller port health* on page 392
- *System log* on page 393
- *Audit log (Core Controller)* on page 393

You can do the following:

- *View log* on page 342 — Details how to view a log.
- *Reset logs* on page 393 — Details how to reset logs.

Core Controller performance

The performance area provides performance data for monitoring and graphing Core Controller packet statistics and information about tier statistics. The screen has the following tabbed views:

- *Performance Data tab* on page 391
- *Tier Statistics tab* on page 392

Performance Data tab

Monitored performance data is displayed in textual and graphical formats The Packet Stats Text section displays the following information:

Entry title	Description
Device	Name of the device.
Total Packets	Total number of packets for the device.
Blocked	Number of blocked packets.
Permitted	Number of permitted packets.
Dropped	Number of dropped packets.
Shunted All	Number of plackets not sent through that are sent back to the network.

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:

- **Packet Stats** — Status of packets inspected by IPS
- **CPU** — How much of the CPU capacity is in use
- Tiers Ratio Graph (A-side)
- Tiers Ratio Graph (B-side)
- Shunt Ratio
- **Max iLink Transmit**

To display current values, click **Refresh**. To view Real-time data, click **Realtime**. See *View realtime graph data* on page 342.

Tier Statistics tab

The tier statistics area provides information on packets and speed as measured in Mbps by tier. This area also displays ratios and utilization for A-side and B-side traffic.

Core Controller port health

The port health area provides a comprehensive tabbed view of Core Controller 10G Ports, iLink port statistics, iLink ports by Core Controller segment, and includes a tab for any unassigned iLink ports. Port information is displayed in text and graphical formats. The graphical display tracks input/output by port and provides information about the following:

- Media
- Line Speed
- Link Status
- Duplex Status

To display current values, click **Refresh**. To edit port details, click the **Edit** button associated with a particular graph.

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**.

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 *Viewing system health* on page 425.

The following table details the system log details:

Heading	Description
ID	The ID of the alert in the log.
Time	The time of the alert added to the log.
Severity Level	The severity level of the alert in the log.
Component	The component affected by the alert or event, such as report, policy, and OAM.
Message	The description of the alert.

Reset logs

To reset a log, see *Reset events/logs* on page 342.

Note: Resetting all logs does not reset the audit log.

Audit log (Core Controller)

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.

The following table details the audit log details:

Heading	Description
ID	An ID number assigned by the device that is used for reference purposes.
Time	The time of the alert added to the log.
Message	The description of the alert.
Access Level	The access level of user causing the alert. Can include SMS for the system, SuperUser, and so on.
Interface	The interface used that generated the alert or event: WEB or SYS.
IP Address	The IP address of the system that generated the alert or event.
Component	The component affected by the alert or event, such as report, policy, and OAM.
Result	The result of the event, such as PASS for successful.
User	The user account causing the alert.

You can do the following:

- *View log* on page 342 — Details how to view a log.
- *Reset events/logs* on page 342 — Details how to reset logs.

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.

Exception rules (Core Controller)

The Core Controller uses exception rules, which are similar to trust filters on the IPS. Traffic that matches an exception rule is not sent to the IPS devices for inspection, but is instead sent back onto the network. You can define up to eight exception rules.

Exception rules are not ordered. No one rule is given precedence over another. When the Core Controller receives traffic, the exception rule engine determines if the traffic matches any defined rule and routes the traffic accordingly.

Using the Exception Rule wizard, you can create new exception rules based on the following parameters:

- Ethernet Type
- IP Protocol
- VLAN value
- MPLS value
- IP protocol
- Source or destination IP address
- Destination port

Note: The Core Controller supports a maximum of eight exception rules.

Create/edit exception rules

1. On the Devices screen, expand the **All Devices** in the navigation pane.
2. Select a Core Controller device and expand the options.
3. Select **Exception Rules**.

   The Flow Management Exception Rules screen displays.
4. Do one of the following:
   - Click **New** to create a new rule.
   - Select an existing rule, and click **Edit**.
5. Specify a **Name** for the exception rule, and select **Enabled**.
6. Click **Next** or select **Protocol** in the wizard navigation pane.
7. Select the Ethernet Type. For IP Protocol, specify the Source/Destination ports and addresses.
8. Click **Next** or select **VLAN and MPLS** in the wizard navigation pane.
9. Do one of the following:
   - To match all frames, select **No VLAN tag or MPLS label checking**.

- To exempt frames from inspection, select the **VLAN** or **MPLS** option and define the value or range of frames.

10. Click **Next** or select **Protection Points** in the wizard navigation pane.
11. Select the incoming ports where the Exception Rule is to be applied.
12. Click **Finish**.

Flow management (Core Controller)

The Core Controller uses flow management methods to manage traffic from the 10GbE segments to the associated iLinks. Flow management guarantees traffic flow affinity, so that all traffic associated with a flow of packets is routed to the same IPS segment. For example, traffic that enters the Core Controller on port A of 10GbE Segment 1 is sent out on Port B of 10GbE Segment 1 after it has been processed by the IPS. More than one iLink must be set up on the Core Controller.

Flow management

The Core Controller applies one of four flow management methods to incoming traffic. These methods are designed to examine IP protocol, source IP addresses, and destination IP addresses and use the information to route the traffic to iLinks. The most suitable flow management method varies depending on your network traffic.

Packet processing

The Core Controller only supports IPv4 traffic. Any non-IPv4 traffic is distributed evenly, across an iLink group. The following tunnel types are supported:

- 802.1q (VLAN), ethType==0x8100
- 802.1ad, ethtype==0x88a8
- ethType==0x9100

Note: Packet frames larger than 1548 bytes are not processed using flow management method. These packets are not sent to the IPS devices and are sent back out onto the network.

This section contains the following topics:

- *Flow management device settings* on page 396
- *Flow management methods* on page 400
- *Flow management rules* on page 405

Flow management device settings

The following flow management global settings apply to all Core Controller segments on the current device:

- **Maximum Frame Size** — Size (in bytes) of the largest packet that will be will processed using a flow management method and then routed to an iLink. All packets exceeding the specified size are delivered directly to the other side of the Core Controller segment without further inspection.
- **Learning Mode** — If enabled, statistics are computed for all flow management methods. The statistics are generated by processing all incoming packet headers. However, the packets are immediately shunted to the other side of the Core Controller segment. They are not passed to any iLinks or IPS devices.

Note: Learning mode should only be enabled to allow the Core Controller to characterize the traffic on your network. The statistics generated will allow you to choose a suitable flow management method. During normal operation, learning mode should be disabled.

Maximum frame size

The maximum packet size is the largest packet that will be processed using a flow management method and then routed to an iLink. Packets that exceed this limit are passed through the Core Controller and not passed to an iLink for inspection. For example, you might wish to configure the Core Controller to pass jumbo frame traffic back onto the network instead of sending it to the IPS. The default is maximum packet size is 1548 bytes.

Learning mode

In learning mode, the Core Controller does not send traffic to the iLinks. The flow management methods are applied to the traffic so that you can view the performance of the flow management methods and evaluate which method works best for your network. After you view the flow management statistics, you can use this information to specify which flow management method that you want to use on particular segments or across all Core Controller segments.

Edit flow management global settings

1. On the Devices screen, expand the **All Devices** in the navigation pane.
2. Select a Core Controller device and expand the options.
3. Select **Flow Management.**
4. In the Flow Management Global Settings screen, specify the **Maximum Frame** size from 64 to 9600 bytes.
5. For Learning Mode:
   - Select this option to evaluate which flow management method to use for your network traffic.
   - Deselect this option after determining the best flow management method for your network traffic.
6. Click **OK**.

Flow management methods

The SMS provides statistical information about flow management methods for each Core Controller segment. After careful evaluation of this information and your network traffic patterns, you can assign the best flow management method. The best flow management method is the one that most evenly distributes traffic among available iLinks and gives a balanced flow. The statistical data is presented in the following formats:

- *Flow Management Methods table* on page 401
- *Flow management method graphs* on page 402

Flow Management Methods table

The Flow Management Methods table lists information about the effectiveness of the methods based on traffic for each Core Controller segment. The SMS calculates an average flow score for each method, calculates the standard deviation, and assigns a flow score rank. You can then use this information to evaluate the best flow management method for your network traffic.

The Core Controller has options to control the time for score computation. You can use a flexible time range for various times intervals in the last 24 hours. The resulting scores and rankings can be used to accurately analyze changes to the Core Controller.

The flow Management Methods table provides the following information:

- **Method** — The number of the flow management method.
- **Ranking** — The assigned rank based on the average flow score with a lower number indicating the better ranking.
- **Average Flow Score** — A measure of iLink traffic based on the previous 24 hours with a lower number indicating the better flow method.
- **Standard Deviation** —The variation in the iLink traffic from the average traffic distribution with a lower number indicating a more balanced flow.
- **Number of Scores** — Number of flow scores used to determine Average Flow Score.
- **Assigned** — An indication of which flow management method is current applied to a Core Controller segment.

Flow management method graphs

The graphs represent a visual display of flow management statistical data for each Core Controller Segment. Each graph plots the flow score based on data for the previous 24 hours. Each point on the graph includes a high and low measure based on the variance of the flow score.

You can perform the following tasks:

- *View variable flow management stats* on page 403
- *Determine the best flow management method* on page 404
- *Reassign flow management methods* on page 405

View variable flow management stats

1. On the Devices screen, expand the **All Devices** in the navigation pane.
2. Select a Core Controller device and expand the options.
3. Select **Flow Management** from the navigation pane and then select the Core Controller Segment tab associated with the segment you want to analyze.
4. Select a time interval from the drop-down list:
    - Last 15 Minutes
    - Last 30 Minutes
    - Last Hour
    - Last 2 Hours
    - Last 4 Hours
    - Last 8 Hours
    - Last 12 Hours
    - Last 24 Hours
5. Specify a **Start Time** and an **End Time.**
6. Pick **Recalculate**.

    The results display in the graphs in the Flow Management Methods area.

Determine the best flow management method

1. On the Devices screen, expand the **All Devices** in the navigation pane.
2. Select a Core Controller device and expand the options.
3. Select **Flow Management** from the navigation pane and then select the Core Controller Segment tab associated with the segment you want to analyze.
4. On the Flow Management Methods table, click the header for **Average Flow Score** to sort the entries. If the lowest scores are close in value, go to the next step. Otherwise, choose the method associated with the lowest score or rank.
5. If the lowest **Average Flow Scores** are close in value, use the **Standard Deviation** values to determine the best method to use. Lower standard deviations represent a more balanced traffic flow. The lowest standard deviation is the best flow management method to use.

Reassign flow management methods

Before you begin, consult *Determine the best flow management method* on page 404.

1. On the Devices screen, expand the **All Devices** in the navigation pane.
2. Select a Core Controller device and expand the options.
3. Select **Flow Management** from the navigation pane and then select the Core Controller Segment tab associated with the segment.
4. Select a flow management method from the table, and then click **Assign**.

Flow management rules

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). For a rule to be valid at least one criteria and one iLink must be selected. The rules display in the Flow Management Rules table.

If no iLinks are available, the CoreController blocks the traffic. If you do not want the traffic to be blocked, you can select the shunt option which allows the traffic to continue without being inspected.

Configuration includes the following:

1. Enable/disable the rule.
2. Select the protocol-related criteria for the rule.
3. Select the iLink where the rule is applied to incoming traffic.
4. Select the order in which the rules are applied.

Configure Core Controller flow management rules

1. On the Devices screen, expand the **All Devices** in the navigation pane.
2. Select a Core Controller device and expand the options.
3. Expand **Flow Management** from the navigation pane, and then select **Rules**.
4. Click **New** to create a new rule or select an existing listing, and then click **Edit** to change an existing rule.
5. Specify a **Name** for the exception rule, and then select **Enabled**.
6. In the Criteria area, configure the following items:
   - Ethernet Type
   - IP Number
   - Click **Next** or select **iLink Selection** from the wizard navigation pane.
7. Select the action to take if no iLinks are available:
   - Block traffic
   - Do not inspect traffic
8. To view the iLinks for a specific segment, select the appropriate segment tab. If you want to view only active iLinks for the segment, select the **Active** check box.
9. From the Available iLinks area, select one or more iLinks, and then use the arrow buttons to move the desired available services to the Selected Services area.
10. Repeat steps 8 and 9 for any other segments.

    Important: After a rule is associated with an iLink, you cannot change the iLink. You must remove the iLink from the flow management rule configuration or delete the rule before making any changes to the associated iLink.

11. Click **Finish**.

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*.

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**.

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* on page 408
2. *Configure the SSL appliance* on page 408
3. *Configure SNMP on the SSL appliance* on page 408

4. *Add the SSL appliance to the SMS* on page 408

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 408.

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

To add the SSL appliance as a new device to be managed by the SMS, follow the same general steps for adding any device to the SMS.

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 409
- *Network configuration* on page 410
- *Event monitoring (SSL appliance)* on page 410
- *System health* on page 411
- *Performance* on page 411
- *Port health* on page 412
- *Traffic* on page 412
- *System log* on page 415

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 411
- *Performance* on page 411
- *Port health* on page 412
- *Traffic* on page 412
- *System log* on page 415

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 412
- *Net tab* on page 412
- *SSL tab* on page 413
- *Switch tab* on page 413

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.

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. See *Download SMS client software* on page 6.

   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. For more information, see *Download SMS client software* on page 6.

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), 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.

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. See *Download SMS client software* on page 6.

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 node count license

The SMS Note Count License panel grants your SMS server authority to manage a specific number of TippingPoint security devices. The SMS product includes a default license key that allows management of up to 25 devices. If you need to manage more than 25 devices, you must purchase a new license and use it to upgrade the key.

Only devices managed by the SMS server count against the license key. If you unmanage or delete a device, it no longer counts against your SMS license. See *Unmanaging or remanaging a device* on page 286.

The SMS Node Count License panel displays the SMS license key as a string of X characters. This panel also indicates the number of devices that the license key allows to be managed and the number of devices the SMS is currently managing.

Upgrade your SMS license key

1. Contact your TippingPoint sales representative to purchase a new license.
2. After you have purchased the new license, TippingPoint will make the license available for you. Ask the representative for specific details.
3. When you have the new license key, click **Upgrade** at the right of the SMS License Key panel.
4. In the SMS License dialog, enter your new license key in the appropriate field, and click **Apply**.

   The information displayed on the SMS Node Count License panel is updated with the details of your new license.

TippingPoint license package

The TippingPoint license package contains customer information about the status and the availability of TippingPoint products and services for licensed devices. If your SMS has TMC connectivity, you can configure the System Preferences to poll for license package updates. See *Security preferences* on page 15.

Important: If you have a transitional license or your SMS is not configured to automatically send inventory listings to the TMC, you must manually create and supply an inventory file. See .

The TippingPoint License Package panel displays the following license information:

- **Status** – Top-level indicator of the status of your license package
- **Version** – License package version
- **Package Timestamp** – Day and time that the current license package was created
- **Notification Settings** – Current notification options for receiving results of the SMS daily check for license 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 package update. See *View license status details* on page 421 and *Import a license package* on page 421.

The SMS runs a daily check for licensed capability expiration and other license package issues. The Notification Settings on the TippingPoint License 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.

Throughput and SSL Inspection licenses

TPS devices running TOS v4.1 support higher throughput licenses. 2200T TPS devices support SSL inspection capabilities.

Use the TMC to update the license package and assign an SSL Inspection or Throughput Upgrade license to a 440T or 2200T device.

If you purchased an SSL Inspection or Throughput Upgrade license when you ordered the device, you must also update the license package and assign the license to the device. You are not required to assign the license that you purchased with the device to that device.

SSL Inspection and Throughput Upgrades are licensed separately. To request a license, contact your sales representative.

For more information, see *Verify the license package* on page 528.

Edit notification settings

1. On the TippingPoint License 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**.

   If you have a transitional license, or if your SMS is not configured to automatically send a device inventory list to the TMC, you must manually create an inventory file and upload it to the TMC.

Import a license package

1. Log on to the TMC at *https://tmc.tippingpoint.com*.
2. From the TMC, select **My Account > License Manager**.
3. Download and save the license package to your local system.

   Note: If this is the first time you have obtained a license package from TMC, you must provide an inventory file to TippingPoint technical support.

4. In the SMS client, open the General screen in the Admin Workspace.
5. On the TippingPoint License Package panel, click **Import**.
6. Select the license package you downloaded, and click **Open**.
7. Click **OK**.

   The SMS client allows you to view license status details and to view licensed capabilities for each device.

View license status details

1. Click **Status Details**.
2. The License Status Details dialog displays license status and information for each managed device.

Details include device name and IP address, next license expiration date, and license status.

3. To view licensed capabilities for an individual device, select a row and click **Details**.

   Licensed Capabilities displays capability, expiration, action, and detailed status information.

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 .

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, SecBlade, 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 290.

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 461.

High Availability (HA)

SMS High Availability (HA) consists of two SMS servers, one designated as the primary server, the other designated as the secondary server. 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 505.

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:

     The SMS certificate key is available on the TMC at **My Account** > **FIPS Certification Package**
     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 *Features* on page 13.

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 *Features* on page 13.

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.

Information	Description
Interface	Network interface, typically shown as primary port or secondary port.
Total In: Bytes	Total number of bytes that have passed into the port.

Information	Description
Total Out: Bytes	Total number of bytes that have passed out of the port.
Total In: Discards	Number of inbound packets discarded, although no errors were detected.
Total Out: Discards	Number of outbound packets discarded, although no errors were detected.
Total In: Errors	Sum of all errors that prevented the final transmission of inbound packets.
Total Out: Errors	Sum of all errors that prevented the final transmission of outbound packets.

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 *Features* on page 13.

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 *Features* on page 13.

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 473.

You can adjust table properties to customize how the SMS client displays system log information. See *Features* on page 13.

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.

Information	Description
Number	System-assigned identification number for reference purposes.
Time	Date and time the operation occurred.
User	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.

Information	Description
Host	Name of the host from which the user operation occurred.
Session ID	Identification number assigned by the server for the login session. You might also see the following session ID numbers: -1 indicates the user is not yet authenticated. 0 or -2 might indicate system actions instead of user actions.
Operation	Description of the action performed by the user.
Status	Result of the operation; valid status is either success or failure.

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 473.

You can adjust table properties to customize how the SMS client displays system log information. See *Features* on page 13.

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 427 and *Export SMS system log entries* on page 427.

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.

Field	Description
Session ID	System-assigned identification number for the login session.
User Name	User name of the account with which the session connection is established.
IP Address	IP address of the system that initiated the session and with which the SMS has an active connection.
Groups	Groups to which the user account is a member. Also specifies the New Resource Group (target creation group for the account).
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, 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 435.

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 428.

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 both 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 430. For more information on configuring CAC Authentication, see
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), and TACACS+ 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.

Setting	Description
IP Address	IP address of the RADIUS server.
Port	Port on the RADIUS server that listens for authentication requests; the default value is 1812.
Authentication Protocol	Authentication method used on the RADIUS server: • PAP • MD5 • PEAP/EAP-MSCHAPv2 To use the PEAP/EAP-MSCHAPv2 protocol, you must first import an X509 certificate for the RADIUS 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. For more information about certificate management, see .

Setting	Description
Secret/Confirm Secret	String used to encrypt and sign packets between RADIUS clients and the RADIUS server, set in the RADIUS client configuration file.
Timeout	Timeout, in seconds, for communication with the RADIUS server; the default value is 3 seconds.

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.

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 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.

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.

Setting	Description
Server Address	IP address or host name of the Active Directory server.
Enable SSL	Select **Using LDAPS** to enable Lightweight Directory Access Protocol (LDAP) over SSL. If enabled, you must also import an Active Directory SSL certificate. See *Configure Active Directory authentication* on page 433.

Setting	Description
Port	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.
Timeout	Timeout, in seconds, for communication with the Active Directory server; the default value is 30 seconds.
Search Base	Top-level distinguished name in the Active Directory hierarchical structure where the authentication request begins.`Example: DC=adomain, DC=example, DC=com`
Admin Name/DN	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.`Example: Administrator@DOMAINNAME`
Admin Password	Active Directory server administrative password.

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 428. 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.

Setting	Description
Authentication Mode	Select one: **Allow only users defined in the SMS to log in** or **Allow AD users to log in with or without an SMS account**. 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.
Authorization Mode	If you configured Authentication Mode to allow only users defined in the SMS to log in, then you can select either of two options: **Use SMS local group mappings** or **Use active directory group mappings**. Otherwise, Authorization Mode uses active directory group mappings.
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: • Reject Authentication • 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. • Accept Authentication – Select an SMS user group to which the user is assigned for authorized access.

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 .

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.

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.

Setting	Description
IP Address / Hostname	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).
Port	Port on the TACACS+ server that listens for authentication requests; the default is port 49.

Setting	Description
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, in 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.

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.

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).

CAC authentication on the SMS	Description
ActivClient software	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.
Certificate management	PKI certificates come from an approved Certificate Authority (CA) and are used to verify and authenticate the card holder. Go to **Admin** > **Certificate Management** > **CA Certificates** to import, replace, and view certificate details.
Personal identifier	The Personal identifier is a 10-digit number used to uniquely identify the card holder. Go to **Admin** > **Authentication and Authorization** > **Authentication** to import, edit, or delete personal identifiers.
CAC authentication	When CAC authentication is enabled on the SMS: • 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. • The SMS will not allow an administrator to designate user accounts to be authenticated locally (local authentication). Go to **Admin** > **Authentication and Authorization** > **Authentication** to select the authentication source that the SMS will use to authenticate users.
Managing user roles and user accounts	The SMS uses capabilities and roles to give users permissions to perform specific actions. Go to **Admin** > **Authentication and Authorization** > **Roles** to set the capabilities for each role. 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). Go to **Edit/Create Role** > **Capabilities** > **Admin** > **SMS Management** > **Access Management** > **Access SMS CLI** to expand or limit this capability.

CAC authentication on the SMS	Description
	When CAC authentication is enabled on the SMS, the Personal Identifier will be required when you create a new user account.

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

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.

Windows operating system	ActivClient version
Windows 7 (32- and 64-bit)	ActivClient 6.2 or ActivClient 7.0.2
Windows 8 (32- and 64-bit)	ActivClient 6.2 or ActivClient 7.0.2

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**.

1. Go to **Admin** > **Authentication and Authorization** > **Authenticaion**.
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 443.

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 445.

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 *Snap shot 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 in the SMS. A *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 428. 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 443 and *Edit a user role* on page 444.
   - 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:

Category	Description
Devices	Select devices (if any) that group members have access permissions to manage.
Segment Groups	Select segment groups (if any) that group members have access permissions to manage.
Profiles	Select profiles (if any) that group members have access permissions to manage.
DV Toolkit Packages	Select DV Toolkit packages that group members have access permissions to manage.
Action Sets	Select action sets that group members have access permissions to manage.
Reports	Select reports that group members have access permissions to manage.

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 445.
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.

Field	Description
Enabled	Indicates whether the user ID is enabled (green checkmark) or disabled (blank).
User Id	Displays the user identifier, which is commonly referred to as *username*. This is the identifier a user provides to log in to the SMS client.
Groups	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.
Password Exp	Displays the settings for password expiration. The system-wide security level affects password requirements.
Name	Displays the name of the contact for the user account, specified in Contact Details.
Email	Displays the email address for the user account, specified in Contact Details.
Local	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+.

Administration of SMS user accounts involves functionality located on this screen as well as other parts of the *Authentication and authorization* on page 428 area. To manage user sessions, see *Managing active sessions* on page 428.

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 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.

Security level	Username requirements
Level 0	A valid user name must: • Differ from existing users by more than capitalization. • Consist of letters, numbers, and non-alphanumeric characters (examples include ! ? $ * #).
Level 1 and Level 2	A valid user name must: • Contain at least 6 characters with a maximum of 150 characters. • Differ from existing users by more than capitalization. • Consist of letters, numbers, and non-alphanumeric characters (examples include ! ? $ * #).

Note: A user name cannot contain spaces.

Security level is system-wide. To view or modify the system-wide settings, select the **Edit** > **Preferences** option from the SMS Client menu bar. See *System preferences* on page 15.

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 preferences* on page 15. We recommend that you use Level 2 security, which enforces the highest level of security for access to the SMS server.

Security levels have the following password requirements:

Security level	Password requirements
Level 0 – Low	A password does NOT have to be defined. If you choose to define a password, any length and format is allowed.
Level 1 – Medium	Passwords must contain at least 8 characters.
Level 2 – High	Passwords must meet Level 1 restrictions and the following: • Must contain at least two alphabetic characters. • Must contain at least one numeric character. • Must contain at least one non-alphanumeric character (examples include ! ? $ * #).

Note: A password cannot contain spaces.

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 428.

The user inherits the access permissions and user role capabilities defined for an assigned group. See *Managing user groups* on page 445.

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:

Field	Description
Enabled	Select **Enabled** to enable this user account when it is created, or clear the check box to create a disabled account.
User Id	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 448.
Password/ Confirm Password	Enter a password for the account that meets security level requirements. See *Table* on page 449. Re-enter the password in the Confirm Password field.
Password Expiration	Select **Enabled** and specify a number of days (1–365) to enable password expiration for the account.
Change password on next login	Select **Change password on next login** to require the user to change the account password on next login.
Authentication	Select **Local Authentication Only** if this SMS user must authenticate using SMS local credentials. See *Authentication source* on page 431.

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 449.

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.

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.

Column	Description
Data	Name of the database data.
Rows	Current number of rows of data in the database.
Max Rows	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.
Age	Number of days to keep data before clearing it. The system clears data older than this setting. You can edit this setting.
Status	Cleanup status.
Last Cleanup	Last time the entries were cleaned. Cleanup occurs daily. You can also initiate an immediate cleanup by clicking **Cleanup Now**.

Column	Description
Events	Filter hits retrieved from managed devices.
Audit Log	Audit log records for the SMS.
Core Controller Flow Management Method Stats	Flow Management Method Stats for managed Core Controllers.
Device Audit Log	Audit log records for managed devices.
Device Monitoring Data	Monitoring statistics for managed devices.

Column	Description
Device SSL Log	SSL inspection log for managed devices.
Device System Log	System log records for managed devices.
Device Traffic Data	Traffic statistics for managed devices.
Firewall Block	X-series firewall block logs.
Firewall Traffic	X-series firewall traffic statistics.
Historical Events	Filter hit-based data for SMS reporting.
Historical DDOS Stats	Device DDOS statistics for SMS reporting.
Historical IP User Mapping	IP user mapping data for SMS reporting.
Historical Port Traffic Stats	Device port traffic statistics for SMS reporting.
Historical Rate Limit Stats	Device rate limit statistics for SMS reporting.
Historical Threshold Stats	Device traffic threshold statistics for SMS reporting.
Network Mapping	Network mapping and IP correlation data for Responder.
IP Address Lookup Results	IP addresses and IP address groups for event IP address lookup.
IP User Mapping	IP user and group mapping.
Next Generation Firewall Profile Snapshots	Profile information for managed NGFW appliances.

Column	Description
Next Generation Firewall Events	Firewall event data from managed NGFW appliances.
Next Generation Firewall VPN Log	VPN logs from managed NGFW appliances.
Notifications	Latest SMS and managed device log notifications.
Profile Change History	Inspection profile version history.
Response History	Response History events for Responder.
sFlow®	sFlow® statistics from managed devices.
SMS Monitoring Data	SMS-specific monitoring data.
Events HTTP Context	URI metadata (i.e., hostname, URI, and Method) from managed devices.
User ID IP Correlation	User log in and group information from the Identity Agent.
VPN	X-series VPN logs.
Segment Traffic Stats	Segment traffic statistics from managed devices.

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 clean up 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*.

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.

Setting	Description
Include... most recent Digital Vaccine(s)	Select the number (1–6) of Digital Vaccines to include in the backup. The most recent Digital Vaccine is always included in a backup.

Setting	Description
Include... most recent Device TOS packages	Select up to the six most recent Device TOS packages to include in the backup.
Include... most recent Custom packages	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.
Include contents of events table	Select this option to include data from the Events table in the backup.
Email the backup results	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 *Server properties* on page 460.
Use timestamp as suffix of the backup file name	Select this option to append the current timestamp to the end of the backup filename.
Encrypt backup	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.

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.

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 463.

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.

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.

Setting	Description
Name	Hostname of the SMS. The name should easily and uniquely identify each SMS system.
Contact	Name or email address of the system administrator responsible for the server.
Location	Location of the server or the administrator.
Serial Number*	Serial number of the server.
Management Port Speed*	Port speed.
Management Port Duplex*	Port duplex setting (full or half).
Management Port Negotiation	Option to enable auto negotiation for the management port.

* 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 423.
   - SMS will not be able to communicate with the Identity Agent. For more information, see *User ID IP Correlation* on page 517
   - 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.

Setting	Description
SSH	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.
HTTPS	Secure network communication for Web pages. Enabling HTTPS enables Web services for the SMS. HTTPS is enabled by default. See *TippingPoint SMS Web Services API*.
HTTP	Unsecure network communication connection for Web pages. Enabling HTTP enables Web services for the SMS. See *TippingPoint SMS Web Services API*.
Telnet	Unsecure network communication connection used for CLI. Requires Super User access.
Ping	Allows the SMS to respond to an ICMP request. Ping is enabled by default.

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.

Setting	Description
Ethernet MAC ID*	Unique identifier assigned by the manufacturer to network interface cards (NICs) capable of supporting the IPv4 standard.
Scope Link Address*	Unique identifier assigned by the manufacturer to network interface cards (NICs) capable of supporting the IPv6 standard.
IP Address	Internet protocol (IP) address of the SMS server used for management communication.
Subnet Mask	Subnet mask of the IP address.
Gateway	Network gateway through which SMS Server traffic flows.
IPv6 Address	IP version 6 address of the SMS Server.
Default Router	IP address of the default router through which SMS Server traffic is routed to/from the network.

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:

Setting	Description
Server Address	IP address or hostname of the SMTP mail server through which the SMS can send email messages.
SMTP Port	Port on the mail server that listens for SMTP requests; this is typically port 25.

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 469.
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. See *IDResolver* on page 29.

The SMS provides built-in User ID IP correlation through the User Resolver feature. See . 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.

To enable and configure IDResolver, see *IDResolver* on page 29.

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 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 473

SMS audit syslog on page 474

Device system syslog on page 474

Device audit syslog on page 475

Snort syslog for MARS [Deprecated] on page 476

Snort syslog for V2 [Deprecated] on page 477

SMS 2.0/2.1 syslog on page 477

SMS 2.5 syslog on page 479

ArcSight CEF Format v3.5 [Deprecated] on page 481

ArcSight CEF Format v4.1 [Deprecated] on page 484

ArcSight CEF Format v4.2 on page 487

The SMS supports *Device audit syslog* on page 475 and *Device system syslog* on page 474 for logging data from managed devices, and supports *Snort syslog for MARS [Deprecated]* on page 476 and *Snort syslog for V2 [Deprecated]* on page 477 for sending Snort syslog events.

SMS system syslog

Column	Definition
0	Severity — 2 is `Info`, 3 is `Warning`, 4 is `Error`, 5 is `Critical`
1	Message
2	Event timestamp in milliseconds

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

Column	Definition
0	User
1	Client address
2	Client port
3	Session ID
4	Status
5	Description
6	Event timestamp in milliseconds

Event sample data

The following is a log message for one event, as it would appear on the syslog:

```
labuser<tab>152.67.137.78<tab>-1<tab>2<tab>success<tab>View SMS System
Log<tab>1169157145027
```

The default settings are TAB for delimiter and Security/Authorization for facility.

Device system syslog

Column	Definition
0	Device name
1	Severity

Column	Definition
2	Component
3	Message
4	Time

Event sample data

The following is a log message for one event, as it would appear on the syslog:

```
110-400<tab>INFO<tab>UDM<tab>Completed UDM Load request (force =
0)<tab>1318265740029
```

Device audit syslog

Column	Definition
0	Device name
1	Access level
2	Interface
3	Source IP address
4	Category
5	Result
6	Device user

Event sample data

The following is a log message for one event, as it would appear on the syslog:

```
110-400<tab>Super
User<tab>WEB<tab>239.142.226.15<tab>SMS<tab>PASS<tab>root00
```

Snort syslog for MARS [Deprecated]

Column	Definition
0	Date (timestamp)
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:

```
Oct 10 11:03:13 snort[19]: [1:0:1] 1766: HTTP: IIS Index Server
File Disclosure [Classification: Misc Attack] [Priority: 3] {http}
211.207.172.50 -> 102.191.115.79
```

Snort syslog for V2 [Deprecated]

Column	Definition
0	Device identifier
1	SID
2	Filter name
3	Classification
4	Priority
5	Protocol
6	Source address
7	–>
8	Destination address

Event sample data

The following is a log message for one event, as it would appear on the syslog:

```
snort[19]: [1:0:1] 2328 HTTP HolaCMS Admin Auth Credential
Exposure [Classification: Misc Attack] [Priority: 3] {HTTP}
220.169.39.148:35548 -> 220.169.39.221:80
```

SMS 2.0/2.1 syslog

Column	Definition
0	Syslog category — "<32>" — defined facility and severity

Column	Definition
1	Action type — 7 is Permit, 8 is Block, 9 is P2P
2	Severity — 0 is Normal, 1 is Low, 2 is Minor, 4 is Critical
3	Policy UUID — TippingPoint UUID for policy
4	Signature UUID — TippingPoint UUID for signature
5	Signature name — user-friendly name for signature and policy
6	Signature number
7	Signature protocol — protocol of signature (IP, UDP, TCP, HTTP, etc.)
8	Source address
9	Source port
10	Destination address
11	Destination port
12	Hit count — number of attacks during aggregation period
13	Device slot — this slot can be 3,5,7,8
14	Device segment — device segment of above slot that got event
15	Device name — user-friendly name of the device event was received
16	TippingPoint Taxonomy ID — category ID assigned to the signature

Column	Definition
17	Event timestamp in milliseconds
18	Additional comments about the event
19	Sequence number of the event in the SMS

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>3<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.

Column	Definition
0	Syslog category — "<32>" — defined facility, and the severity
1	Action type — 7 is Permit, 8 is Block, 9 is P2P
2	Severity — 0 is Normal, 1 is Low, 2 is Minor, 3 is Major, 4 is Critical
3	Policy UUID — TippingPoint UUID for policy
4	Signature UUID — TippingPoint UUID for signature
5	Signature name — user-friendly name for signature and policy

Column	Definition
6	Signature number
7	Signature protocol — protocol of signature (IP, UDP, TCP, HTTP, etc.)
8	Source address
9	Source port
10	Destination address
11	Destination port
12	Hit count
13	Source zone name
14	Destination zone name
15	Incoming physical port
16	VLAN ID
17	Device name — user-friendly name of the device event was received
18	TippingPoint taxonomy ID — category ID assigned to signature
19	Event timestamp in milliseconds
20	Additional comments about the event
21	Sequence number of the event in the SMS

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.

ArcSight CEF Format v3.5 [Deprecated]

Column	CEF key name	Definition
0	CEF	CEF header (Version|Device Vendor|Device Product|Device Version|Signature ID|Name|Severity|)
1	app	Application protocol
2	cnt	Base event count
3	dst	Destination address
4	dpt	Destination port
5	act	Device action
6	cn1	Device custom number 1: VLAN tag
7	cn1Label	Device custom number 1 label
8	cn2	Device custom Number 2: taxonomy ID
9	cn2Label	Device custom number 2 label

Column	CEF key name	Definition
10	cn3	Device custom number 3: packet trace
11	cn3Label	Device custom number 3 label
12	cs1	Device custom string 1: profile name
13	cs1Label	Device custom string 1 label
14	cs2	Device custom string 2: policy UUID
15	cs2Label	Device custom string 2 label
16	cs3	Device custom string 3: signature UUID
17	cs3Label	Device custom string 3 label
18	cs4	Device custom string 4: zone names
19	cs4Label	Device custom string 4 label
20	cs5	Device custom string 5: device name
21	cs5Label	Device custom string 5 label
22	cs6	Device custom String 6: message parameters
23	cs6Label	Device custom string 6 label
24	src	Source address
25	spt	Source port

Column	CEF key name	Definition
26	externalID	External ID (event ID)
27	rt	Event time
28	cat	Device event category
29	proto	Transport protocol
30	deviceInboundInterface	Device inbound interface (physical port in)

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=1318264810021
cat=Exploits
transportProtocol=TCP
deviceInboundInterface=2
```

ArcSight CEF Format v4.1 [Deprecated]

Column	CEF key name	Definition
0	CEF	CEF header (Version|Device Vendor|Device Product|Device Version|Signature ID|Name|Severity|)
1	app	Application protocol
2	cnt	Base event count
3	dst	Destination IPv4 address
4	dpt	Destination port
5	act	Device action
6	cn1	Device custom number 1: VLAN tag
7	cn1Label	Device custom number 1 label
8	cn2	Device custom number 2: taxonomy ID
9	cn2Label	Device custom number 2 label
10	cn3	Device custom number 3: packet trace
11	cn3Label	Device custom number 3 label
12	cs1	Device custom string 1: profile name
13	cs1Label	Device custom string 1 label

Column	CEF key name	Definition
14	cs2	Device custom string 2: policy UUID
15	cs2Label	Device custom string 2 label
16	cs3	Device custom string 3: signature UUID
17	cs3Label	Device custom string 3 label
18	cs4	Device custom string 4: zone names
19	cs4Label	Device custom string 4 label
20	cs5	Device custom string 5: device name
21	cs5Label	Device custom string 5 label
22	cs6	Device custom string 6: message parameters
23	cs6Label	Device custom string 6 label
24	src	Source IPv4 address
25	spt	Source port
26	externalID	External ID (event ID)
27	rt	Event time
28	cat	Device event category
29	proto	Transport protocol

Column	CEF key name	Definition
30	deviceInboundInterface	Device inbound interface (physical port in)
31	c6a2	Source IPv6 address
32	c6a3	Destination IPv6 address
33	request	URI string
34	requestMethod	URI method
35	dhost	URI host

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 Message Parms
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

Column	CEF key name	Definition
0	CEF	CEF header (Version|Device Vendor|Device Product|Device Version|Signature ID|Name|Severity|)
1	app	Application protocol
2	act	Flow control of the filter
3	c6a1	Client IPv6 address
4	c6a1Label	Client IPv6 address field label
5	c6a2	Source IPv6 address
6	c6a2Label	Source IPv6 address field label
7	c6a3	Destination IPv6 address
8	c6a3Label	Destination IPv6 address field label
9	cat	Filter name category
10	cn1	Device custom number 1: VLAN ID
11	cn1Label	Device custom number 1 label
12	cn2	Device custom number 2: taxonomy ID
13	cn2Label	Device custom number 2 label

Column	CEF key name	Definition
14	cn3	Device custom number 3: packet trace
15	cn3Label	Device custom number 3 label
16	cs1	Device custom string 1: profile name
17	cs1Label	Device custom string 1 label
18	cs2	Device custom string 2: profile UUID
19	cs2Label	Device custom string 2 label
20	cs3	Device custom string 3: filter signature UUID
21	cs3Label	Device custom string 3 label
22	cs4	Device custom string 4: zone names (source and destination)
23	cs4Label	Device custom string 4 label
24	cs5	Device custom string 5: device name
25	cs5Label	Device custom string 5 label
26	cs6	Device custom string 6: filter message parameters
27	cs6Label	Device custom string 6 label
28	cnt	Event hit count
29	deviceInboundInterface	Physical port in

Column	CEF key name	Definition
30	dhost	Host name of the URI
31	dntdom	Destination domain name
32	dpt	Destination port
33	dst	Destination IPv4 address
34	duser	Destination username
35	dvchost	Device name
36	externalId	Event ID
37	proto	Network protocol
38	request	URI string
39	requestMethod	URI method
40	rt	Event time stamp
41	sntdom	Source domain name
42	sourceTranslatedAddress	Client IPv4 address
43	spt	Source port
44	src	Source IPv4 address
45	suser	Source user name

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=smsName
cs5Label=Device Name
cs6= cs6Label=Filter Message Parms
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
sourceTranslatedAddress=50.60.222.111
c6a1= c6a1Label=Client
IPv6 suser=userName
sntdom=reptilien-freunde.net
duser=userName
dntdom=reptilien.net
```

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 491. 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.

Field	Description	Type
`actionType`	Action type that is used on the filter that triggered the event. Supported action types include the following: • `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`	Integer
`arcSightFilterName`	Name of the filter that triggered the event	String
`arcSightSeverity`	Severity — `0` is `Normal`, `1` is `Low`, `2` is `Minor`, `3` is `Major`, `4` is `Critical`	Integer

Field	Description	Type
`categoryName`	Name of the filter category	String
`clientAddress`	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. **Note:** This field matches the `srcAddress` field when TCIP/XFF collection is enabled but TCIP/XFF is unavailable for the traffic flow that triggered 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	IPv4 or IPv6 address
`clientAddressv4`	TCIP/ XFF client IP address in IPv4 format (for example, `10.0.0.1`) from HTTP traffic when configured in the profile settings. **Note:** This field matches the `srcAddress` field when TCIP/XFF collection is enabled but TCIP/XFF is unavailable for the traffic flow that triggered 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 • An IPv6 address was captured	IPv4 address
`clientAddressv6`	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.	IPv6 address

Field	Description	Type
	Note: This field matches the `srcAddress` field when TCIP/XFF collection is enabled but TCIP/XFF is unavailable for the traffic flow that triggered 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 • An IPv4 address was captured	
`correlationId`	Session identifier for an event coming from an NGFW appliance. It can be used to correlate all the NGFW events for a single session. **Note:** This field will only be available from NGFW appliances.	Long
`destAddress`	Destination address of the event (for example, `10.0.0.2`)	IPv4 or IPv6 address
`destAddressv4`	Destination IPv4 address (for example, `10.0.0.2`) **Note:** This field will be empty if the `destAddress` is an IPv6 address.	IPv4 address
`destAddressv6`	Destination IPv6 address (for example, `2001:db8:85a3::8a2e:370:7335`) **Note:** This field will be empty if the `destAddress` is an IPv4 address.	IPv6 address
`destPort`	Destination port number	Integer

Field	Description	Type
destUserDomain	Active Directory domain name of the user at the destination IP address (for example, marketing.acme.net) **Note:** In order for this field to display, the Identity Agent must be configured for the SMS.	String
destUserMachine	Computer name for the user at the destination IP address (for example, computername.marketing.acme.net) **Note:** In order for this field to display, the Identity Agent must be configured for the SMS.	String
destUserName	Active Directory logged in username at the destination IP address (for example, johndoe.marketing.acme.net) **Note:** In order for this field to display, the Identity Agent must be configured for the SMS.	String
destZone	Destination zone name (for example, 1-2B) **Note:** This field will only be available from NGFW appliances.	String
deviceName	User-provided name of the device event was received from	String
deviceSegment	Segment on the device where the event occurred (for example, 2)	Integer
deviceSlot	Device Slot (for example, 11)	Integer
deviceTimezone	Device time zone (for example, CST)	String
eventID	SMS event identifier	Long

Field	Description	Type
	Note: In the SMS, this is the **Event No**. field, which is available on the Event Details for Inspection and Firewall events.	
`eventTimestamp`	Event timestamp in milliseconds since epoch (for example, `1445012290091`)	Long
`filterName`	Name of the filter that triggered the event	String
`fiterNameV2`	Name of the filter that triggered the event and contains the same information as the `filterName` field except for the colon (:) and semi-colon (;) punctuation	String
`firewallRuleUUID`	UUID of the Firewall rule that is applied to the traffic (for example, `DEFAULT` will appear for the default block rule) **Note:** This field will only be available from NGFW appliances.	String
`flowControl`	Flow control of the filter (for example, `block` or `permit`)	String
`hitCount`	Number of times this event occurred during aggregation period	Integer
`inInterfaceName`	Inbound interface name **Note:** This field will only be available from NGFW appliances.	String
`inspectionProfileUUID`	Profile UUID (for example, `c6da0827-798b-49ad-85e8-bb8e0ae531b5`) **Note:** This field will only be available from NGFW appliances.	String

Field	Description	Type
`msgParameters`	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|exceeds|1|3`) **Example**: 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)`	String
`outInterfaceName`	Outbound interface name **Note:** This field will only be available from NGFW appliances.	String
`packetTrace`	Packet trace associated with the event — `0` is if there is no packet trace, `1` is if there is a packet trace **Note:** This field will not be available from TPS devices and NGFW appliances.	Boolean
`physicalPortIn`	Physical port in	Integer
`policyUUID`	UUID for the policy (for example, `c6da0827-798b-49ad-85e8-bb8e0ae531b5`) **Note:** You can also use this field in conjunction with the SMS Web Services API.	String
`profileName`	Name of the profile on the device segment/interface where the event occurred	String
`protocol`	Name of the protocol (for example, `HTTP`, `ICMP`, etc.)	String

Field	Description	Type
protocolLower	Name of the protocol in lowercase letters (for example, http, icmp, etc.)	String
severity	Severity — 0 is Normal, 1 is Low, 2 is Minor, 3 is Major, 4 is Critical	Integer
severityType	Text of the severity (for example, Low, Minor, Major, etc.)	String
signatureName	User-friendly name for the filter (for example, 0027: IP Options: Record Route (RR)) **Note:** You can also use this field in conjunction with the SMS Web Services API.	String
signatureNumber	Filter number (for example, 27) **Note:** You can also use this field in conjunction with the SMS Web Services API.	Integer
signatureUUID	UUID for the filter (for example, 0000001-0001-0001-0001-000000000027) **Note:** You can also use this field in conjunction with the SMS Web Services API.	String
smsName	User-provided name of the SMS (hostname)	String
snortClass [deprecated]	Snort Classification (for example, Misc Attack)	String
snortDate [deprecated]	Event timestamp (for example, Oct 16 10:20:35)	Date
snortDestAddress [deprecated]	Destination address and port of the event (for example, 10.0.0.2:1368)	IP address: Port

Field	Description	Type
`snortName` [deprecated]	Name of the filter that triggered the event	String
`snortNameV2` [deprecated]	Name of the filter that triggered the event	String
`snortPriority` [deprecated]	Severity — `0` is `Normal`, `1` is `Low`, `2` is `Minor`, `3` is `Major`, `4` is `Critical`	Integer
`snortProtocol` [deprecated]	Name of the protocol (for example, `HTTP, ICMP`, etc.)	String
`snortProtocolV2` [deprecated]	Name of the protocol (for example, `HTTP, ICMP,` etc.)	String
`snortSid` [deprecated]	Snort rule identifier (for example, `[1:0:1]`)	String
`snortSrcAddress` [deprecated]	Source address and port of the event (for example, `10.0.0.3:80`	IP address: Port
`srcAddress`	Source address of the event (for example, `10.0.0.3`)	IP address
`srcAddressv4`	Source IPv4 address. (for example, `10.0.0.3`). This field will be empty if the `srcAddress` is an IPv6 address.	IPv4 address
`srcAddressv6`	Source IPv6 address (for example, `2001:db8:85a3::8a2e:370:7336`). This field will be empty if the `srcAddress` is an IPv4 address.	IPv6 address
`srcPort`	Source port number	Integer
`srcUserDomain`	Active Directory domain name of the user at the source IP address (for example, `marketing.acme.net`)	String

Field	Description	Type
	Note: In order for this field to display, the Identity Agent must be configured for the SMS.	
`srcUserMachine`	Computer name for the user at the source IP address (for example, `computername.marketing.acme.net`) **Note:** In order for this field to display, the Identity Agent must be configured for the SMS.	String
`srcZone`	Source zone name **Note:** This field will only be available from NGFW appliances.	String
`taxonomyID`	Category ID assigned to the signature	Long
`uriHost`	URI hostname from the HTTP header when HTTP context is configured for the profile and reported by the IPS device (for example, `example.com`)	String
`uriMethod`	HTTP method from the HTTP header when HTTP context is configured for the profile and reported by the IPS device (for example, `GET`)	String
`uriString`	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`)	String (8k limit)
`vlanTag`	Vlan ID	Integer
`Delimiter`	Determines the character the SMS uses as a delimiter for event data in the syslog (`tab`, `comma`, `semi-colon`, or `pipe`)	

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 473
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 491. 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.

Setting	Description
`Syslog Server`	Hostname or IP address of the remote syslog server
`Protocol`	Transport protocol used in sending event notifications to the remote syslog server. Valid options are `UDP`, `TCP`, and `Encrypted TCP`.

Setting	Description
	Note: 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.
`Port`	Port on the remote syslog server used for communicating syslog events.
`Log Type`	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: • **SMS System**: SMS system logging • **SMS Audit**: SMS audit logging • **Device System**: Device system logging • **Device Audit**: Device audit logging • **Snort Syslog (MARS) [Deprecated]**: Send Snort-configured-for-MARS events • **Snort Syslog V2 [Deprecated]**: Send Snort Version 2 events • **SMS 2.0 / 2.1 Syslog Format**: Send SMS v2.0 / 2.1 log events • **SMS 2.5 Syslog Format**: Send SMS v2.5 log events • **ArcSight CEF Format v3.5 [Deprecated]**: Send events to an ArcSight connector (Deprecated – does not support IPv6) • **ArcSight CEF Format v4.1 [Deprecated]**: Send events to an ArcSight connector (Deprecated – adds HTTP context information and IPv6 support) • **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 473 for descriptions and examples of the syslog formats.

Setting	Description
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 .

   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 500 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 500.
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 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 423.

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 596.

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 a two-node, high availability (HA) cluster, increasing availability of the SMS server in case an unexpected event causes the primary SMS server to fail or become inaccessible. The SMS HA cluster consists of two SMS servers, one designated as the active (primary) SMS server, the other designated as the passive (secondary) SMS server.

During initial HA configuration, the SMS cluster performs a synchronization of the database from the active server to the passive server. To keep the passive server current, the active SMS replicates critical SMS data to the passive server, 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.

The most important aspects of the SMS HA cluster are the heartbeat connection and database replication. Periodically, you should verify that both activities are performing as expected.

Compatibility requirements

The active and passive SMS servers must meet the following compatibility requirements to configure the HA cluster:

- **Version number** – both systems must be running the same version number (including patch number).
- **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 primary SMS cannot be running a 1K key and the secondary SMS be running a 2K key. 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.

Bandwidth requirements

The SMS has replication bandwidth requirements for heartbeat, digital vaccine (DV) and upgrade package download, and event traffic.

- Less than 10 Kb/s bandwidth is required for heartbeat and system usage/administration operations, such as policy management.
- A minimum of 1 Mb/s 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 Mb/s keeps the two systems reasonably synchronized. See *Software updates* on page 19.
- Event traffic requires approximately 1.5 Mb/s per 1,000 events/second. See *Events* on page 41.

Best practices

When configuring the HA cluster, we recommend that both SMS systems be the same model and have similar disk memory and disk space.

Deactivate the active SMS server

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. See *Swap HA cluster nodes* on page 510.
- **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. See *Invoke failover to activate a passive SMS* on page 510.

Configuring an SMS HA cluster

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.

Cluster Status and Replication Delay metrics are displayed in graphs to help you track the status of the SMS HA cluster. The Replication Delay metrics show how many seconds the passive SMS is behind the active SMS in data replication.

Configure an SMS HA cluster

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 sever 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 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.

Synchronize the SMS HA cluster

1. On the HA Cluster Status panel, click **Synchronize**.
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.

Disable the SMS HA cluster

1. On the HA Cluster Status panel, click **Disable**.
2. Ensure one of the SMS servers is rendered inaccessible to SMS clients and devices.

   When disabled, the two nodes of the SMS HA cluster now act independently. You must ensure one of the SMS servers is inaccessible so that the two servers do not compete with each other. The best way to do this is to power down one of the servers.

Adjust HA timeout values

The cluster uses a heartbeat to communicate operating status to each other. When the cluster is operating in a normal state, the passive (secondary) SMS periodically sends a heartbeat signal to the active (primary) SMS at a rate of once a minute. If the active SMS responds, the cluster operates as usual. If the active SMS fails to respond within three consecutive pings, or if another health check failure is detected, the passive SMS makes a few more attempts to communicate with the active SMS before initiating a failover process.

When you initially configure the cluster, you set the total heartbeat timeout and the mitigation timeout values. See *Configuring an SMS HA cluster* on page 506.

After the high availability feature is configured, you can adjust the timeout values. For example, if the passive and active 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. On the HA Cluster Status panel, click **Timeouts**.
2. In the dialog box, adjust the total heartbeat and mitigation timeout values as needed.

Viewing active and passive SMS details

The Active SMS and Passive SMS panels display the following details for active and passive SMS servers:

- System name
- Status

- Maintenance IP address
- Heartbeat IP address

Swap HA cluster nodes

1. On the Admin (High Availability) screen, click **Swap**.
2. Click **OK** to start the swap process.

   During this process the passive SMS server is promoted to active status and the active server is re-configured to the role of passive SMS server.

   This process can take several minutes, during which time the cluster is re-synchronized, nodes are restarted, and the client is temporarily disconnected to reestablish the 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 failover to activate a passive SMS

This task describes how to activate a passive SMS server and immediately begin using it as the active SMS server. This action is useful when you need to perform maintenance tasks on the active node. To return the failed-over node to active status, you must manually re-synchronize and restart the server.

1. On the Admin (High Availability) screen, click **Failover**.
2. Select **OK** to invoke failover, and then activate the passive SMS server.

   The active server fails over to the passive server, which now becomes your active server. You can power off the deactivated server and perform maintenance.

   To reactivate your passive server and reinstate your cluster to a fully functioning high-availability state, you must bring the deactivated server back online, synchronize the cluster databases and restart the server. See *Synchronize the SMS HA cluster* on page 508.

Named resources

The SMS server uses named resources to assist grouping and unique identification of resources referred to by various features in SMS. Named resources are similar to aliases, and named resource groups are similar to groups of aliases, such as an email distribution list. SMS supports, and in some cases requires the creation of, named IP addresses, VLAN IDs, and email addresses.

For example, when an SMS server is configured to deliver SMTP messages, the recipient list is required to be a Named Email Address Group. 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.

The SMS client references or requires one or more of these named resource types in each of the following areas:

- **Devices** — Exception Rules, Servers, Management Routes
- **Events** — IPS Events (Source and Destination Addresses)
- **Profiles** — Restrictions and Exceptions (Source and Destination Addresses)
- **Active Response** — Policies (Inclusions and Exclusions)

You must have superuser access to create a named resource; both Superuser and Admin users can view named resources. Users logging in with the Operator role have no access to named resources.

SMS uses three types of resources: unnamed, named, and permanent. See the following table for information about each.

Locked Resource	Description	User Capabilities
Unnamed resources	Created automatically from user input and used for auto complete.	Edit: No Delete: Yes
Named resources	Created by the user.	Edit: Yes Delete: Yes
Permanent resources	Created by the SMS and not by the user.	Edit: No Delete: No

In the Admin workspace, select **Named Resources** in the navigation pane to display the Admin (Server Properties) screen. Three tabs comprise this screen: Named IP Addresses, Named VLAN IDs, and Named Email Addresses.

Note: Named resources are used only in 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.

Create, edit, and delete named resource groups

Named resource groups are used to simplify assigning actions, notifications, and so on to multiple resources.

Create a new named resource group

1. Select the tab representing the named resource group you want to create **Named IP Addresses**, **Named VLAN IDs**, or **Named Email Addresses**.
2. In the Named Resource Groups area, click **New**. The Create Named Resource Group dialog box appears.

At the top is a field in which you enter the name of the group, and following that are two list boxes. The left one identifies resources available for inclusion in a group. The right one identifies resources you've selected to include in the group.

3. In the dialog, assign a Name to uniquely identify the group.
4. Use the arrows between the two list boxes to move resources. To include a name resource into the group, select it in the left (Available) list box, then click the right arrow to move it to the right (Selected) list box.

   Note: If no entries exist in the left (Available) list box, then no named resources of this type have been defined. Click **New** to define an individual named resource, or alternatively quit creating a new group and instead create the individual named resources until you've defined the ones you want to include in a named resource group. See *Define a new named resource* on page 514.

5. When you have moved all named resources into the Select Named Resource list box on the right, click **OK** to save the new Named Resource Group.

Show users of an existing named resource group

1. Select the tab representing the named resource group whose users you want to view either **Named IP Addresses**, **Named VLAN IDs**, or **Named Email Addresses**.
2. To view which SMS entities(Active Response policies, Profile exceptions, or Event notifications), use a specific named resource group, select the named resource group in the table, and then click **Show Users**.

Edit a new named resource group

1. Select the tab representing the named resource group you want to edit either **Named IP Addresses**, **Named VLAN IDs**, or **Named Email Addresses**.
2. In the table, select the named resource group you want to edit, and then click **Edit**. Alternatively, you can right-click the named resource group, and then select **Edit** from the drop-down menu.
3. Make the desired modifications, and then click **OK**.

Save As a named resource group

1. Select the tab representing the named resource group you want to duplicate either **Named IP Addresses**, **Named VLAN IDs**, or **Named Email Addresses**.
2. In the table, select the named resource group you want to duplicate, and then click **Save As**.
3. As desired, modify the name of the duplicated names resource group, modify the members of the group, and then save it.

Delete a named resource group

1. Select the tab representing the named resource group you want to delete either **Named IP Addresses**, **Named VLAN IDs**, or **Named Email Addresses**.

2. In the table, select the named resource group you want to delete, and then click **Delete**. Alternatively, you can right-click the named resource group and select **Delete** from the drop-down menu.
3. Click **Yes**.

Create, edit, and delete named resources

A named resource is an individual resource, typically created to be included in a named resource group.

Import a list of named resources from a file

1. Select the tab representing the named resource you want to import either **Named IP Addresses**, **Named VLAN IDs**, or **Named Email Addresses**.
2. In the Named Resource area, click **Import**.
3. Browse to locate the file whose contents you want to import. The file must be text (.txt) file or a comma-separate value (.csv) file. The imported values must not contain spaces in the names, and the file must not contain a header row.
4. Select the file, and then click **Open**. If the file format is valid, the Finish button is enabled.
5. Click **Finish**.

Export a list of named resources to a file

1. Select the tab representing the named resource you want to export either **Named IP Addresses**, **Named VLAN IDs**, or **Named Email Addresses**.
2. In the Named Resource area, click **Export**.
3. Browse to the directory in which you want to save the file, enter a filename, and then click **Save**.

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.

   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**.

Define a new named resource

1. Select the tab representing the named resource you want to define either **Named IP Addresses**, **Named VLAN IDs**, or **Named Email Addresses**.
2. In the Named Resource area, click **New**.

   The Create Named Resource dialog box appears.
3. In the dialog box, assign a Name to uniquely identify the named resource.
4. Enter the requested information, such as IP host, subnet, or range, when defining a named IP address, or VLAN ID or VLAN ID range when defining a named VLAN ID, or an email address when defining a named email address.
5. Click **OK**.

Show users of a named resource

1. Select the tab representing the named resource whose users you want to view either **Named IP Addresses**, **Named VLAN IDs**, or **Named Email Addresses**.
2. To view SMS entities (Active Response policies, Profile exceptions, or Event notifications), use a specific named resource, select the named resource in the table, and then click **Show Users**.

Edit a named resource

1. Select the tab representing the named resource you want to edit either **Named IP Addresses**, **Named VLAN IDs**, or **Named Email Addresses**.
2. In the table, select the named resource you want to edit, and then click **Edit**. Alternatively, you can right-click the named resource, and then select **Edit** from the drop-down menu.
3. Make the desired modifications, and then click **OK**.

Delete a named resource

1. Select the tab representing the named resource you want to delete; either **Named IP Addresses**, **Named VLAN IDs**, or **Named Email Addresses**.
2. In the table, select the named resource you want to delete, and then click **Delete**. Alternatively, you can right-click the named resource, and then select **Delete** from the drop-down menu.
3. Click **Yes**.

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.

Column	Description
Order	Order of priority.
Icon	Icon that distinguishes the event when viewed.
Name	Name or identifier of the IP address group.
Address(es)	Addresses included in the IP address group; an asterisk (*) indicates all addresses.

Column	Description
Geo	Indicates whether Geo Locator lookup service is enabled for the address group.
NR	Indicates whether Named Resources lookup service is enabled for the address group.
DNS	Indicates whether DNS lookup service is enabled for the address group.
User ID	Indicates whether User ID lookup service is enabled for the address group.
Rep	Indicates whether reputation filter lookup service is enabled for the address group.
End Point	Indicates whether End Point Attributes lookup service is enabled for the address group.

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:
      - Host/Subnet/Range – add one or more IP addresses, subnets, or ranges.
      - Named IP Address Groups – select one or more named IP address groups.
      - 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 24.
7. Click **Finish**.
8. Click **OK**.

Note: You can access all the IP Lookup services from the Tools menu. See *Tools* on page 24. 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. The 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 461.

Polling times

The following table defines the polling times for the security login events and metadata and diagnostics.

Item	Polling time
Security login events	Every 4-5 seconds
Metadata and diagnostics	Every 15 minutes

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 451.

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 518.
2. *Create an Agent Group* on page 519.
3. *Select an Identity Agent to be in a group* on page 519.
4. *Enable the Agent Group* on page 520 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.

Column	Description
Time	Specifies the date and time that the event was retrieved by the SMS.
IP Address	Specifies the IP address of the security login event.
User Name	Specifies the user name.
Domain	Specifies the user domains.
Machine	Specifies the user machines.
Member of Groups	Specifies all of the groups for the user.

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 451.

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.

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.

The Geo Locator Database screen displays the following information:

- **Type** — Type of database file; for example, "Signed Geo Locator DB."
- **Date** — Date and timestamp of the current database file.
- **Version** — Version number of the current database file.

To display the Geo Locator Database screen, click **Geo Locator Database** in the Admin navigation pane.

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: SMS versions 3.3 and 3.5 require database files with a file extension of `.dat`. These files must be downloaded directly from MaxMind and extracted prior to importing. You can download the GeoLite City database in Gzip format from MaxMind Development GeoIP Products at *http://dev.maxmind.com/geoip/*.

Download a Geo Locator database file from the TMC

1. Log on to the TMC at *https://tmc.tippingpoint.com*.
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

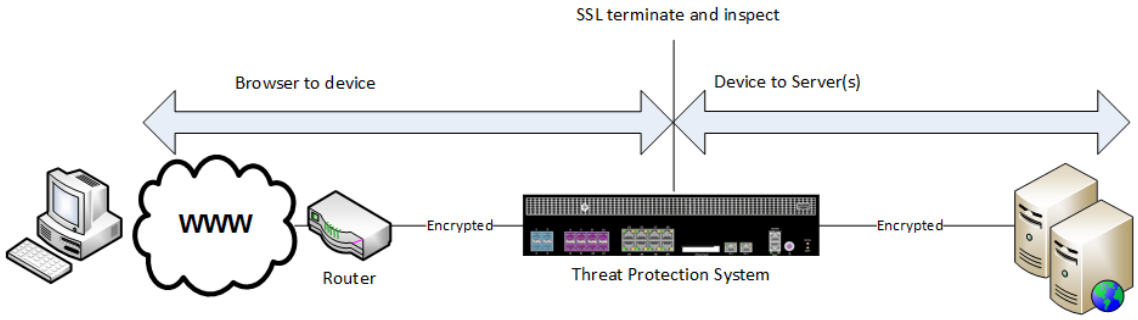
1. On the Geo Locator Database screen, click **Import**.
2. In the dialog, locate the database file you downloaded (valid file extensions are **.pkg** or **.dat**).
3. Select the file, and click **OK**.
4. In the Import Completed dialog, click **OK**.

   The Lookup button on the Geo Locator Database screen enables you to open the IP Lookup utility from this screen. See *IP Lookup* on page 24.

SSL Inspection

Overview

The TippingPoint Threat Protection System (TPS) 2200T provides in-line, real-time threat protection for inbound SSL traffic. The 2200T 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 reverse proxy that receives and decrypts SSL data, inspects it 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:

Consideration	Description
Perfect Forward Secrecy (PFS)	SSL Inspection extends key exchange support to Ephemeral Elliptic Curve Diffie-Hellman with RSA signatures (ECDHE-RSA). ECDHE-RSA enables PFS support for inspection of encrypted SSL sessions.
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

Consideration	Description
	SSL inspection does not include support for GTP or IPv6 encapsulations. * GRE support includes the mandatory GRE fields. We also support optional GRE key configuration, but the key needs to be the same value for both directions. We do not support other optional GRE fields, such as GRE sequence number.
Quarantine hosts and redirecting HTTP traffic to another site	The 2200T TPS does not redirect SSL sessions on a quarantined host. When configuring an Action Set to **quarantine hosts**, if you also configure the response to **redirect HTTP traffic to a web site**, the host of HTTPS traffic is quarantined, but not redirected.
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, and RepDV filtering against the encrypted traffic.
Trust as an Action	If traffic management trust is selected, then SSL inspection is bypassed. If a filter hits a trust, then IPS and reputation inspection stop, but the TPS continues to proxy the SSL session between the client and the server.
Packet trace	Packet Trace as an action includes the decrypted traffic.

Consideration	Description
Traffic capture	Traffic capture by tcpdump does not include the decrypted contents.
L2FB/ZPHA	When the 2200T TPS enters Layer 2 Fallback (L2FB) or Zero Power High Availability (ZPHA), the proxied SSL sessions are cleared.

Requirements

Make sure your environment meets the following requirements:

- TippingPoint 2200T with SSL Inspection Upgrade license. SSL inspection is not supported on the TippingPoint 440T.
- Inbound IPv4 traffic only.
  - SSL inspection does not support IPv6, including IPv4 over IPv6 tunneling.
  - SSL inspection of outbound IPv4 traffic and IPv6 traffic is not supported.
- VLAN translation cannot be used in conjunction with SSL inspection.
- SSL certificate and private key from the server that hosts the SSL/TLS compliant application.
- Cipher suite support:
  - 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)

    Note: TLS Heartbeat Extension (*https://tools.ietf.org/html/rfc6520*) is not supported.
  - Key exchange:
    - Ephemeral Elliptic Curve Diffie-Hellman with RSA signatures (ECDHE-RSA) (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)
  - RC4 (disabled by default)
- MAC:
  - SHA384 (enabled by default)
  - SHA256 (enabled by default)
  - SHA1 (enabled by default)
  - MD5 (disabled by default)

Manage SSL inspection from the SMS

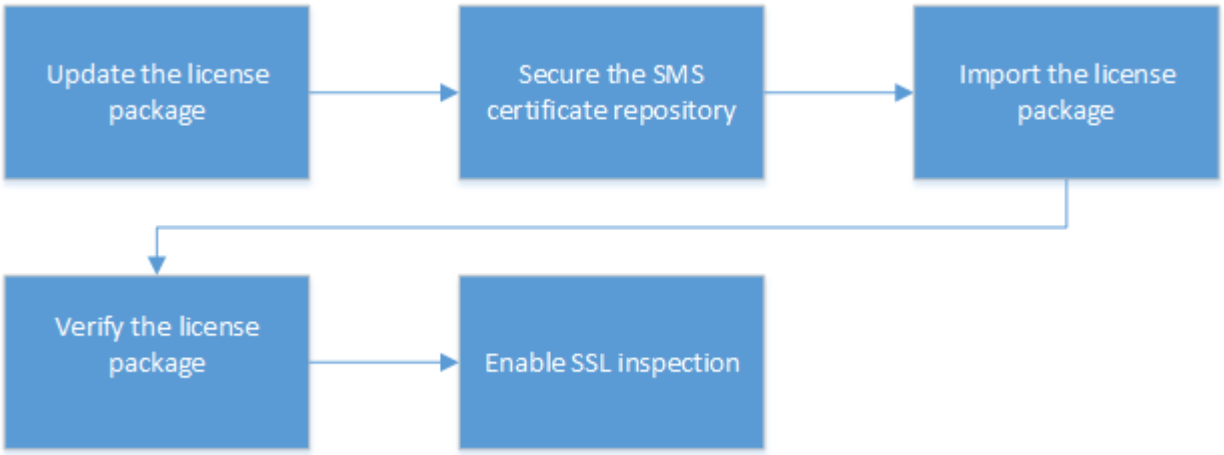
See the following sections for information about setting up and managing SSL inspection from the SMS.

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. Unlike other licensed features, you must reboot the TPS to enable the SSL inspection license.

The process for enabling SSL inspection is described below:



1. *Update the license package on TMC* on page 527.
2. *Secure the SMS certificate repository* on page 527.
3. *Import the license package* on page 528.
4. *Verify the license package* on page 528.
5. *Enable SSL inspection* on page 528.

Update the license package on TMC

Use the TMC to update the license package and assign an SSL inspection license to a 2200T device.

If you purchased an SSL inspection license when you ordered the device, you must also update the license package and assign the SSL inspection license to the device. You are not required to assign the SSL inspection license that you purchased with the device to that device. However, an SSL inspection license is only applicable to a 2200T device.

SSL inspection is licensed separately. To request a SSL Inspection Upgrade, contact your sales representative.

1. Log in to the TMC at: *https://tmc.tippingpoint.com/TMC/*
2. From the TMC, select **My Account > License Manager**.
3. Assign the SSL Inspection license to the 2200T device.
4. Click **Submit** to request an updated license package.

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. You must provide a password for the SMS certificate repository in order to import certificates with private keys into the SMS.

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.

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.

Import the license package

If the SMS is configured to automatically download the updated license package, you may skip this step.

1. Log on to the TMC at *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.

   Note: If this is the first time you have obtained a license package from TMC, you must provide an inventory file to TippingPoint technical support.

4. In the SMS client, open the General screen in the Admin Workspace.
5. On the TippingPoint License Package panel, click **Import**.
6. Select the license package you downloaded, and click **Open**.
7. Click **OK**.

   The SMS client allows you to view license status details and to view licensed capabilities for each device.

Verify the license package

Verify the SSL inspection license upgrade is installed on each 2200T that you want to perform SSL inspection. To complete the SSL inspection license upgrade, you must also reboot the device.

1. In the SMS client, open the General screen in the Admin Workspace.
2. On the TippingPoint License Package panel, click **Status Details**.
3. The License Status Details dialog displays license status and information for each managed device.

   Details include device name and IP address, next license expiration date, and license status.

4. To view licensed capabilities for an individual device, select a row and click **Details**.

   Licensed Capabilities displays capability, expiration, action, and detailed status 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.

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**.

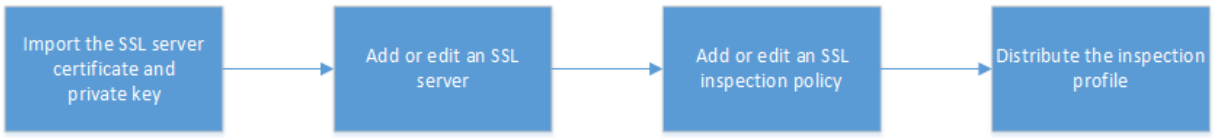
   The Supported SSL Ciphers dialog box is displayed.

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 allows SSL inspection.
   - **Persist Private Keys**. Select this check box to store private keys for SSL server certificates on the TPS device. If this is unchecked then those keys will not be persisted on the device so after every reboot the device will automatically retrieve the private keys from the SMS

Configure SSL inspection

Configure SSL inspection to specify the SSL sessions you want the 2200T to inspect. The 2200T does not inspect SSL sessions that do not match the SSL inspection profile. The process for setting up SSL inspection is described below:



To set up SSL inspection:

1. *Import the SSL server certificate and private key* on page 529.
2. *SSL servers* on page 530.
3. *Add or edit an SSL inspection policy* on page 531.
4. *Distribute the inspection profile* on page 532.

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 temporarily persist its 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. We recommend using a naming convention 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)**.
6. When selecting:
   - **PEM/DER** format, the private key must be imported in a separate file. Be sure to select the **Include a Private Key** checkbox, 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.
7. Click **OK**.

   The appliance imports the certificate and associated private key, and the certificate is displayed in the Device Certificates table.

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

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`. We recommend naming 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 2200T to write log information about SSL inspection to the external log disk (external Cfast). 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 2200T 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 533.
- **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 2200T blocks an SSL session. This option overrides the TCP reset action set, if enabled, on a DV filter. We recommend that you 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**. You are now ready to assign the SSL Server to an SSL inspection policy.

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.

Add or edit an 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 named IP address groups of client IP exceptions. Assign the SSL inspection policy to the inspection profile that carries the traffic of interest.

Tip: To view a summary of the existing SSL server policies, select **Profiles** > **Inspection Profiles** > **[profile name]** > **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 panel, click **Add** or **Edit**.

   The SSL Profile Editor opens.
4. Enter the SSL profile name, for example, myapp_SSLprofile.
5. Under Server Policies, click **Add**.

   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 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 SSL inspection profile to the appropriate inspection segments on the corresponding 2200T device or devices.

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 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.

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 2200T 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. 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.

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.
- 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 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 replacing certificate is 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.
- 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**.
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.
3. (Optional) Provide a password to encrypt the private key.
4. 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.

Give permissions for SSL inspection

From the SMS, give role-based permissions for SSL inspection. By default, SSL inspection permissions are given to the Administrator role.

Give 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.

1. Select **Admin > Authentication and Authorization > Roles.**
2. 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.
3. In the Role dialog box, click the **Capabilities** property sheet.
4. 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**.
5. Click **OK**.

Give access to SSL servers

When managed by the SMS, you can give group access to the SSL servers that you have defined as part of your SSL inspection configuration. By default, a group has access to all SSL servers, including new SSL servers that have yet to be defined. See the following section for more information.

1. Select **Admin > Authentication and Authorization > Groups.**
2. Click **New** to create a group or **Edit** to change an existing group.
3. In the Group dialog box, click the **SSL Servers** property sheet.
4. Check or uncheck the SSL servers to which the group has access.
5. Click the **Profiles** property sheet.
6. Check or uncheck the SSL inspection profiles to which the group has access.
7. Click **OK**.

Manage SSL inspection from the LSM

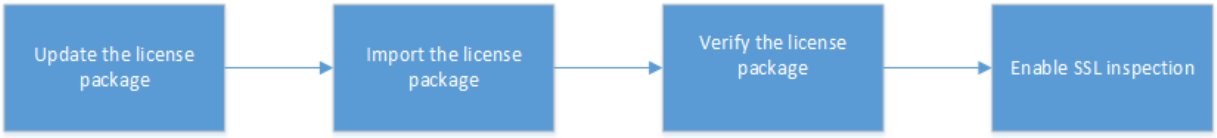
See the following sections for information about setting up and managing SSL inspection from the 2200T LSM.

Before you configure SSL inspection

Before you configure SSL inspection, update the device settings for SSL inspection.

Important: To inspect SSL sessions, the device must be licensed for SSL inspection. Unlike other licensed features, you must reboot the 2200T to enable the SSL inspection license.

The process for enabling SSL inspection is described below:



1. *Update the license package on TMC* on page 536.
2. *Import the license package* on page 536.
3. *Verify the license package* on page 537.
4. *Enable SSL inspection* on page 537.

Update the license package on TMC

Use the TMC to update the license package and assign an SSL inspection license to a 2200T device.

If you purchased an SSL inspection license when you ordered the device, you must also update the license package and assign the SSL inspection license to the device. You are not required to assign the SSL inspection license that you purchased with the device to that device. However, an SSL inspection license is only applicable to a 2200T device.

SSL inspection is licensed separately. To request a SSL Inspection Upgrade, contact your sales representative.

1. Log in to the TMC at: *https://tmc.tippingpoint.com/TMC/*
2. From the TMC, select **My Account > License Manager**.
3. Assign the SSL Inspection license to the 2200T device.
4. Click **Submit** to request an updated license package.

Import the license package

On the 2200T, use the LSM to import an updated license package that gives SSL inspection to the device. To complete the installation, reboot the device.

1. Log on to the TMC at *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.

   When the download completes, log out of the TMC.

   Note: If this is the first time you have obtained a license package from TMC, you must provide an inventory file to TippingPoint technical support.
4. Log in to the LSM on the 2200T device where you want to import the license package.
5. From the LSM menu bar, select **System > Update > System, DV, Licenses**.
6. In the License Version panel, click **Install**.
7. In the Install License Package dialog, click **Browse** to select the package you downloaded from the TMC.

8. Click **Install**.

   You are prompted to reboot the device to apply changes. If necessary, save any uncommitted changes to the Running configuration and save them to the Startup configuration before you reboot the device.

Verify the license package

Verify the SSL inspection license upgrade is installed on the 2200T. To complete the SSL inspection license upgrade, you must also reboot the device.

1. From the 2200T LSM menu bar, select **System > Update > System, DV, Licenses**.
2. In the License Version panel, browse the list of licenses and validate that the SSL Inspection feature has a Permit status of **Allow**.

   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 TMC* on page 536 for more information.

Enable SSL inspection

From the LSM, 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 LSM banner displays a notification.

1. Select **Policy > SSL Inspection**.

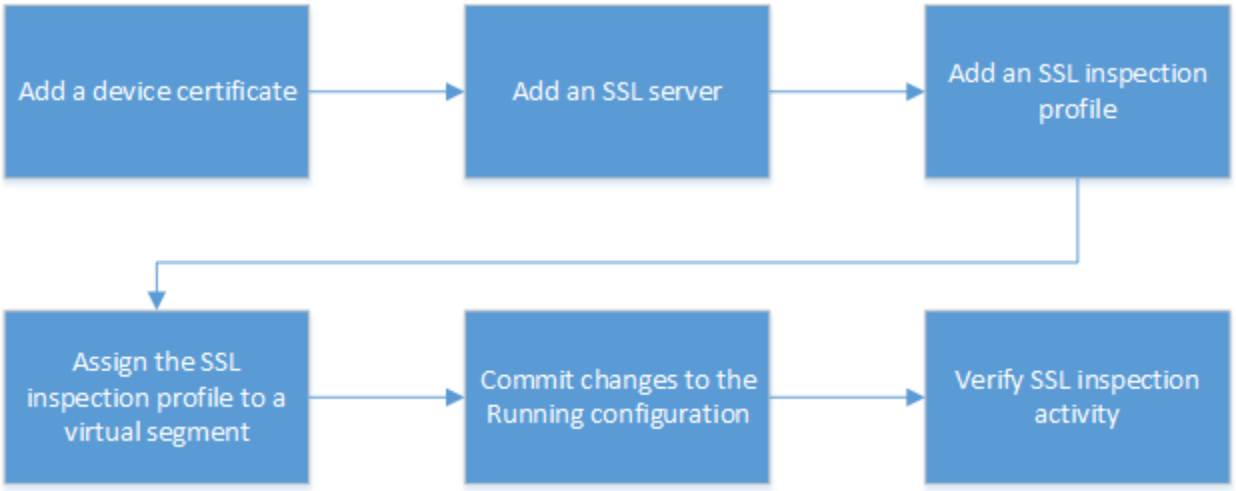
   The SSL Inspection Profiles panel opens.

2. Select **Enable SSL Inspection**.

   If the **Enable SSL Inspection** checkbox is grayed, verify the license package allows SSL inspection.

Configure SSL inspection

Configure SSL inspection to specify the SSL sessions you want the 2200T to inspect. The 2200T does not inspect SSL sessions that do not match the SSL inspection profile. Configuring SSL inspection is a deferred commit operation. After you complete your configuration, commit your changes. The process for setting up SSL inspection is described below:



To set up SSL inspection:

1. *Import the SSL server certificate and private key* on page 538.
2. *Add or edit an SSL server* on page 539.
3. *Add or edit an SSL inspection profile* on page 540.
4. *Assign the SSL inspection profile to a virtual segment* on page 541.
5. *Commit changes to the Running configuration* on page 542.
6. *Verify SSL inspection activity* on page 542.

Import the SSL server certificate and private key

From the LSM, add or edit a device certificate to import both the SSL certificate and private key from the server of interest. To commit changes to the TPS, you must import both the SSL certificate and its private key. The TPS does not attempt to validate the status of a device certificate.

1. Select **Authentication > X.509 Certificates > Device Certificates**.
2. In the Device Certificate 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. We recommend using a naming convention 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)**.
6. When selecting:

- **PEM** format, the private key must be imported in a separate file. Be sure to select the **Include a Private Key** checkbox, 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. Note that only one certificate/private key pair will be imported, along with all of the CA certificates contained in the file.

7. 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 LSM, add an SSL server to specify the SSL server configuration to proxy, 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. DV filters are applied to the incoming traffic, but are not applied 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.

1. Select **Policy > SSL Inspection > Servers**.
2. In the SSL Servers panel, click **Add** or **Edit**.

   The Edit SSL Server dialog box displays.

3. In the **SSL Server Config** tab, specify the following settings:
   - **Name -** Enter the server name, for example, `myapp_pop3`. We recommend naming the server so that you easily associate it with your web server.
   - **Server Certificate:** Select the SSL certificate for your web server. **Note:** The LSM does not validate the server certificate.
   - **Server Addresses:** Specify the server IPv4 address or CIDR range.
   - **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**.
   - **SSL 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`.

- **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 log disk (external Cfast). 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 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 542.
- **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. We recommend that you 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**. You are now ready to assign the SSL server to an SSL inspection profile.

Add or edit an SSL inspection profile

From the LSM, add or edit an SSL inspection profile to specify the SSL traffic that you want to protect. An SSL inspection profile is a set of server policies, each of which specifies an SSL server and a list of client IP exceptions. Assign the SSL inspection profile to the virtual segment that carries the traffic of interest.

1. Select **Policy > SSL Inspection > Profiles**.
2. In the SSL Inspection panel, click **Add** or **Edit**.

   The SSL Profile Editor opens.

3. Enter the SSL profile name, for example, myapp_SSLprofile.
4. Under Server Policies, click **Add**.

   The Add SSL Server Policy dialog box opens.

5. 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 client IP addresses to exclude from SSL inspection.

6. Click **OK**.

   You are now ready to assign the SSL inspection profile to a virtual segment.

Assign the SSL inspection profile to a virtual segment

From the LSM, assign the SSL inspection profile to the appropriate virtual segments on the 2200T device.

1. From the LSM menu, click **Network > Virtual Segments**.
2. Click **Add** or **Insert** to create a new virtual segment, or click **Edit** to edit an existing virtual segment. Virtual segments that are created by the system can have their profiles modified but are otherwise read-only.
   - Clicking **Add** adds the new virtual segment after all the other user-created virtual segments.
   - Clicking **Insert** inserts the new virtual segment just before the currently selected virtual segment.
   - All system-created virtual segments always appear at the end of the list.
3. In the Add Virtual Segment dialog or Edit Virtual Segment dialog, specify the following:
   - Name – (Required) Name used to identify the virtual segment. Each virtual segment must have a unique name.
   - Description – An optional parameter to provide more detailed information about the virtual segment.
   - IPS Profile – Security profile that you want to apply to the virtual segment. A virtual segment can have only one IPS profile applied to it.
   - Reputation Profile – Reputation profile that you want to apply to the virtual segment. A virtual segment can have only one Reputation profile applied to it.
   - Traffic Management Profile – Traffic Management profile that you want to apply to the virtual segment. A virtual segment can have only one Traffic Management profile applied to it.
   - SSL Inspection Profile – SSL inspection profile that you want to apply to the virtual segment. A virtual segment can have only one SSL inspection profile applied to it.
   - Physical Segments – Physical segment associated with the virtual segment. All physical segments are directional.
   - Traffic Criteria – (Required) Specify any one or all of the following: VLAN ID, Source IP, and Destination IP. For example, omit VLAN ID and specify Destination IP. When specifying a VLAN ID, specify a value between 1 and 4094 in which the segment is included. There can be no duplicate VLAN IDs or overlapping VLAN ranges. No more than 512 VLAN IDs per virtual segment (a

VLAN range of 1–100 counts as 100 IDs). At least one traffic criteria (VLAN ID, source IP address, or destination IP address) must be defined for each virtual segment.

- Source IP Address – Source CIDR associated with the virtual segment. Addresses must be valid IPv4 format. The host portion of address/mask must be 0 (zero). No more than 250 addresses may be specified.
- Destination IP Address – Destination CIDR associated with the virtual segment. Addresses must be valid IPv4 format. The host portion of address/mask must be 0 (zero). No more than 250 addresses may be specified.

4. Click **OK**.

Note: Virtual segments must be created with a physically available segment. If creating a virtual segment generates a UDM warning in the system log, ensure you have associated the virtual segment with a valid physical segment.

Commit changes to the Running configuration

From the LSM, commit your changes to the Running configuration.

Depending on the type of configuration change, the device commits changes to the Running configuration:

- Automatically. An *instant commit* is one that is applied immediately to the Running configuration. Only some items, including Action Sets and Notification Contacts, are instant-commit features. A bright yellow notice is displayed on all features that use instant commit.
- Manually. A *deferred commit* is one that is not immediately committed to the Running configuration. Uncommitted changes are placed into a pending state until you explicitly commit them to the Running configuration. When you log out of the LSM, pending changes are lost.

  Defer your commit until you have completed the necessary configuration changes, then commit all of the changes at once. For example, when creating an SSL server, you must also import a device certificate and assign to the server before you can commit your changes.

To commit your pending changes to the Running configuration, in the Configuration menu, click **Commit pending changes**.

After you configure SSL inspection

After you configure SSL inspection, monitor SSL inspection activity to verify the 2200T device is inspecting the SSL sessions you want. If you want to restrict access to SSL configuration, give permissions to SSL inspection.

Verify SSL inspection activity

From the LSM, monitor SSL inspection activity.

View information about SSL inspection activity by choosing from the following:

- **Monitor > Sessions > SSL Sessions** displays active session count information for up to 50 SSL sessions. Filter the list to view details for the sessions you want.
- **Monitor > Network > SSL Bandwidth** displays overall SSL traffic seen and amount inspected.
- **Reports > Activity > SSL > Connections** displays the total number of new SSL connections that were created during the 1-minute reporting interval.
- **Reports > Activity > 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 **Monitor > Logs > SSL Inspection**. 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.

To display sessions details, such as connection resets, click **Columns > Details**. If you do not see SSL sessions for a particular server, enable logging on that server and then review this log for useful troubleshooting information. When you finish troubleshooting, disable logging on the server. Note that you can also configure notification contacts and thresholds for SSL inspection logs.

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.
- The Reputation Block and Alert logs (**Monitor > Reputation**) do not report on SSL sessions because Reputation is analyzed prior to SSL Inspection.

Give permissions for SSL inspection

From the LSM, give role-based permissions for SSL inspection. By default, SSL inspection permissions are given to the Administrator role.

Give role-based permissions to:

- SSL inspection profiles
- SSL servers
- SSL global settings
- SSL log
- SSL reports

Note: Only custom user roles can be edited; the default user roles cannot be edited.

1. Select **Authentication > User Roles.**
2. Click **Add** to create a user role or **Edit** to change an existing custom user role.

3. Enter a name.
4. (Optional) Enter a description for the user role.
5. Select one of the default roles to use as a template base role for the new role.
6. Check or uncheck each capability, including SSL inspection, for the new role.
7. Select either **Read-only** or **Read/Write** for the state.
8. Click **OK**.

Best Practices

Use this checklist to verify your SSL inspection configuration conforms to the recommended best practices.

❑	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 2200T does not validate the certificate and private key.
❑	Set role-based access controls to limit access to SSL inspection.
❑	Check the System log for errors.
❑	Keep your certificates up-to-date. Whenever you update a certificate on your server, be sure to also update the certificate on the 2200T. If a certificate expires, the System log generates an error.
❑	When managed by the SMS, you can choose to persist private keys on the SMS instead of on the 2200T device. For more information, see the *SMS User Guide*.

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 2200T 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 2200T 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?

To verify	Do this
The TPS is not bypassing SSL sessions	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 2200T does not inspect them. If necessary, reconfigure SSL inspection to reduce the number of concurrent SSL connections. For information about configuring SSL inspection to block SSL sessions that exceed the maximum threshold, contact TippingPoint Technical Support.
SSL inspection license is installed and valid	For a managed device, see *Verify the license package* on page 528 for more information. For an unmanaged device, see *Verify the license package* on page 537 for more information.
SSL inspection is enabled	For a managed device, see *Enable SSL inspection* on page 528 for more information. For an unmanaged device, see *Enable SSL inspection* on page 537 for more information.

To verify	Do this
The correct certificate and key are installed	For a managed device, see *Import the SSL server certificate and private key* on page 529 for more information. For an unmanaged device, see *Import the SSL server certificate and private key* on page 538 for more information.
The SSL server matches the correct IP address and port	For a managed device, see *SSL servers* on page 530 for more information. For an unmanaged device, see *Add or edit an SSL server* on page 539 for more information.
The profile is applied to the correct virtual segments	For a managed device, see *Distribute the inspection profile* on page 532 for more information. For an unmanaged device, see *Assign the SSL inspection profile to a virtual segment* on page 541 for more information.
The virtual segment includes the desired SSL server IP addresses and ports	Verify the SSL clients are reaching the SSL server.

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 (*show tse* on page 549).

   Entries are only present for the life of the session. If necessary, use the *debug np ssl-clear* on page 550 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 (*debug* on page 550) 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 information about troubleshooting configuration issues, see *Basic troubleshooting* on page 544.
3. Run the debug np stats show npSslInspProtocolStats command. If there are:

- Non-zero entries in "other cipher" it is probably an unsupported cipher. The other error counters can narrow where you need to look, to at least narrow it down to server vs. client side.
- 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 they are all zero, then no traffic is even being sent for inspection. If there is any TCP traffic matching a profile, these will be non-zero.

CLI Reference for the 2200T device

This section describes the CLI commands for the 2200T device related to configuring and troubleshooting SSL inspection.

Troubleshoot

This section describes the 2200T CLI commands related to troubleshooting SSL inspection.

show license

Syntax

```
show license
```

Example

```
ips{}show license
License: 5.0.0.46
Feature                  Status          Permit   Expiration   Details
--------                 ------          -------  ----------   --------
License                  OK              Allow    9/30/2015
Update TOS               OK              Allow    9/30/2015
Update DV                OK              Allow    9/30/2015
MalwareAuxDv             OK              Allow    9/30/2015
Auxiliary DV:ScadaAux    OK              Allow    9/30/2015
Auxiliary DV:Other       OK              Allow    9/30/2015
ReputationDV             OK              Allow    9/30/2015
SSL Inspection           OK              Allow    9/30/2015
Throughput Upgrade       Info            Deny     Never        Not licensed to
                                                               use this feature.
Feature                  Active       After Reboot
-------                  ------       ------------
Throughput Upgrade       20000 Mbps   No change
SSL Inspection           Allow        No change
```

display conf

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

Syntax

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

Example

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

```
ips{}display conf running
aaa                 actionsets        autodv            certificates
dns                 gen               highavailability  inspection-bypass
interface           ips               log               notifycontacts
ntp                 reputation        segment1          segment2
segment3            segment4          segment5          segment6
segment7            segment8          snmp              ssl-inspection
traffic-management virtual-segments  vlan-translations debug
```

Example

Displays SSL configuration.

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

```
    detection-port 999
    decrypted-service http
    cipher-suite RSA-3DES-EDE-CBC-SHA1
    cipher-suite RSA-AES128-CBC-SHA1
    cipher-suite RSA-AES256-CBC-SHA1
    protocol TLSv1.0
    protocol TLSv1.1
    protocol TLSv1.2
    certificate swdevts4b_cert
    logging
    tcp-reset
  exit
  # SSL PROFILES
  profile "swdevts4b"
    policy "swdevts4b"
      enable
      server "swdevts4b"
    exit
  exit
  profile "swdevts4b_profile"
    policy "swdevts4b_policy"
      enable
      server "swdevts4b_server"
    exit
  exit
  # LOG SERVICE
    log sslInspection "Management Console" ALL
    log sslInspection "Remote System Log"  ALL
```

show tse

Shows threat suppression engine information.

Syntax

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

Example of connection-table blocks

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

Protocol Src/Dest IP  Port         Src/Dest IP  Port  Reason
TCP      10.1.3.1     36051        10.1.3.2     44    6551: TCP: IPS Test Filter

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

Example of rate-limit

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

Protocol Src/Dest IP  Port   Src/Dest IP  Port   Reason
TCP      10.1.3.1     36052  10.1.3.2     44     6551: TCP: IPS Test Filter

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

Example of ssl-inspection

```
ips{}show tse ssl-inspection
SSL Inspected Sessions: 1 of 1 shown.

Client IP  Port   Interface  Proto    Cipher
---------- -----  ---------- -------  ----------------------
10.1.3.1   42523  5B         TLSv1.2  TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

Server IP  Port   Interface  Proto    Cipher
---------  ------ ---------  ------   ----------------------------
10.1.3.2   443    5A         TLSv1.2  TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
```

debug

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

Syntax

```
debug

Valid entries at this position are:

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

Examples

See the following examples for more information about debug commands.

debug factory-reset

```
debug factory-reset

WARNING!!!

This command WILL reset this device to factory default configuration.

This will remove all network and security configuration, user accounts
log files, snapshots and applied software upgrades

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

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

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

debug np best-effort options

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

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

Subcommands

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

Subcommand	Description	Usage
`enable`	Enables Best Effort mode.	`debug np best-effort enable [-queue-latency <microseconds>] [-recover-percent <percent>]`
`disable`	Disables Best Effort mode.	`debug np best-effort disable`

Options

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

Option	Description	Usage
`-queue-latency`	Defines the latency threshold at which Best Effort mode is entered. The default is 1000 microseconds.	`debug np best-effort enable -queue-latency <microseconds>`
`-recover-percent`	Defines the recovery percentage at which Best Effort mode is exited. The default is 20%; if the latency threshold is 1000 microseconds, the device exits Best Effort mode when latency drops to 200 microseconds (20% of 1000).	`debug np best-effort enable -recover-percent <percent>`

debug np mcfilt-regex options

Microfilter regular expression statistics.

`debug np regex [clear|show option]`

Option	Description
`clear`	Clears regular expression statistics.
`show average`	Sorts and displays network processor information based on average time.
`show count`	Specifies the number of entries to display. Default: 10
`show evaluations`	Sorts and displays network processor information based on the number of evaluations.

Option	Description
`show matches`	Sorts and displays network processor information based on the number filter matches.
`show maximum`	Sorts and displays network processor information by maximum time. Default: The default display if you do not specify another option.
`show total`	Sorts and displays network processor information by total time.

debug np regex options

Regular expression statistics.

```
debug np regex [clear|show option]
```

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

debug np stats options

Show/clear engine statistics.

```
debug np stats [clear|help|show]
```

Option	Description
`clear`	Clears regular expression statistics.
`help`	Lists available statistics tables.
`show`	Shows system information. **Note:** When an active session is closed, the session count is decremented. If the session count was already set to zero by the `clear` command, then the session count will incorrectly appear as a very large number.

debug np stats show npSslInspStats Example

The following example displays potential culprits of SSL inspection:

```
ips{}debug np stats show npSslInspStats
Connections:
 clientConnections = 1        ; Number of client connections
 clientConnectionFailures = 0 ; Number of client connection failures
 serverConnections = 1        ; Number of server connections
 serverConnectionFailures = 0 ; Number of server connection failures
 refusedConnections = 9       ; Number of refused sessions
Sessions:
 activeSessions = 0           ; Number of active sessions
 inspectedSessions = 1        ; Number of inspected sessions
 blockedSessions = 0          ; Number of blocked sessions
 trustedSessions = 0          ; Number of trusted sessions
 flushTrustedSessions = 0     ; Number of flushed trusted sessions
 shuntedSessions = 0          ; Number of shunted sessions
 blockedMaxSslConnections = 0 ; Number of blocked sessions due to max conn limit
 allowedMaxSslConnections = 0 ; Number of allowed sessions due to max conn limit
Renegotiation:
 renegotiationServerSide = 1 ; Number of renegotiations initiated by the server
 renegotiationClientSide = 2 ; Number of renegotiations initiated by the client
 renegotiationProxy = 0      ; Number of renegotiations initiated by the proxy
Certificate Requests:
 clientCertificateRequests = 0 ; Number of client certificates requested by server
```

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

debug np congestionx Example

The following example displays potential culprits of network congestion:

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

debug np diagx Example

The following example displays diagnostic information:

```
ips{} debug np diagx -details
Switch (packet flow from top left counterclockwise)
         1A               0               0
     Bypass               0               0
     Uplink               0               0      RX Dropped   0     RX Pause   0

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

Time since last snapshot: 1 minute, 12 seconds
```

debug np regex Example

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

```
ips{}debug np regex show average
-------------------------------------------------------------------------------
Filter      CRC      Flag  Max(us)  Avg(us)       Evals    Matches   Total(us)
-------------------------------------------------------------------------------
   3179  0x0f7b8828   P        795      768           4          0        3073
   4062  0xaf664079   PS       595      466           4          4        1866
   5995  0xed3a9991   R        308      234           4          0         938
  10762  0xf4a09ead   P        614      169           8          0        1350
   6413  0xbea34771   R        114      109           2          0         218
```

```
  10777  0x602fe470   R        417      105          55       0        5750
   6416  0xb34d4b62   R        102      102           1       0         102
   6417  0x65b97c0b   R         98       98           1       0          98
   6356  0x4b09bc88   R        103       85           4       0         341
   6662  0x96dcebfe   P        130       80          18       0        1439
```

debug np ssl-clear Example

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

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

debug np stats Example

The following example displays system information:

```
ips{}debug np stats help
  udmAggStats                 (CP only)    UDM Aggregation Statistics
  cpMiscStats                 (CP only)    Control Plane Miscellaneous Stats
  npMetadataStats             (DP only)    Event Metadata Statistics
  npIrrStats                               NetPal Inverted Reroute Stats
  npMicrofilterStats          (DP only)    NetPal Microfilter Statistics
  npHttpResponseStats         (DP only)    HTTP Response Statistics
  dpalStats                   (CP only)    DPAL counters
  asFlowControlStats                       Action Set Flow Control Stats
  fqStats                     (DP only)    FlowQueue Stats
  npScanSweepMemStats                      NetPal Scan/Sweep Memory Stats
  npScanSweepStats                         NetPal Scan/Sweep Statistics
  dpsIpcClassStats                         dpsIpc per-class stats
  npZlibStats                              NetPal Zlib Statistics
  sleuthPatterns              (CP only)    Sleuth pattern table stats
  ruleStatsStats                           stats about rule stats
  dpsIpcConv                               dpsIpc Conversion stats
  npTrafficCaptureStats                    NetPal traffic capture stats
  dpsIpcRpcStats              (CP only)    dpsIpcRpc Stats
  dpwdStats                   (CP only)    DP Watchdog Statistics
  eccStatsXlrC                (CP only)    XLRC's ECC Stats
  eccStatsXlrB                (CP only)    XLRB's ECC Stats
  eccStatsXlrA                (CP only)    XLRA's ECC Stats
  eccStats                    (DP only)    ECC Stats
  dpsTiming                   (DP only)    Timing Subsystem
  dpsIpcCPStats               (CP only)    dpsIpc CP Stats
  lwipStats                   (DP only)    lwip Stats
  dpsIpcStats                              dpsIpc Stats
  snakeStats                               Snake Stats
  npTurboSimLfhStats          (DP only)    Turbo Simulator LF Hash Stats
  npQuarantineActionLfhStats  (DP only)    Quarantine Action LF Hash Stats
```

```
  npQuarantineAqciLfhStats    (DP only)    Quarantine AQCI LF Hash Stats
  npQuarantineStats                        NetPal Quarantine Packet Stats
  npSynProxyStats             (DP only)    NetPal SYN Proxy Statistics
  npIpReputationIpcStats                   IP Reputation command IPC Stats
  npIpReputationRequestStats  (CP only)    (null)
  npIpReputationCallbackStats (DP only)    IP Reputation Callback Stats
  npDnsReputationStats        (DP only)    DNS Reputation Statistics
  npIpReputationStats         (DP only)    IP Reputation Statistics
  npHreStats                  (DP only)    Rule Statistics
  npSoftLinxStats             (DP only)    NetPal SOFTLINX Statistics
  trhaStats                   (CP only)    TRHA Statistics
  npTcpStateStats             (DP only)    TCP State module stats.
  rlStats                     (DP only)    Policy Rate Limiter Statistics
  npHCDspStats                (DP only)    NetPal HardCode Statistics
  npIPDgrams                  (DP only)    (null)
  npZoneStats                 (DP only)    ZoneStats
  npTelnetStats               (DP only)    TELNET Decode Statistics
  npSnmpStats                 (DP only)    SNMP Decode Statistics
  npSmtpStats                 (DP only)    SMTP Decode Statistics
  npSmbStats                  (DP only)    SMB Decode Statistics
  npRpcStats                  (DP only)    RPC Decode Statistics
  npMsrpcStats                (DP only)    MS-RPC Decode Statistics
  npOspfStats                 (DP only)    OSPF Decode Statistics
  npImapStats                 (DP only)    IMAP Decode Statistics
  npHttpStats                 (DP only)    HTTP Decode Statistics
  ahpStats                    (DP only)    ahp Stats
  npFtpStats                  (DP only)    FTP Decode Statistics
  npDnsStats                  (DP only)    DNS Decode Statistics
  udmCbStats                               UDM Callback Statistics
  npTTStats                                NetPal Trust Table Statistics
  npCTStats                                NetPal Connection Table Statistics
  pcbStats                    (DP only)    PCB Stats
  txStats                     (DP only)    TX Stats
  rxStats                     (DP only)    Rx Stats
  threadFwdStats              (DP only)    NetPal Parse Packet Statistics
  npHardCodeStats             (DP only)    HardCode Packet Statistics
  npFilterStatsInst           (DP only)    (null)
  npReparseStatsInst          (DP only)    NetPal Non-ingress Parse Packet Stats
  npParseStatsInst            (DP only)    NetPal Parse Packet Statistics
  npTcpReas                   (DP only)    TCP Reassembly Statistics
  npReasIpv6                  (DP only)    IPv6 Reassembly Statistics
  npReas                      (DP only)    IPv4 Reassembly Statistics
  dpk                         (DP only)    Data Plane Stats
  triv                                     Sample stats
ips{}debug np stats show trhaStats
TRHA:
    trhaSend = 0    ; trhaSend
    trhaReceive = 0 ; trhaReceive
```

```
    trhaDropped = 0 ; trhaDropped
Host Communication:
    hostCommSend = 0    ; hostCommSend
    hostCommReceive = 0 ; hostCommReceive
    hostCommDropped = 0 ; hostCommDropped
Delay:
    delayTotal = 0 ; delayTotal
    delayCount = 0 ; delayCount
```

debug np port Example

The following example displays system information:

```
ips{}debug np port show
PORT status:
Local Device 0  (switch in NORMAL mode) --------------------------------
Port  Bcm  Num    Admin    Status Speed  AutoNeg Pause  Mode  MTU  Medium SP MMU
                                                                          cells
 enet1  ge1  3    Disabled DOWN   1Gbps  auto      -    GMII  1526  Fiber  0   0
 enet2  ge0  2    Disabled DOWN   1Gbps  auto      -    GMII  1526  Fiber  0   0
 enet3  ge3  5    Disabled DOWN   1Gbps  auto      -    GMII  1526  Fiber  0   0
 enet4  ge2  4    Disabled DOWN   1Gbps  auto      -    GMII  1526  Fiber  0   0
 enet5  ge5  7    Disabled DOWN   1Gbps  auto      -    GMII  1526  Fiber  0   0
 enet6  ge4  6    Disabled DOWN   1Gbps  auto      -    GMII  1526  Fiber  0   0
 enet7  ge7  9    Disabled DOWN   1Gbps  auto      -    GMII  1526  Fiber  0   0
 enet8  ge6  8    Disabled DOWN   1Gbps  auto      -    GMII  1526  Fiber  0   0
 enet9  ge9  11   Enabled  UP     1Gbps  auto    none  SGMII  1526 Copper  0   0
enet10  ge8  10   Enabled  UP     1Gbps  auto    none  SGMII  1526 Copper  0   0
enet11  ge11 13   Enabled  UP     1Gbps  auto    none  SGMII  1526 Copper  0   0
enet12  ge10 12   Enabled  UP     1Gbps  auto    none  SGMII  1526 Copper  0   0
enet13  ge13 15   Disabled DOWN       -  auto      -   SGMII  1526 Copper  0   0
enet14  ge12 14   Disabled DOWN       -  auto      -   SGMII  1526 Copper  0   0
enet15  ge15 17   Enabled  UP     1Gbps  auto    none  SGMII  1526 Copper  0   0
enet16  ge14 16   Enabled  UP     1Gbps  auto    none  SGMII  1526 Copper  0   0
uplnk0  xe0  26   Uplink   UP    10Gbps  none    none  XGMII 16356  Fiber  0   0
uplnk1  xe1  27   Uplink   UP    10Gbps  none    none  XGMII 16356  Fiber  0   0
uplnk2  xe2  28   Uplink   DOWN  10Gbps  none      -   XGMII 16356  Fiber  0   0
uplnk3  xe3  29   Uplink   DOWN  10Gbps  none      -   XGMII 16356  Fiber  0   0
ips{}debug np port diags 1A
Port:                   enet1 (uport 1; port 3)
Enable state:           Disabled
Link status:            DOWN
Laser status:           SFP absent and laser off
Linkscan mode:          SW
Auto-negotiated:        (no link)
Port ability:           fd = 100MB,1000MB
                        hd = <none>
                        intf = gmii
                        medium = <none>
```

```
                          pause = pause_tx,pause_rx,pause_asymm
                          lb = none,MAC,PHY
                          flags = autoneg
Advertised ability:       fd = 1000MB
                          hd = <none>
                          intf = <none>
                          medium = <none>
                          pause = <none>
                          lb = <none>
                          flags = <none>
STP mode:                 Forward
Learn mode:               FWD
Untag priority mask:      0
Multicast flood (pfm):    FloodNone
Interface:                GMII
Max_frame size:           1526
MDIX mode:                ForcedNormal, Normal
Medium:                   Fiber
```

debug show settings Example

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

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

show np tier-stats

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

Syntax

```
show np tier-stats
```

Example

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

```
-------------------------------------------------------
Tier 2 (Software Fastpath):
-------------------------------------------------------
Rx Mbps               =        261.7  (838.2)
Rx Packets/Sec        =     31,054.0  (74,982.0)
Tx trust packets/sec  =          0.0  (0.0)
Utilization           =         23.7% (76.2%)
Ratio to next tier    =        100.0% [99.6%]
-------------------------------------------------------
Tier 3 (IPS Engine Fastpath):
-------------------------------------------------------
Rx Mbps               =        261.7  (836.4)
Rx Packets/Sec        =     31,054.0  (74,781.0)
Tx trust packets/sec  =          0.0  (0.0)
Utilization           =         23.7% (76.0%)
Ratio to next tier    =          0.0% (0.0%)
-------------------------------------------------------
Tier 4 (IPS Engine Slowpath):
-------------------------------------------------------
Rx Mbps               =          0.0  (0.0)
Rx Packets/Sec        =          0.0  (2.0)
Rx due to:
   Trigger match       =          0.0% (0.0%)
   Reroute             =          0.0% (50.0%)
   TCP sequence        =          0.0% (0.0%)
   Protocol decode     =          0.0% (0.0%)
Utilization           =          0.0% (0.0%)
Ratio to deep         =          0.0% (0.0%)
-------------------------------------------------------
Tier 5 (SSL Inspection):
-------------------------------------------------------
Rx Mbps               =        252.7  (257.7)
Rx Packets/Sec        =     21,823.0  (22,256.0)
Utilization           =         22.9% (23.4%)
```

show ssl-inspection congestion

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

Syntax

```
show ssl-inspection congestion
```

Example

```
ips{}show ssl-inspection congestion
SSL connection rate:      3.15 conn/sec
```

```
SSL current connections:  152 of max 100000 connections
SSL congested action:     Pass
```

keystore

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

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

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

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

Syntax

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

Related commands

Command	Description
ips{running-certificates}private-key on page 562	Import the private key from your web server into the local keystore on the device.
ips{running-certificates}certificate on page 562	Import the certificate from your web server into the local keystore on the device.
ips{running-sslinsp}server on page 565	Add an SSL server to the device with the same security settings as your web server, and assign the corresponding certificate and private key.

Configure

This section describes the CLI commands related to configuring SSL inspection.

ips{running-certificates}certificate

Add or update a device certificate with the certificate contents from your web server. To inspect secure sessions, the 2200T requires both the certificate and private key from your web server.

We recommend naming the certificate so that you can safely and reliably assign it to the correct SSL server.

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

Syntax

```
certificate CERTNAME
```

Example

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

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

Related commands

Command	Description
ips{running-certificates}private-key on page 562	Import the private key from your web server into the local keystore on the 2200T device.
ips{running-sslinsp}server on page 565	Add an SSL server to the 2200T device with the same security settings as your web server, and assign the corresponding certificate and private key.

ips{running-certificates}private-key

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

To inspect secure sessions, the 2200T requires both the certificate and private key from your web server.

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

Syntax

```
private-key CERTNAME
```

Example

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

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

Related commands

Command	Description
ips{running-certificates}certificate on page 562	Import the certificate from your web server into the local keystore on the 2200T device.
ips{running-sslinsp}server on page 565	Add an SSL server to the 2200T device with the same security settings as your web server, and assign the corresponding certificate and private key.

ips{running-sslinsp} Context Commands

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

Note: While SSL inspection is disabled, you can configure SSL inspection to specify the SSL sessions you want to inspect. However, the 2200T will not inspect secure sessions.

Syntax

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

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

ips{running-sslinsp}enable

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

To enable SSL inspection, the 2200T must be licensed for SSL inspection. Use the LSM to verify the SSL inspection license.

Syntax

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

Example

Enable SSL inspection to begin inspecting SSL sessions.

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

ips{running-sslinsp}log sslInspection

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

Important: To generate SSL inspection log entries, enable logging on the SSL server for troubleshooting purposes only. By default, an SSL server does not generate logging information. See *ips{running-sslinsp}server* on page 565 for more information.

Syntax

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

Example

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

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

ips{running-sslinsp}server

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

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

Syntax

```
[delete] server SERVERNAME
```

Example

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

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

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

Tip: The `protocol SSL-PROTOCOL` and `cipher-suite SSL-PROTOCOL` options have "auto-" commands to allow selection of cipher suites by protocol or protocols by cipher suite, respectively. This will add or delete ciphers based on what protocol is selected and what it supports. For more information about the available commands in the subcontext, type `help` and press Enter.

```
ips{running-sslinsp-server-myserver}help
Valid commands are:
  certificate SERVERCERT
  cipher-suite all|(protocol SSL-PROTOCOL)|CIPHER-SUITE
  compression enable|disable
  decrypted-service SERVICENAME
  delete cipher-suite all|(protocol SSL-PROTOCOL)|CIPHER-SUITE
  delete description
  delete detection-port (all|PORT [to LAST-PORT])
  delete ip address( all|A.B.C.D/M)
  delete protocol all|SSL-PROTOCOL [auto-delete-ciphers]
  delete rekey-interval
  description TEXT
  detection-port PORT [to PORT]ex
  display [xml]
  help [full|COMMAND]
  ip address( A.B.C.D|A.B.C.D/M)
```

```
  logging enable|disable
  protocol all|SSL-PROTOCOL [auto-add-ciphers]
  rekey-interval INTERVAL
  tcp-reset enable|disable
```

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

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

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

(Required) Specify the **IP address** of your web server by entering up to 8 IPv4 addresses (separated by commas), or by specifying a CIDR range, such as 192.168.0.1/24.

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

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

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

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

```
ips{running-sslinsp-server-myserver}display
server "myserver"
  ip address 192.168.0.1/24
  detection-port 443
  decrypted-service http
  protocol TLSv1.0
```

```
  protocol TLSv1.1
  protocol TLSv1.2
  cipher-suite TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
  cipher-suite TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
  cipher-suite TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
  cipher-suite TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
  cipher-suite TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
  cipher-suite TLS_RSA_WITH_3DES_EDE_CBC_SHA
  cipher-suite TLS_RSA_WITH_AES_128_CBC_SHA
  cipher-suite TLS_RSA_WITH_AES_128_CBC_SHA256
  cipher-suite TLS_RSA_WITH_AES_256_CBC_SHA
  cipher-suite TLS_RSA_WITH_AES_256_CBC_SHA256
  logging disable
  compression disable
  tcp-reset enable
exit
```

Related commands

Command	Description
ips{running-certificates}certificate on page 562	Import the certificate from your web server into the local keystore on the device.
ips{running-certificates}private-key on page 562	Import the private key from your web server into the local keystore on the device.
ips{running-vsegs-VSEG_NAME}ssl-profile on page 569	Update the virtual segment to assign the SSL inspection profile.
ips{running-sslinsp}profile on page 567	Assign the SSL server to an SSL inspection profile.

ips{running-sslinsp}profile

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

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

Syntax

```
[delete] profile PROFILENAME
```

Example

Create a profile named myprofile.

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

The context changes to the `myprofile` subcontext.

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

```
ips{running-sslinsp-myprofile}help
Valid commands are:
  delete description
  delete policy all|POLICYNAME
  description TEXT
  display [xml]
  help [full|COMMAND]
  policy NEWPOLICYNAME
  policy POLICYNAME
  rename policy POLICYNAME NEWPOLICYNAME
```

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

```
ips{running-sslinsp-myprofile}policy mypolicy
```

The context changes to the **mypolicy** policy.

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

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

(Optional) Update the policy to specify any source IP addresses that you do not want to inspect. Secure sessions between the server and the specified source IP addresses are not inspected. In the following example, the server policy will not inspect inbound encrypted traffic between **mysslserver** and client IP addresses within the range of 10.7.0.1/24.

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

Related commands

Command	Description
ips{running-certificates}certificate on page 562	Import the certificate from your web server into the local keystore on the device.
ips{running-certificates}private-key on page 562	Import the private key from your web server into the local keystore on the device.
ips{running-vsegs-VSEG_NAME}ssl-profile on page 569	Update the virtual segment to assign the SSL inspection profile.
ips{running-sslinsp}server on page 565	Add an SSL server with its assigned security certificate and private key.

ips{running-vsegs-VSEG_NAME}ssl-profile

Edit the virtual segment to assign an SSL inspection profile.

Syntax

```
ssl-profile PROFILENAME
```

Example

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

Related commands

Command	Description
ips{running-sslinsp}profile on page 567	Create an SSL-inspection profile.

commit

Commits your pending configuration changes to the Running configuration.

When you commit configuration changes, or when changes are committed automatically, the changes are committed to the Running configuration, and the changes are visible to all users. However, when the

device reboots, the Running configuration is reset to the Startup configuration. Uncommitted changes and committed changes in the Running configuration are lost.

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

Syntax

```
commit
```

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

```
ips{running}commit
```

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

Related commands

Command	Description
save-config on page 570	Copy the Running configuration to the Startup configuration.

save-config

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

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

Syntax

```
save-config
```

Examples

Copies the Running configuration to the Startup configuration. Note that in order to run this command from the top-level prompt, you must commit or discard your pending configuration changes.

```
ips{}save-config
```

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

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

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

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

Related commands

Command	Description
commit on page 569	Commit your pending changes to the Running configuration.

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 572

Password recovery on page 572

Network changes on page 573

IPS port out-of-service on page 574

SMS error messages on page 574

TMC connectivity on page 576

Geo Locator maps do not display correctly on page 577

Login error messages

To recover from errors that occur in the Login dialog box, see the following items.

Error message	Action
Connect Failed	• Verify that you entered the correct IP address or fully qualified hostname for the server. • Verify that the server is properly connected to the network and that the network is up.
Can't authenticate! Retype and try again	Verify that you typed the correct username and password.

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 447
   - 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 447
   - 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 filter* on page 141 and *Traffic Management filters* on page 169.

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.
```

Modifying filter action settings

In the SMS, you can select several filters at a time to modify the settings. If you want to modify the action set settings for the filters, an error message displays suggesting a recommended action.

Note: To modify the action set for multiple filters within a category, we recommend using the Category Settings for a category of filters. The Category Settings affect action set changes across all filters for a category. See *Profiles* on page 102.

You may receive the following message:

```
Using Category Settings is recommended when modifying several filters.
```

Adding exceptions

The SMS has a set limit for the number of filters you may modify and save for a profile. This limit promotes better performance for your system. Adding an exception to a set of selected filters counts against this limit setting.

Note: To add exceptions to multiple filters, we recommend creating an exceptions through the Shared Settings. Shared Settings allow you to create and distribute a single exception to all filters within appropriate filter categories. See *Profiles* on page 102 and *Traffic Management filters* on page 169.

When you attempt to add too many exceptions to individual filters, you receive the following message:

```
Using Shared Settings is recommended when adding exceptions to several
filters.
```

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 filter, of filter objects, 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 102 and *Traffic Management filters* on page 169.

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. In the CLI, you might get an error message when you issue the `get health.tmc-valid` command from the CLI.

Message	Meaning
OK	SMS was able to connect to both the TMC server and TMC package server

Message	Meaning
Cannot connect to server <hostname>: host unreachable	Network error prevented the SMS from contacting TMC
DNS lookup failure for server <hostname>	TMC server hostname could not be resolved
This SMS is not registered on TMC	TMC is rejecting the SMS connection because the SMS has not been registered with the TMC
TMC connection error: <error>	Other errors connecting to TMC
TMC Proxy authentication error	TMC proxy is rejecting your authentication
TMC Proxy: DNS lookup failure for TMC server <hostname>	TMC proxy failed the DNS lookup for the TMC server
TMC Proxy: host <hostname> unreachable	TMC proxy could not contact the TMC server
Possible proxy DNS lookup error on package server <hostname>	TMC package server proxy is likely failing with a DNS error
TMC package server error: <error>	Other errors from the TMC package server
Network error connecting to TMC package server <hostname>	SMS could not reach the TMC package server
DNS lookup failure for TMC package server <hostname>	TMC package server hostname could not be resolved

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).

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

Port	Service	From	To	Description
Network ports required to use the SMS client				
22/TCP	SSH	SMS client	SMS server	CLI management of SMS
9033/TCP	SMS	SMS client	SMS server	Required for the SMS client to connect to the SMS server
10042/TCP	SMS	SMS client	SMS server	Required for the SMS client to connect to the SMS server
443/TCP	HTTPS	SMS client browser	SMS server	File downloads, such as client installation, exported reports, Web services (if configured)
Network ports required for the SMS to manage TippingPoint devices				
161/UDP	SNMP (agent)	SMS server	IPS	SMS management
443/TCP	HTTPS	SMS server	TPS, IPS, NGFW	SMS management

Port	Service	From	To	Description
8162/UDP	SNMP (trap)	IPS	SMS server	SNMP traps from device to SMS
8163/UDP	SNMP (trap)	IPS	SMS server	SNMP traps from device to SMS
Network ports required for the SMS to access the TMC for software and security updates [1]				
80/TCP	HTTP	SMS server	Outbound	Digital Vaccine updates from TMC
443/TCP	HTTPS	SMS server	TMC	Updates from TMC For new SMS installations, this port is the **NEW** default for communication with the TMC
4043/TCP	HTTPS	SMS server	TMC	Updates from TMC If your installation is prior to V 2.5.1, this port is the default for communication with the TMC. Upgrading does not change this port setting

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** on the SMS client.

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.

Port	Service	From	To	Description
Active Response ports				
23/TCP	Telnet	SMS server	External switch	Active Response switch disconnect action
25/TCP	SMTP	SMS server	Mail server	Active Response email action
80/TCP	HTTP	SMS server	Remote host	Active Response Web action
162/UDP	SNMP	SMS server	Remote host	Active Response SNMP action
162/UDP	SNMP	SMS server	Remote host	Active Response NMS action
514/UDP	Syslog	SMS server	Syslog server	Active Response Syslog action

Port	Service	From	To	Description
1812/UDP	RADIUS	External switch	SMS server	RADIUS proxy (required for Active Response switch disconnect action)
Active Response (triggers) for the port availability				
80/TCP	HTTP	External host	SMS server	Trigger Active Response/ via URL, IP correlation lookup, IP or MAC lookup
162/UDP	SNMP	NMS server	SMS server	SNMP traps from an SNMP client or NMS server, such as 3Com Network Directory (3ND) to Active Response
443/TCP	HTTPS	External host	SMS server	Trigger Active Response via URL, IP correlation lookup, IP or MAC lookup

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 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*.

Port	Service	From	To	Description
22/TCP	SSH	SMS primary	SMS secondary	Secure remote command execution and file replication
		SMS secondary	SMS primary	
1098/TCP	RMI	SMS primary	SMS secondary	JAVA RMI for HA configuration and remote peer administration
		SMS secondary	SMS primary	
1099/TCP	RMI registry	SMS primary	SMS secondary	JAVA RMI for HA configuration and remote peer administration
		SMS secondary	SMS primary	
3306/TCP	MySQL	SMS primary	SMS secondary	Database replication
		SMS secondary	SMS primary	
4444/TCP	RMI	SMS primary	SMS secondary	JAVA RMI for HA configuration and remote peer administration
		SMS secondary	SMS primary	
10042/TCP	SMS	SMS primary	SMS secondary	CLI command replication
		SMS secondary	SMS primary	

Optional ports

The following table lists and describes the optional ports that you can make available.

Port	Service	From	To	Description
SMS client port				
23/TCP	Telnet	SMS client	SMS server	CLI
10042/TCP	SMS	SMS client	SMS server	SMS backup restore
SMS client browser port				
80/TCP	HTTP	SMS client browser	SMS server	File downloads, such as client installation, exported reports, Web services
SNMP client port				
161/UDP	SNMP	SNMP client	SMS server	To query SMS SNMP MIBs
Device ports				
123/UDP	NTP	IPS	SMS server	Required only if IPS uses SMS for NTP time synchronization
6343/UDP	sFlow®	IPS	sFlow® server	Send sFlow® data from NX-platform IPS to one or more sFlow® servers

Port	Service	From	To	Description
10043/TCP	SMS provision	IPS	SMS server	Remote Authentication
SMS server ports				
389/TCP	Active Directory	SMS server	AD server	SMS AD LDAP authentication
636/TCP	Active Directory	SMS server	AD server	SMS AD LDAP over SSL authentication
3306/TCP	Database	SMS server	Any	External database access
			External server	External replication
53/TCP/UDP	DNS	SMS server	Name server	Name resolution
135/TCP	ID correlation	SMS server	AD server	SMS AD authentication
239/UDP	IP2ID	SMS server	IPS (A10)	IDsentrie
111/TCP/UDP	NFS	SMS server	File server	Report export, database backup
369/TCP/UDP				
2039/TCP/UDP				

Port	Service	From	To	Description
123/UDP	NTP	SMS server	NTP server (time source)	Time synchronization from external NTP server
1812/UDP	RADIUS	SMS server	RADIUS server	SMS user authentication
49/TCP	TACACS+	SMS server	TACACS+ server	SMS user authentication
137/TCP/UDP	Samba	SMS server	File server	Report export, database backup
138/TCP/UDP				
139/TCP/UDP				
1512/TCP/UDP				
25/TCP	SMTP	SMS server	Mail server	Email notifications, such IPS events, Active Response
514/UDP	Syslog	SMS server	Syslog server	SMS audit and syslog

Filters

Filters are a part of security profiles and can be customized to address specific network security needs. Filters are policies with settings and rules for managing and blocking traffic on a network. Each filter includes an action set that contains instructions for managing data and a category setting. The TMC assesses each attack filter and assigns it to one of the categories.

Filter	IPS	E-Series	IPS-N
Application Protection (category)			
Vulnerabilities	X	X	X
Exploits	X	X	X
Security Policy	X	X	X
Reconnaissance	X	X	X
Virus	X	X	X
Spyware	X	X	X
Identity Theft	X	X	X
Infrastructure Protection (category)			
Advanced DDoS/ Thresholding		X	
Network Equipment	X	X	X
Traffic Normalization	X	X	X

Filter	IPS	E-Series	IPS-N
Traffic Thresholds	X	X	X
Reputation			X
Performance Protection (category)			
Peer to Peer	X	X	X
Instant Messaging	X	X	X
Streaming Media	X	X	X
Traffic Management (category)			
IP Filtering	X	X	X
Other (categories)			
VPN			

Note: Specific devices may not support certain types of filters. For more information, see the Release Notes for the SMS release your are using. Release Notes are available from the TippingPoint Threat Management Center (*https://tmc.tippingpoint.com*).

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.

	New Device					
Old Device	**440T**	**2200T**	**110**	**330**	**660N**	**1400N**
440T	Y	Y	N	N	N	N
2200T	N	Y	N	N	N	N
110	Y	Y	Y	N	N	N
330	Y	Y	N	Y	N	N
660N	Y	Y	N	N	Y	N
1400N	N	Y	N	N	N	Y

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.

	New Device									
Old Device	**1200**	**2400**	**210E**	**600E**	**1200E**	**2400E**	**5000E**	**10**	**110**	**330**
1200	Y	Y	Y	Y	Y	Y	Y	DL	Y	Y
2400	N	Y	Y	Y	Y	Y	Y	DL	Y	Y
210E	DL	DL	Y	DL	DL	DL	DL	DL	DL	DL
600E	PD	PD	Y	Y	Y	Y	Y	DL	Y	Y
1200E	PD	PD	Y	Y	Y	Y	Y	DL	Y	Y
2400E	PD	PD	Y	Y	Y	Y	Y	DL	Y	Y
5000E	PD	PD	Y	Y	Y	Y	Y	DL	Y	Y
10	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
110	Y	Y	Y	Y	Y	Y	Y	DL	Y	Y
330	Y	Y	Y	Y	Y	Y	Y	DL	Y	Y

	New Device													
Old Device	**10***	**110**	**330***	**660N**	**1200N**	**1400N**	**2500N**	**5100N**	**6100N**	**2600NX**	**5200NX**	**6200NX**	**7100NX**	**7500NX**
10*	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y	Y
110	DL	Y	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y	Y

	New Device													
Old Device	**10***	**110**	**330***	**660N**	**1200N**	**1400N**	**2500N**	**5100N**	**6100N**	**2600NX**	**5200NX**	**6200NX**	**7100NX**	**7500NX**
330*	DL	Y	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y	Y
660N	N	N	N	Y	N	Y	Y	Y	Y	Y	Y	Y	Y	Y
1200N	N	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
1400N	N	N	N	Y	N	Y	Y	Y	Y	Y	Y	Y	Y	Y
2500N	N	N	N	Y	N	Y	Y	Y	Y	Y	Y	Y	Y	Y
5100N	N	N	N	Y	N	Y	Y	Y	Y	Y	Y	Y	Y	Y
6100N	N	N	N	Y	N	Y	Y	Y	Y	Y	Y	Y	Y	Y
2600NX	N	N	N	N	N	N	N	N	N	Y	Y	Y	Y	Y
5200NX	N	N	N	N	N	N	N	N	N	N	Y	Y	Y	Y
6200NX	N	N	N	N	N	N	N	N	N	N	Y	Y	Y	Y
7100NX	N	N	N	N	N	N	N	N	N	N	Y	Y	Y	Y
7500NX	N	N	N	N	N	N	N	N	N	N	Y	Y	Y	Y

* 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 592 and *Replacing an existing NX model with another NX model* on page 592

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

- SecBlade devices can only replace or be replaced by another SecBlade device.
- 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.

Reputation information

The TippingPoint Reputation Database contains records of suspect IP and domain addresses 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 160 and *Reputation database* on page 203.

Reputation import rules

The SMS allows you to enter data in the Reputation Database by importing a CSV 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

- The import file must be in comma-separated value (CSV) format; each line consists of one or more fields separated by commas.
- 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 or DNS name 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 or DNS domain name) 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.

Port	Protocol	Ciphers/Algorithms	Description
443	TLSv1.0 TLSv1.1 TLSv1.2 SSLv2Hello	TLS_RSA_WITH_AES_128_CBC_SHA SSL_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA256 (only supported with TLSv1.2)	HTTPS service • SSL provided by SunJSSE • Encryption algorithms provided by SunJCE (Non-FIPS) and NSS (FIPS)
10042, 9033	TLSv1.0 TLSv1.1 TLSv1.2	TLS_RSA_WITH_AES_128_CBC_SHA SSL_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA256 (only supported with TLSv1.2)	Client-server communication • SSL provided by SunJSSE • Encryption algorithms provided by SunJCE (Non-FIPS) and NSS (FIPS)
10043	TLSv1.0 TLSv1.1 TLSv1.2 SSLv2Hello	TLS_RSA_WITH_AES_128_CBC_SHA SSL_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA256 (only supported with TLSv1.2)	Device provision manager (device remote authorization)
22	SSH-2	aes128-ctr aes192-ctr aes256-ctr	SSH service • SSH provided by OpenSSH

Port	Protocol	Ciphers/Algorithms	Description
			• Encryption algorithms provided by OpenSSL

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.

TREND MICRO INCORPORATED
225 E. John Carpenter Freeway, Suite 1500
Irving, Texas 75062 U.S.A.
Phone: +1 (817) 569-8900, Toll-free: (888) 762-8736
Email: support@trendmicro.com

www.trendmicro.com
Item Code: APEM47353/160315